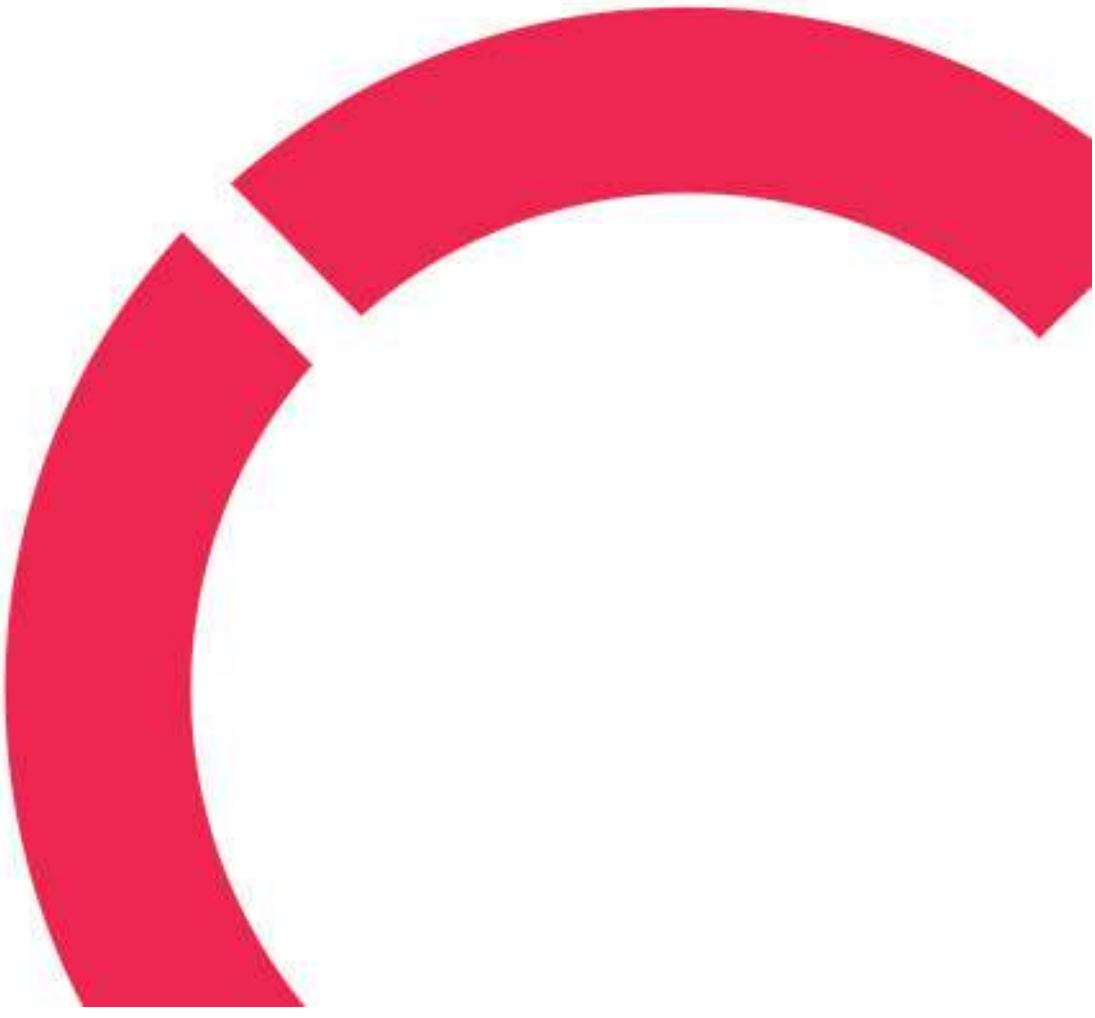
Saku Hirsikangas

RIVERBED AIRPCAP NX

Wi-Fi-verkon liikenteen seuranta AirPcap-ohjelmistolla

Opinnäytetyö
CENTRIA-AMMATTIKORKEAKOULU
Tieto- ja viestintätekniikan koulutus
Toukokuu 2023



TIIVISTELMÄ OPINNÄYTETYÖSTÄ

Centria-ammattikorkeakoulu	**Aika** Toukokuu 2023	**Tekijä/tekijät** Saku Hirsikangas
Koulutus Tieto- viestintätekniikka		☒ AMK ☐ YAMK
Työn nimi RIVERBED AIRPCAP NX. Wi-Fi-verkon liikenteen seuranta AirPcap-ohjelmistolla		
Työn ohjaaja Jari Isohanni		**Sivumäärä** 39
Työelämäohjaaja Tom Tuunainen		

Opinnäytetyön aiheena oli Wi-Fi-verkon liikenteen seuranta AirPcap-ohjelmistolla, työsisältää yleisesti asiaa langattomista verkoista, tietoliikenteestä ja sen seurannasta, lakitiedosta ja testauksista ja niistä syntyneistä johtopäätöksistä. Tämän opinnäytetyön tavoitteena oli oppia ymmärtämään, miten Aircap- ohjelmistoa voidaan hyödyntää osana tietoturvatestausta.

Opinnäytetyö käsittelee myös Aircrack-ng:n asennuksesta ja käyttöönotosta. Aircrack-ng on ohjelmistopaketti Wi-Fi-verkkojen analysointiin ja hakkerointiin. Aircrack-ng on valmiiksi asennettu Kali-käyttöjärjestelmään, jota käsitelllään myös tässä työssä.

Aircrack-ng-ohjelmistolla ja Riverbedin toimiessa langattomana verkkoadapterina pystytään seuraamaan langottomassa verkossa olevia laitteita ja access point:ja.

Asiasanat
Aircrack-Ng, IEEE 802.11, Kali, Riverbed AirPcap Nx, Wi-Fi, WLAN

ABSTRACT

Centria University of Applied Sciences	**Date** May 2023	**Author** Saku Hirsikangas
Degree programme Information and Communication Technology		
Name of thesis RIVERBED AIRPCAP NX. Wi-Fi network traffic monitoring with AirPcap software		
Centria supervisor Jari Isohanni		**Pages** 39
Instructor representing commissioning institution or company Tom Tuunainen		

The topic of the thesis was the monitoring of Wi-Fi network traffic with the AirPcap software, thesis contains general information about wireless networks, data traffic and its monitoring, legal information and testing, and the resulting conclusions. The goal of this thesis is to learn to understand how the Aircap software implements its planned communication monitoring.

Also thesis goes through installing and deploying of Aircrack-Ng. Aircrack-ng is a software package for analyzing and hacking Wi-Fi networks. Aircrack-ng is pre-installed on the Kali operating system, which I also will be using in this thesis.

With the Aircrack-ng software and Riverbed acting as a wireless network adapter, it is possible to monitor devices and access points in a wireless network.

Key words
Aircrack-Ng, IEEE 802.11, Kali, Riverbed AirPcap Nx, Wi-Fi, WLAN

KÄSITTEIDEN MÄÄRITTELY

A-MPDU

Aggregoidut MAC-protokolladatayksiköt (A-MPDU:t) yhdistävät useita kehyksiä yhdeksi lähetykseksi, jota seuraavat lohkokuittaukset.

A-MSDU

Aggregated MAC Service Data Unit (A-MSDU) kokoaa useita MSDU:ita yhdeksi kehyslähetykseksi.

BIOS

BIOS (lyhenne sanoista Basic Input-Output System) on tietokoneohjelma, joka etsii ja lataa käyttöjärjestelmän päämuistiin ja käynnistää sen, kun tietokone käynnistyy.

DFS

Tietojenkäsittelytieteessä deep-first search (DFS) on graafialgoritmi, joka etsii kaikkia muita solmuja, jotka ovat tavoitettavissa tietyn solmun kautta.

DNS-palvelin

DNS, Domain Name System, on Internetin nimipalvelujärjestelmä, joka tarjoaa tietokoneille IP-osoitteet, joista ne voivat löytää verkkosivustoja.

DSSS

Suorasekventointi (engl. Direct Sequence Spread Spectrum). FHSS:n lisäksi suorasekvenssihajaspektri on toinen tekniikka, jota käytetään CDMA:n toteuttamiseen.

ESS

ESS (Extended Service Set) on useiden tukiasemien luoma langaton verkko, joka näyttää käyttäjälle yhtenä, saumattomana verkkona, kuten koti- tai toimistoverkkona, joka on liian suuri tarjoamaan luotettavaa peittoa yhdestä tukiasemasta.

FHSS

Frequency Hopping Spread Spectrum on toinen tekniikka, jota käytetään CDMA:n toteuttamiseen DSSS:n lisäksi.

HT-tila

HT-tila määrittää tuetun tiedonsiirtonopeuden tai suoritustehotilan.

IEEE 802.11

IEEE 802.11 on IEEE-standardi langattomille WLAN-paikallisverkoille.

IP-osoite

IP-osoite ("Internet Protocol address" tai "Internet Protocol address") on numerosarja, jota käytetään IP-verkkoon kytketyn laitteen tunnistamiseen. MAC-osoitteita käytetään tunnistamaan verkkosovittimet verkon alemmalla tasolla.

ISA100-standardi

ISA100 on loppukäyttäjälähtöinen, teollisuusstandardeihin perustuva, verkkosuojattu, vankka langaton protokolla laitteiden, kuten lämpötilalähettimien, yhdistämiseen prosessinvalvonta- ja ohjausjärjestelmien ohjausjärjestelmiin.

ISM-alue

ISM Radio (ISM < Engl. industrial, science and medical) on joukko radiotaajuusalueita, jotka on varattu muiden elektronisten laitteiden (ISM-laitteiden) kuin todellisten radiolaitteiden käyttöön.

Kali-käyttöjärjestelmä

Kali Linux on Debian-pohjainen Linux-jakelu, joka on suunniteltu digitaaliseen rikostekniseen tutkimukseen ja penetraatiotestaukseen. Sitä ylläpitää ja rahoittaa Offensive Security.

MGWS-standardi

Multi-Gigabit Wireless System (MGWS) on Euroopan televiestintäinstituutin (ETSI) aloite määritellä järjestelmä langattomille lähiverkoille (WLAN) ja langattomille henkilökohtaisille verkoille (WPAN), joilla on erittäin korkea tiedonsiirtonopeus. gigabittiä sekunnissa.

MIMO

MIMO-tekniikka (Multiple-Input and Multiple-Output) viittaa viestintätekniikkaan, joka käyttää useita antenneja lähetykseen ja vastaanottoon samanaikaisesti.

MU-MIMO

Multi-User MIMO (MU-MIMO) on joukko usean tulon monilähtötekniikoita (MIMO) monitie-langattomaan viestintään, jossa useat käyttäjät tai päätelaitteet, joista kukin lähettää radiota yhden tai useamman antennin kautta, kommunikoivat keskenään.

OFDMA

OFDMA (Orthogonal Frequency Division Multiple Access) on Wi-Fi 6:n tekniikka, joka parantaa langattoman verkon suorituskykyä luomalla itsenäisesti moduloituja alikantoaaltoja taajuuksille. Tämä lähestymistapa mahdollistaa samanaikaiset siirrot useille asiakkaille ja useilta asiakkailta.

PDA-laitteet

PDA-laite tai lyhyesti Personal Digital Assistant on kädessä pidettävä elektroninen laite (mobiililaite), jota käytetään tietojen tallentamiseen ja järjestämiseen.

RC4

Salaustekniikassa RC4 (Rivest Cipher 4, joka tunnetaan myös nimellä ARC4 tai ARCFOUR, eli ns. RC4, katso alla) on stream-salaus. Vaikka se tunnetaan ohjelmiston yksinkertaisuudestaan ja nopeudestaan, RC4:stä löydettiin useita virheitä, jotka tekivät siitä epävarman.

RS-232

RS-232 (Recommended Standard 232) on vakiotietoliikenneväylä, jota käytetään kahden tietokonelaitteen väliseen tietoliikenteeseen.

SSID

SSID on lyhenne sanoista service set identifier, joka tarkoittaa langattoman lähiverkon toimialueen nimeä. Sen avulla voidaan eristää samalla alueella olevat WLAN-verkot toisistaan ja liittää ne haluttuun verkkoon.

TKIP

TKIP (Temporal Key Integrity Protocol) on langattoman lähiverkon suojausprotokolla, joka vanhentui Wi-Fi 802.11 -standardissa vuonna 2012.

TPC

Transmit Power Control eli lähetystehon ohjaus on tekninen mekanismi, jota käytetään joissakin verkkolaitteissa estämään liialliset tarpeettomat häiriöt eri langattomien verkkojen, kuten omistajaverkon ja naapuriverkon, välillä.

URL-osoite

URL-osoite on yksilöllinen osoite Internetissä oleville tiedoille, kuten verkkosivustolle tai verkkokaupalle. URL-osoite on johdettu sanasta Uniform Resource Identifier, mikä tarkoittaa, että se on yhtenäinen, konkreettinen merkkijono, joka kertoo tiedon sijainnin.

WEP

WEP (Wired Equivalent Privacy) on ensimmäinen IEEE 802.11 -standardin salausmenetelmä, joka suojaa työasemien ja tukiasemien välistä langatonta viestintää.

Wi-Fi

Wi-Fi tarkoittaa langatonta paikallisverkkoa, joka käyttää IEEE 802.11 -standardin mukaista tekniikkaa.

WiGig

WiGig, joka tunnetaan myös nimellä 60 GHz Wi-Fi, viittaa joukkoon 60 GHz:n langattomia verkkoprotokollia. Se sisältää nykyisen IEEE 802.11ad -standardin ja myös IEEE 802.11ay -standardin.

WLAN

WLAN (lyhenne sanoista wireless local area network), eli langaton lähiverkko, on paikallinen viestintäverkko, jossa Internetiin yhdistetty reititin toimii tukiasemana, eli luo mikroaaltokentän langattoman Internet-yhteyden aikaansaamiseksi.

WPA

WPA tai Wi-Fi Protected Access on WLAN-verkoissa käytetty salausprotokolla.

WPA2

WPA2 on uusin tietoturvastandardi langattomille 802.11-verkoille, jotka on suunniteltu vastaamaan tietoturvaongelmiin

WPA3

WPA3, joka tunnetaan myös nimellä Wi-Fi Protected Access 3, on kolmas versio Wi-Fi Alliancen kehittämästä suojaussertifiointiohjelmasta. WPA3 on WPA2:n viimeisin päivitetty toteutus, ja se on ollut käytössä vuodesta 2004. Wi-Fi Alliance aloitti WPA3-sertifioitujen tuotteiden sertifioinnin vuonna 2018.

WSN

Langattomalla anturiverkolla tarkoitetaan alueellisesti hajallaan olevien erillisten antureiden verkkoa, jotka valvovat ja tallentavat ympäristön fyysisiä olosuhteita ja välittävät kerätyt tiedot keskitettyyn paikkaan.

1 JOHDANTO

Tietoliikenne ei ole turvallista, ja sen takia on kehitetty tietoturvalaitteita ja ohjelmistoja seuraamaan tietoliikennettä. Niihin lukeutuu Riverbed AirPcap Nx-laitteisto/ohjelmisto. Tietoliikennettä voidaan seurata nykytekniikalla esimerkiksi eri viranomaisten, mutta myös rikollisten hyödyksi. Internetissä ja matkapuhelinverkoissa lähetettyjen viestien seurannalla on mahdollista tarkastaa paitsi niiden sisältö, myös niin sanotut metatiedot eli kuka lähetti viestin kenelle, minne viesti meni ja kenen kanssa olit. (Ervasti 2015.)

Tämän opinnäytetyön tavoitteena oli tutkia Riverbed Aircap Nx-laitteistostoa ja ohjelmistoa, joilla voidaan seurata langattoman verkon liikennettä. Tietoliikenteeseen liittyvä aihe oli mielessäni alusta asti ja tietoliikenteen seuranta Riverbedillä vaikutti hyvin mielenkiintoiselta. Tässä työssä käsitellään aiheita langattoman verkon rakenteista, 802.11-standardista, suojatusta ja suojattomasta tietoliikenteestä, tietoliikenteen seurannan lainsäädännästä ja Riverbed AirPcap Nx-laitteesta. Opinnäytetyöhön kuuluu myös käytännön testauksia ja niistä syntyvistä johtopäätöksistä. Lisäksi työ käsittelee Aircrack-ng:n asentamisesta ja käyttöönottoa. Aircrack-ng on ohjelmistopaketti Wi-Fi-verkkojen analysointiin ja murtamiseen. Aircrack-ng on esiasennettu Kali-käyttöjärjestelmään, jota käytän myös tässä opinnäytetyössä.

2 LANGATTOMAT VERKOT

Langallisten yhteyksien lisäksi on kehitetty laaja valikoima langattomia viestintäratkaisuja, ja langattomat vaihtoehdot kilpailevat jo monilla alueilla kiinteiden verkkojen kanssa. Tähän on monia syitä. Langaton yhteys on osoittautunut hyödylliseksi, kun nopeat laajakaistayhteydet tuodaan harvaan asutuille alueille. Langattomat lähiverkot yleistyvät työpaikalla ja kotona, koska langattomat laitteet tarjoavat eri vapausasteita laitteiden sijoittamisessa kuin perinteiset kierretyt parikaapelit. Langattomat verkot julkisilla paikoilla tarjoavat kannettavien tietokoneiden käyttäjille viestintäyhteyden ilman, että käyttäjän tarvitsee tietää verkkoarkkitehtuurista tai tukiasemien sijainnista. (Granlund 2007, 65.)

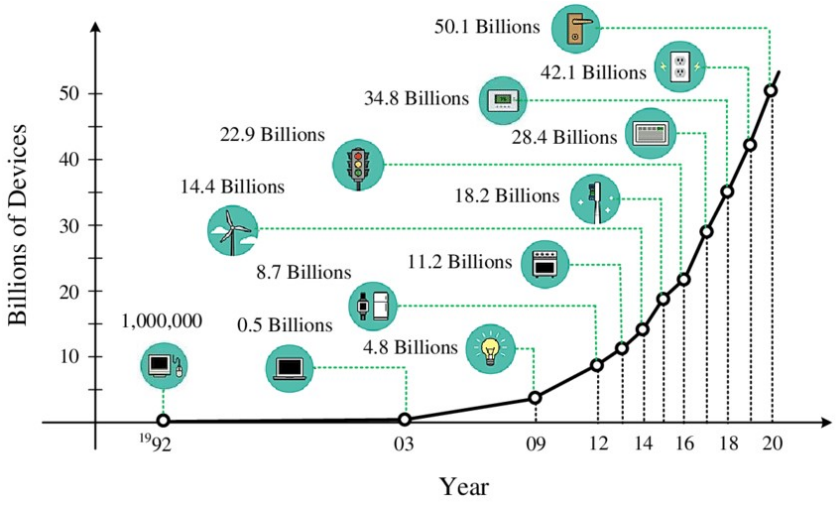
Wi-Fi on suosittu langaton verkkotekniikka. Wi-Fi tulee sanoista "Wireless Fidelity". NCR Corporation/AT&T keksi Wi-Fi:n vuonna 1991 Alankomaissa. Tämän tekniikan avulla tietoja voidaan vaihtaa kahden tai useamman laitteen välillä ilman kiinteää verkkoyhteyttä. Wi-Fi kehitettiin mobiililaitteisiin, vaikka kannettaviin tietokoneisiin ja nykyään käytetään laajalti myös mobiilisovelluksissa ja elektroniikassa, vaikka DVD-soittimissa, digitaalikameroissa ja televisioissa. Wi-Fi-yhteyden kanssa viestimiseen on kaksi vaihtoehtoa, joko asiakasyhteyden kautta tukiasemaan tai asiakas-asiakasyhteyden kautta. (Elprocus 2020.)

KUVA 1. Wi.Fi-tekniikka (Elprocus 2020)

Wi-Fi on IEEE 802.11 -standardisarjaan perustuva langattomien verkkoprotokollien perhe, jota käytetään yleisesti laitteiden lähiverkko- ja Internet-yhteyksissä. Niiden avulla lähellä olevat digitaaliset laitteet voivat vaihtaa tietoja radioaaltojen avulla. Nämä ovat maailman laajimmin käytetyt tietokonever-

kot, joita käytetään maailmanlaajuisesti koti- ja pientoimistoverkoissa, pöytätietokoneiden ja kannettavien tietokoneiden, tablettien, älypuhelimien, älytelevisioiden, tulostimien ja älykaiuttimien yhdistämiseen sekä langattomien reitittimien kautta. julkisissa paikoissa, kuten internetkahviloissa, hotelleissa, kirjastoissa ja lentokentillä, jotta vierailijoille voidaan tarjota Internet-yhteys mobiililaitteilla. (Garber 2014.)

Wi-Fi on Wi-Fi Alliancen tavaramerkki, joka rajoittaa termin "Wi-Fi Certified" käytön tuotteisiin, jotka ovat läpäisseet yhteen toimivuuden sertifiointitestin. Vuodesta 2017 lähtien toiminut Wi-Fi Alliance koostuu yli 800 yrityksestä maailmanlaajuisesti. Vuonna 2019 Wi-Fi-verkoissa toimi yli kolme miljardia laitetta. (Research and Markets 2020.)



KUVA 2. Wi-Fi laitteiden kasvu (ResearchGate)

Wi-Fi toteuttaa osan IEEE 802 -protokollaperheestä, joten se on suunniteltu toimimaan saumattomasti langallisen Ethernetin kanssa. Yhteensopivat laitteet voivat muodostaa yhteyden Internetiin langattoman tukiaseman kautta sekä verkkoon langallisten laitteiden ja Internetin kautta. Erilaiset IEEE 802.11 -protokollastandardit määrittelevät eri versiot Wi-Fi:stä ja eri radiotekniikat määrittelevät radiotaajuuden, maksimialueen ja saavutettavan nopeuden. Wi-Fi käyttää yleisimmin 2,4 GHz (120 mm) UHF- ja 5 GHz (60 mm) SHF-radiokaistaa; nämä kaistat on jaettu useisiin kanaviin. Kanavat voidaan jakaa verkkojen välillä, mutta vain yksi lähetin voi lähettää kanavalla kerrallaan tietyllä alueella. (Adi 2020.)

Wi-Fi-radiotaajuuksilla on suhteellisen korkea absorptionopeus, ja ne toimivat parhaiten näköyhteys-yhteyksissä. Monille verkoille esteet, kuten seinät, pilarit, laitteet jne., voivat vähentää merkittävästi kantamaa, mutta esteet voivat auttaa myös minimoimaan eri verkkojen välisiä häiriöitä ruuhkaisissa ympäristöissä. Tukiaseman kantama on noin 20 metriä (66 jalkaa) rakennuksien sisällä ja taas jotkut

väittävät kantaman jopa 150 metriin (490 jalkaa) ulkona. Hotspot-peittoalue voi olla pieni kuin huoneen seinät estävät radioaaltojen etenemisen tai jopa useita neliökilometrejä, kun käytetään useita päällekkäisiä tukiasemia ja sallitaan verkkovierailu niiden välillä. Ajan myötä Wi-Fin nopeus ja spektrinen tehokkuus on parantunut. Jotkin Wi-Fi-versiot voivat saavuttaa jopa 9,6 Gbit/s (gigabittiä sekunnissa) nopeuden lähietäisyydellä oikealla laitteistolla. (Adi 2020.)

2.1 Langattoman verkon rakenne

Langattomat verkot käyttävät samanlaisia komponentteja kuin langalliset verkot, mutta langattomien verkkojen on muutettava tietosignaalit muotoon, joka soveltuu lähetettäväksi ilmateitse. Vaikka langaton verkko on suoraan osa yleistä verkkoinfrastruktuuria, on kiinnitettävä huomiota kaikkiin verkon toimintoihin, jotta vältetään langattoman median aiheuttamat häiriöt. (Cisco Press 2004.)

Tietoverkon topologia, olipa se sitten langallinen tai langaton, kuvaa yleisesti tietoliikennelaitteiston rakennetta tai asettelua. Yksityiskohtaisesti se voi kuvata fyysistä ja loogista kartoitusta siitä, miten eri älylaitteet (jota kutsutaan usein solmuiksi) sijoitetaan ja kommunikoivat keskenään. Kiinteissä verkoissa topologia riippuu osittain solmujen sijainnista ja käytetyistä verkkokomponenteista. Langattoman verkon tapauksessa topologia voi olla useiden tekijöiden funktio, mukaan lukien langaton modulaatiotekniikka, verkkokomponenttien looginen luonne, maantieteellinen topologia ja solmujen välinen etäisyys sekä langattomien laitteiden tukemat protokollat. (McCurdy 2009.)

Langattoman teknologian varhainen käyttöönotto teollisissa sovelluksissa oli yksinkertaisia valvontasovelluksia, joissa johdot korvattiin langattomilla linkeillä. Näihin sovelluksiin liittyy usein riittävän suuri etäisyys reitittimestä, joten johdotus oli epäkäytännöllistä tai ei ainakaan kustannustehokasta. Sitä voidaan käyttää tarjoamaan suoria linkkejä sekä lyhyen että pitkän matkan yhteyksille, joissa näköyhteys on käytettävissä, ja välittämään dataa fyysisiä kuituoptisia linjoja vastaavilla nopeuksilla. Voidaan ajatella tämän langallisena vastineena 4–20 mA:n asetukseksi tai RS-232-liitäntäksi. Tässä esimerkissä kommunikoidaan yksittäisen kiinteän kenttälaitteen, kuten virtaus- tai tasolähettimen, ja ohjaus- tai valvontapaikan välillä. Tämä on yksinkertainen langaton toteutus, joka voidaan ottaa käyttöön erittäin nopeasti ja helposti teollisuusympäristössä ja joka voi tarjota merkittäviä kustannussäästöjä, kun otetaan huomioon kallis johdotus ja johdotuskustannukset joissakin teollisuusympäristöissä. (McCurdy 2009.)

Edistyneempien sovellusten, kuten SCADA:n helpottamiseksi käytetään usein langattomia point-to-multipoint- tai tähtikokoonpanoja. Tämän konfiguraation tyypillinen toteutus on tähtiklusteri, jossa langaton "tukiasema" tai "isäntä" on topologian keskellä ja liikenne ohjataan siihen etälaitteidein kyselyjen perusteella. Monet perinteiset SCADA-asennukset, jotka käyttävät langatonta tekniikkaa telemetriana kommunikoidakseen etäsivustojen kanssa, käyttävät tätä "isäntä/orja"-kokoonpanoa. Tätä toteutusta voidaan myös verrata RS-485-väyläverkon langalliseen asennukseen. Nykyaikaisemmat langattomat Ethernet-verkot, kuten teollisuusstandardi IEEE 802.11a/b/g, käyttävät myös tyypillisesti tähtitopologiaa, jossa "master"-verkkoa kutsutaan usein liityntäpisteeksi ja orjalaitteita kutsutaan asiakkaiksi. (McCurdy 2009.)

Toistimet sisällytetään usein langattomiin verkkoihin verkon peittoalueen laajentamiseksi alueille, joihin langattomat tekniikat eivät pääse yhdellä hypyllä tai joissa RF-polut voivat olla maantieteellisen topologian tai muiden fyysisten kohteiden tukkimia. (McCurdy 2009.)

Viimeisin topologia, josta usein keskustellaan teollisilla langattomilla markkinoilla, on mesh-verkko. Mesh-verkon realistisimmassa toteutuksessa jokainen solmu toimii sekä päätelaitteena että verkon edelleen lähetyslaitteena. Se mahdollistaa itsensä korjaamisen, jatkuvan liitettävyyden ja uudelleenkonfiguroinnin katkenneiden tai estettyjen polkujen ympärillä hyppäämällä solmusta solmuun, kunnes tiedot saavuttavat määrätyn määränpäänsä. Jos solmu katoaa teollista WLAN-tekniikkaa käyttävässä 802.11-verkossa, verkko "parantaa" itsensä uudelleenohjaamalla tietovirran katkenneilta poluilta suljetuille poluille. Kaikilla WLAN-tekniikoilla ei ole tätä mesh-ominaisuutta. (McCurdy 2009.)

2.2 802.11-standardi

Kaikki Wi-Fi-standardit kuuluvat IEEE 802 -sateenvarjon piiriin lähiverkoille ja suurkaupunkialueverkkoille LAN/MAN. Wi-Fi-standardit kuuluvat IEEE 802.11 -perheeseen. Kun ensimmäinen Wi-Fi-standardi julkaistiin vuonna 1997, siihen ei lisätty päätettä. Kuitenkin kun uusia muunnelmia julkaistiin, pääte lisättiin osoittamaan todellista varianttia. Kirjain on pieni. Erilaiset IEEE 802.11 -sateenvarjostandardit kattavat kaiken siirtotiestä yhteen toimivuuden edellyttämiin järjestelmäelementteihin, kuten tietoturvaan, hotspoteihin, palvelun laatuun, verkkovierailuihin ja muihin. (Electronics Notes 2023.)

IEEE 802.11 -standardi sisältää useita teknologisia edistysaskeleita, joita on kehitetty useiden vuosien aikana. Jokainen uusi edistys määritellään standardin muutoksella, joka tunnistetaan yksi- tai kaksikirjaimalla jälkiliitteellä "802.11". Alkuperäinen 802.11-standardi salli vain 2 Mbps:n nopeudet 2,4 GHz:n kaistalla. 802.11b lisää uusia koodausmenetelmiä nostaakseen suorituskyvyn 6 Mbps:iin. 802.11a lisää tuen 5 GHz:n kaistalle ja Orthogonal Frequency Division Multiplexing (OFDM) -koodausmallille, mikä nostaa suorituskyvyn 54 Mbps:iin. 802.11 g tuo OFDM:n 802.11a:sta 2,4 GHz:n taajuusalueelle. 802.11n lisää sarjan tehokkaita parannuksia, jotka lisäävät suorituskykyä noin 10-kertaisesti mahdollistaen 450 Mbps:n signalointinopeuden huippuluokan yritystukiasemille. (Pearson 2009.)

802.11 jakaa jokaisen taajuuskaistan eri tavalla kanaviin. Esimerkiksi taajuusalue 2,4000–2,4835 GHz on jaettu 13 kanavaan, jotka sijaitsevat 5 MHz:n välein. Kanavat 1, 6 ja 11 olivat alun perin ainoat ei-päällekkäiset kanavat, mutta uudemmassa 802.11g-standardissa on nyt neljä ei-päällekkäistä kanavaa - 1, 5, 9 ja 13. Lisensoimattomaan käyttöön käytettävissä olevan taajuuden määrä vaihtelee maittain, se on paljon suurempi 5 GHz:n kaistalla ja tukee tyypillisesti paljon enemmän kanavia kuin 2,4 GHz:n taajuus. (Pearson 2009.)

Kanavien saatavuus vaihtelee maittain ja voi muuttua. Japani sallii 14 kanavaa 2,4 GHz:n kaistalla, kun taas muut maat, kuten Espanja, sallivat aluksi vain kanavat 10 ja 11. Kanavat 1–13 ovat nyt sallittuja Euroopassa ja Aasiassa. Pohjois-Amerikassa ja joissakin Keski- ja Etelä-Amerikan maissa sallitaan vain kanavat 1–11. (Electronics Notes 2023.)

Langattomat 802.11-standardit voivat vaihdella nopeuden, lähetysalueen ja käytetyn taajuuden suhteen, mutta todellisen toteutuksen kannalta ne ovat samanlaisia. Kaikki standardit voivat käyttää joko infrastruktuuria tai ad hoc -verkkosuunnittelua, ja jokainen voi käyttää samoja suojausprotokollia.

- IEEE 802.11: Alkuperäisellä langattomalla 802.11-standardilla on itse asiassa kaksi muunnelmaa. Molemmat tarjoavat 1 tai 2 Mbps siirtonopeudet ja saman RF 2,4 GHz. Ero näiden kahden välillä on se, kuinka tiedot lähetetään RF-median kautta. Toinen käyttää FHSS:ää ja toinen DSSS:ää. Alkuperäinen 802.11-standardi oli liian hidas nykyaikaisiin verkkovaatimuksiin, eikä sitä enää käytetä.
- IEEE 802.11a: Nopeudessa 802.11a-standardi on paljon alkuperäistä 802.11-standardia edellä. 802.11a määrittää nopeudet 54 Mbps asti 5 GHz:n kaistalla, mutta yleisimmät tiedonsiirtonopeudet ovat 6 Mbps, 12 Mbps tai 24 Mbps. 802.11a ei ole yhteensopiva langattomien 802.11b- ja 802.11g-standardien kanssa
- IEEE 802.11b: 802.11b-standardin suurin tiedonsiirtonopeus on 11 Mbps. Nämä laitteet on kuitenkin suunniteltu taaksepäin yhteensopiviksi aikaisemman 802.11-standardin kanssa, joka tarjosi nopeudet 1, 2 ja 5,5 Mbps. 802.11b käyttää 2,4 GHz:n radiotaajuuskaistaa ja on yhteensopiva 802.11g:n kanssa.
- IEEE 802.11e: Yksi avainalueista tiedon lähettämisessä minkä tahansa välineen kautta on palvelun laatu tai QoS ja tiedon priorisointi. IEEE 802.11e käsittelee tätä aihetta, joten voidaan valita määritetty menetelmä.
- IEEE 802.11f: IEEE 802.11f on ehdotus, joka kuvaa valinnaisia IEEE 802.11 -laajennuksia, jotka mahdollistavat langattoman tukiasemaviestinnän useiden valmistajien järjestelmien välillä. IEEE 802.11F:llä oli ongelmia sen käytössä, mutta sitä ei otettu käyttöön kaikkialla alalla, joten se poistettiin vuonna 2006.
- IEEE 802.11g: 802.11g on nykyään suosituin langaton standardi. 802.11g tarjoaa langattoman tiedonsiirtoetäisyyden 150 jalkaa ja nopeudet jopa 54 Mbps, kun 802.11b:n 11 Mbps. Kuten 802.11b, 802.11g toimii 2,4 GHz:n kaistalla ja on siksi yhteensopiva sen kanssa.
- IEEE 802.11h: IEEE 802.11h-2003 -spesifikaatio määrittelee Wi-Fi-yhteyden edellyttämän tehonsäädön. Se ohjaa spektrin ja lähetystehon hallinnan leviämiä ja käsittelee ongelmia, mukaan lukien mahdolliset häiriöt satelliiteille ja tutkaille, jotka myös käyttävät 5 GHz ISM-kaistaa. Standardi sisälsi alun perin Dynamic Frequency Selection (DFS) ja Transmit Power Control (TPC) 802.11a PHY:lle, mutta se on myös integroitu yleiseen IEEE 802.11-2007 -standardiin.

- IEEE 802.11i: Tietoturva on suuri huolenaihe Wi-Fi:lle, ja koska monet Wi-Fi-hotspotit sijaitsevat julkisilla alueilla, hakkerit voivat saada ei-toivotun pääsyn hotspotteja käyttävien ihmisten laitteisiin. IEEE 802.11i -standardia käytetään mahdollistamaan turvallinen päästä päähän -viestintä langattomissa lähiverkoissa. IEEE 80211i -standardi parantaa langattoman todennuksen, salauksen, avaintenhallinnan ja yksityiskohtaisen suojauksen mekanismeja.
- IEEE 802.11j: IEEE 802.11j-2004 on perusstandardin muunnos, joka laajentaa langattoman viestinnän ja signaloinnin japanilaisille 4,9 GHz:n ja 5 GHz:n taajuuskaistoille.
- IEEE 802.11k: IEEE 802.11 -standardi laajentaa RRM (Radio Resource Measurement) -mekanismin langattomiin lähiverkkoihin. Siinä on joitain ehdotuksia WLAN-suorituskyvyn optimoimiseksi.
- IEEE 802.11n: Uusin Network+ Objectives -kohdassa lueteltu langaton standardi on 802.11n. 802.11n-standardin tavoitteena on parantaa merkittävästi suorituskykyä 2,4 GHz ja 5 GHz taajuusalueella. Standardin perustavoitteena on saavuttaa 100 Mbps:n nopeus, mutta oikeissa olosuhteissa 802.11n:n arvioidaan pystyvän jopa huikeisiin 600 Mbps:n nopeuksiin. Todellisuudessa 802.11n on paljon hitaampi.
- IEEE 802.11s: Tämä IEEE 802.11 -standardin muutos käsittelee mesh-verkkojen aihetta. Siinä kerrotaan, kuinka Wi-Fi-laitteet muodostavat yhteyden toisiinsa WLAN-verkkojen luomiseksi, joita voidaan käyttää suhteellisen kiinteissä - ei-mobiilitopologioissa ja langattomissa ad hoc -verkoissa.
- IEEE 802.11u: IEEE 802.11u-2011 on muutos IEEE 802.11-2007 -standardiin. Se lisää toimintoja yhteistyöhön ulkoisten verkkojen kanssa. Sitä käytetään verkkovierailuihin ja myös Hotspot2.0-suunnitelmaan.
- IEEE 802.11ac: IEEE 802.11ac oli suuri harppaus suorituskyvyssä, kun se esiteltiin. Standardi julkaistiin vuonna 2013, ja vaikka monilla yrityksillä oli visio standardin julkaisun jälkeen, kesti jonkin aikaa, ennen kuin tuotteet nähtiin ja niitä käytettiin laajasti sen julkaisun jälkeen. Standardi määrittelee Wi-Fi:n "langattoman verkon siirtotien", joka toimii alle 6 GHz:n taajuuksilla ja tarjoaa vähintään 1 Gbps:n tiedonsiirtonopeuden moniasemakäytössä ja vähintään 500 Mbps yhden linkin kautta. Ominaisuuksiensa ja suorituskyvyn vuoksi Wi-Fi Alliance on antanut standardille nimen Wi-Fi 5.
- IEEE 802.11ad: 802.11ad, joka tunnetaan myös nimellä WiGi tai Gigabit Wi-Fi, on suunniteltu tarjoamaan erittäin korkea tiedonsiirtonopeus ja käyttää näin valtavan kaistanleveyden millimetriaaltokaistoja. Se määritellään Multi-Gigabit Wireless System (MGWS) -standardiksi, joka toimii jopa 60 GHz:n taajuuksilla - WiGig-verkkojen verkkostandardina. Erittäin korkeiden

taajuuksien käytön vuoksi etäisyys on hyvin rajallinen - tyypillisesti vain muutaman metrin, ja esineet, kuten seinät, vaimentavat sitä voimakkaasti, jolloin matalataajuiset signaalit pääsevät läpi.

- IEEE 802.11af: Alueilla, joilla TV-lähettimet tarvitsevat puskurivyöhykkeen, on usein paljon ns. valkoista tilaa, jotta samaa taajuutta käyttävät lähettimet eivät häiritse toisiaan. Näillä alueilla, joilla on vapaata tilaa, pienitehoisia signaaleja voidaan käyttää moniin muihin palveluihin, koska niiden tehotasot tarkoittavat, että ne eivät kulje kovin kauas eivätkä aiheuta häiriöitä ensisijaisille käyttäjille. Yksi tämän tyhjän tilan käyttötarkoitus on Wi-Fi, ja IEEE 802.11af on määritetty toimimaan näillä alueilla. Sitä kutsutaan usein valkoiseksi, koska sitä käytetään ja kuinka usein sitä käytetään.
- IEEE 802.11ah: Vaikka 2,4 ja 5 GHz:n taajuuksia käytetään yleisimmin Wi-Fi-yhteyksiin, on myös joitain alle 1 GHz:n ISM-varauksia. IEEE 802.11ah on suunniteltu käyttämään alle 1 GHz:n lisensoimattomia taajuuksia. Yksi etu on se, että se voi tarjota pitkän matkan viestintää ja siten tukea kaikkea Internetissä. Näiden taajuuskaistojen haittapuoli on, että ne ovat suhteellisen kapeita, mikä voi rajoittaa tiedonsiirtonopeuksia.
- IEEE 802.11ax: 802.11ax:a pidetään 802.11ac:n tulevana seuraajana. Käyttämällä tekniikoita, kuten OFDMA, MU-MIMO jne., se pyrkii lisäämään spektritehokkuutta ja siten parantamaan yleistä käytettävyyttä.

Edellä mainittujen standardien lisäksi IEEE ja sen työryhmät työskentelevät kovasti kehittääkseen uusia Wi-Fi-standardeja. Nämä varmistavat, että tekniikka kehittyy alan vaatimusten mukaisesti ja varmistaa, että IEEE 802.11 Wi-Fi vastaa tuleviin tarpeisiin. Vaikka verkkoliikennestandardit, kuten IEEE 802.11 g, 802.11n ja IEEE 802.11ac, ovat ehkä tunnetuimpia, ne kaikki sisältävät 802.11:n taustalla olevan yhteisen teknologian. Kuten yllä olevasta luettelosta nähdään, on olemassa useita 802.11-standardeja, jotka käsittelevät yleisiä teemoja kaikille Wi-Fi-järjestelmille. Turvallisuus, palvelun laatu, todennus jne. ovat kaikki tärkeitä ja vaativat vankan ympäristön Wi-Fi-tekniikan kehittämiselle ja käytölle. (Electronics Notes 2023.)

802.11n lupaa saada aikaan seuraavan suuren kehityksen langattomassa verkkotoiminnassa, lupaamalla pidemmän kantaman ja räjähtävän nopeita nopeuksia. 802.11n ottaa 802.11-standardin parhaat puolet ja sisältää uusia ominaisuuksia, jotka vievät langattoman verkon uudelle tasolle. Ensimmäinen näistä uusista teknologioista on MIMO-antennitekniikka. (Pearson 2009.)

MIMO on luultavasti avain suurimpaan 802.11n-kehitykseen ja uusiin nopeuksiin. Pohjimmiltaan MIMO käyttää multipleksointia lisäämään langattomien verkkojen kantamaa ja nopeutta. Multipleksointi on tekniikka, jossa yhdistetään useita signaaleja lähetettäväksi yhden johdon tai välineen kautta. MIMO voi lähettää samanaikaisesti useita datavirtoja, jotka lähetetään eri antenneilla samalla kanavalla. Vastaanotin rekonstruoi virran myös useilla antenneilla. Useita polkuja käyttämällä MIMO lisää merkittävästi kapasiteettia sekä luotettavampaa tiedonsiirtoa perinteisiin yksiantennisiin järjestelmiin verrattuna. (Pearson 2009.)

3 TIETOLIIKENNE LANGATTOMISSA VERKOISSA

Langaton viestintä on ollut osa ihmisten elämää esihistoriallisista ajoista lähtien savumerkkien, lippujen ja vilkkuvien peilien avulla, ja se kehittyy edelleen. Nykyaikainen langaton viestintä, joka käyttää viestimiseen sähköisiä signaaleja ja radioaaltoja, on ollut käytössä yli 100 vuotta. Vuonna 1897 Guglielmo Marconi esitteli menestyksekkäästi langatonta lennätystä lähettämällä sähkömagneettisia aaltoja lyhyelle, 100 metrin etäisyydelle. Tämä johdanto tasoitti tietä radioviestinnöille, jonka sana on johdettu säteilyenergiasta. (Teja 2021.)

1900-luvun alkuun mennessä transatlanttinen radiolähetys oli perustettu, ja Marconi käytti Morse-koodia viestien välittämiseen. Sen jälkeen langattomaan viestintään ja langattomiin järjestelmiin liittyvät teknologiat ovat kehittyneet nopeasti, mikä on mahdollistanut edullisen pitkän matkan lähetyksen halvemmilla laitteilla. Toinen skenaario, jossa langaton viestintä korvataan langallisella viestinnällä, on televisiolähetys. Alkuaikoina televisiosignaalit lähetettiin radiolähettimien avulla. Tämä asetus on korvattu kaapelitelevisiolla. Nämä kaksi esimerkkiä osoittavat, että tekniikan kehittyessä meidän on aina valittava parhaiten sopiva tilanne, eli joillain alueilla on käytettävä langallista viestintää, kun taas toisilla alueilla siirtyminen langattomaan palveluun voi olla parempi valinta. (Teja 2021.)

Miksi tarvitaan langatonta viestintää, kun langallinen viestintä voi tehdä suurimman osan siitä, mitä langaton viestintä voi? Langattoman viestinnän tärkein ja tärkeä etu on liikkuvuus. Liikkuvuuden lisäksi langaton viestintä tarjoaa joustavuutta ja helppokäyttöisyyttä, mikä tekee siitä yhä suositumpaa. Kuten matkapuhelinviestintä, langaton viestintä voidaan tehdä milloin tahansa, missä tahansa ja erittäin korkealla suorituskyvyllä. (Teja 2021.)

Toinen tärkeä asia on infrastruktuuri. Kiinteän tietoliikennejärjestelmän infrastruktuurin asentaminen ja asentaminen on kallista ja aikaa vievää työtä. Langaton viestintäinfrastruktuuri voidaan asentaa helposti ja edullisesti. Langaton tiedonsiirto on varteenotettava vaihtoehto hätätilanteissa ja syrjäisissä paikoissa, joissa langallisen tiedonsiirron käyttöönotto on vaikeaa. (Teja 2021.)

3.1 Suojattu liikenne

Tietokoneet ja monet muut laitteet, mukaan lukien älypuhelimet ja PDA-laitteet, voivat muodostaa yhteyden Internetiin langattomasti Wi-Fi-yhteyden avulla. Suojaamaton Wi-Fi-yhteys helpottaa hakkereiden pääsyä yksityisiin tiedostoihin ja tietoihin, ja muukalaiset voivat päästä käyttämään henkilön Internet-yhteyttä (ICO 2023.)

Langaton tietoturva on tärkeä osa turvassa pysymistä verkossa. Internet-yhteyden muodostaminen suojaamattoman linkin tai verkon kautta on turvallisuusriski, joka voi johtaa tietojen katoamiseen, tilitietojen vaarantumiseen ja haittaohjelmien asentumiseen verkkoosi. Oikeiden Wi-Fi-suojaustoimenpiteiden käyttäminen on tärkeää, mutta sitä tehdessä on myös tärkeää ymmärtää erot eri langattomien salausstandardien, mukaan lukien WEP, WPA, WPA2 ja WPA3, välillä. (Kaspersky 2021.)

Wi-Fi Protected Access (WPA) on tietoturvastandardi tietokoneille, joissa on langaton Internet-yhteys. Sen on kehittänyt Wi-Fi Alliance tarjoamaan parempi tietojen salaus ja käyttäjän todennus kuin Wired Equivalent Privacy (WEP), alkuperäinen Wi-Fi-suojausstandardi. 1990-luvun lopulta lähtien Wi-Fi-suojaustyyppejä on kehitetty useita parannuksia varten. (Kaspersky 2021.)

Koska langattomat verkot lähettävät dataa radioaaltojen kautta, tiedot voidaan siepata helposti, ellei turvatoimiin ryhdytä. Wired Equivalent Privacy (WEP), joka esiteltiin vuonna 1997, oli ensimmäinen yritys langattomaan suojaukseen. Tavoitteena on lisätä langattomien verkkojen turvallisuutta salaamalla tietoja. Jos langatonta dataa siepataan, sieppaaja ei tunnista sitä, koska se on salattu. Verkon valtuutetut järjestelmät voivat kuitenkin tunnistaa tiedot ja purkaa sen salauksen. Tämän takia verkossasi olevat laitteet käyttävät samaa salausalgoritmia. (Kaspersky 2021.)

WEP salaa liikenteen 64- tai 128-bittisellä heksadesimaaliavaimella. Tämä on staattinen avain, joka osoittaa kaiken liikenteen laitteesta riippumatta salataan yhdellä avaimella. WEP-avaimen avulla verkossa olevat tietokoneet voivat vaihtaa koodattuja viestejä samalla kun ne piilottavat viestien sisällön tunkeilijoilta. Tätä avainta käytetään yhteyden muodostamiseen langattoman suojauksen yhteenso-pivaan verkkoon. (Kaspersky 2021.)

Yksi WEP:n päätavoitteista oli estää Man-in-the-Middle-hyökkäykset, mitä se teki jonkin aikaa. Protokollan tarkistuksista ja avaimen kasvamisesta huolimatta WEP-standardissa havaittiin ajan mittaan erilaisia tietoturvapuutteita. Kun laskentateho kasvoi, rikollisten oli helpompi hyödyntää näitä puutteita. Haavoittuvuuksiensa vuoksi Wi-Fi Alliance lopetti virallisesti WEP:n vuonna 2004. Nykyään WEP-suojausta pidetään vanhentuneena, vaikka se on edelleen joskus käytössä – joko siksi, että verkonvalvojat eivät ole muuttaneet langattomien reitittimien oletussuojausta tai koska laitteet ovat liian vanhoja tukemaan uusia salausmenetelmiä, kuten WPA. (Kaspersky 2021.)

Seuraavaksi on WPA tai Wi-Fi Protected Access. Tämä protokolla otettiin käyttöön vuonna 2003, ja se korvasi Wi-Fi Alliancen WEP:n. Samanlainen kuin WEP, mutta parannettu suojausavainten käsittely ja käyttäjän todennus. WEP tarjoaa saman avaimen jokaiselle valtuutetulle järjestelmälle, kun taas WPA käyttää Temporal Key Integrity Protocol (TKIP) -protokollaa muuttaakseen dynaamisesti järjestelmän käyttämää avainta. Tämä estää tunkeilijoita luomasta omia salausavaimiaan, jotka vastaavat suojatun verkon käyttämiä salausavaimia. TKIP-salausstandardi korvattiin myöhemmin Advanced Encryption Standardilla (AES). (Kaspersky 2021.)

Kodin Wi-Fi-verkot luodaan ja niihin päästään yleensä fyysisen laitteen kautta, jota kutsutaan laajakaistareitittimeksi, joka tunnetaan myös keskittimenä tai langattomana reitittimenä. On muodostettava yhteys reitittimeen tarkistettava sen suojausasetukset, joita on useita. Tärkeimmät näistä asetuksista ovat järjestelmänvalvojan salasana, langaton suojausavain ja salausmenetelmä. (ICO 2023.)

Helpoin tapa tarkistaa suojaus on, kun muodostetaan yhteys langattomaan verkkoon mistä tahansa laitteesta ensimmäistä kertaa, pyydetään antamaan langaton suojausavain. Jos ei ole vaihdettu sitä aiemmin, löydät sen yleensä jostain langattomasta reitittimestä, kuten alustasta. Jos henkilöltä ei kysytä salasanaa, kun yhdistetään laitteen ensimmäisen kerran, langaton verkko ei ole suojattu. Jos henkilön on syötettävä salasana, laitteen ja langattoman reitittimen välinen viestintä salataan. Langaton reititin ei kuitenkaan välttämättä käytä vahvinta saatavilla olevaa salausmenetelmää. (ICO 2023.)

Edistyneempi menetelmä edellyttää, että tiedetään langattoman reitittimen IP-osoitteen sekä järjestelmänvalvojan käyttäjänimen ja salasanan. Avaa selain ja kirjoita reitittimen IP-osoite (kuten 192.168.1.10 tai 192.168.1.251) osoitepalkkiin. Saatetaan joutua katsomaan lisätietoja omistajan käsikirjasta. Voidaan käyttää reitittimesi asetuksia selvittämäksi, onko yhteys jo suojattu, ja valita turvallisemman salasanan. Voidaan myös vaihtaa järjestelmänvalvojan salasanan. (ICO 2023.)

Service Set Identifier (SSID) on nimi, jota käytetään verkon tunnistamiseen. Pitää vaihtaa verkon nimi reitittimesi oletusarvosta. Tämä voi vaikeuttaa reitittimen valmistajan tunnistamista ja sen oletusasetusten arvaamista. Yksityisyyssyistä saatetaan haluta myös välttää nimiä, jotka tunnistavat ihmiset tai heidän talonsa (kuten sukunimi tai taloon liittyvä nimi) – käytetään sen sijaan jotain satunnaisempaa. Useimpien nykyaikaisten laitteiden avulla voit piilottaa SSID-tunnus satunnaisilta tarkkailijoilta, mutta tätä ei pidä pitää turvatoimena, koska monet vapaasti saatavilla olevat työkalut voivat silti löytää tällä tavalla piilotettuja verkkoja. (ICO 2023.)

Salaus salaa langattoman verkon kautta lähetetyt viestit, jotta niitä ei voi lukea helposti. Jos verkko ei ole salattu, otetaan salaus käyttöön langattoman reitittimen langattoman verkon suojausasetusten sivulla. Salausta on monessa muodossa, mutta suositellaan Wi-Fi Protected Access II:ta (WPA2), koska vanhemmissa muodoissa, kuten WEP ja WPA ovat tunnettuja puutteita eivätkä ne tarjoa riittävää suojaa. Tämä on parempi vaihtoehto, jos henkilöllä on langaton tukiasema, joka voi hyödyntää WPA3:a, mutta se on tällä hetkellä hyvin uusi protokolla, joten laitetuki on rajoitettu. Joissakin laitteissa käytössä oleva salausmenetelmä näkyy langattoman verkon nimen vieressä, kun yritetään muodostaa yhteyden. (ICO 2023.)

3.2 Suojaamaton liikenne

Henkilökohtaisten tietojen varastamisen riski on suurempi, jos käytetään avointa ja suojaamatonta langatonta verkkoa. Kun henkilökohtaisia tietoja siirretään tietokoneeseen ja suojaamattoman langattoman reitittimen välillä, teknisiä perustaitoja omaava henkilö voi helposti siepata ne. Nämä tiedot voivat olla yhtä vaarattomia kuin vierailtujen verkkosivustojen historia ja tärkeämpiä tietoja, kuten käyttäjänimet ja salasanat. Suojaamaton langaton verkko helpottaa myös muiden pääsyä sähköpostiin, luottamuksellisiin työtiedostoihin tai muualle tietokoneelle. (Spam Laws 2023.)

Joskus kyberhyökkääjät pääsevät suojaamattomien langattomien Internet-verkkojen reitittimiin arvaamalla oletusasetukset. Kun hyökkääjällä on nämä asetukset, hän voi esiintyä DNS-palvelimena ja ohjata uhrin, verkkosivustoille, jotka näyttävät samanlaisilta kuin ne, joilla henkilö vierailee usein. Syötetään käyttäjätunnukset ja salasana, ja hyökkääjällä on välittömästi tiedot, joita he tarvitsevat päästäkseen pankki, PayPaliin tai online-sähköpostiosoitteeseen. Hän käyttää näitä tietoja varastaakseen henkilöltä rahaa tai lähettääkseen viestejä hänen perheellensä ja ystäville pyytääkseen rahaa tai muuta sopimatonta tietoa. (Spam Laws 2023.)

Suojaamattomia verkkoja on helpompi käyttää, mikä tarkoittaa, että henkilö on kaikkien armoilla, jotka haluavat käyttää niitä laittomaan tai rikolliseen toimintaan. Jos verkkohyökkääjät käyttävät verkkoa häiritäkseen ihmisiä, varastaakseen heidän tietojaan tai jopa murtautuakseen turvaluokiteltuihin valtion asiakirjoihin, verkon omistajana voidaan haastaa oikeuteen, vaikka henkilö ei tietäisi, että hänen verkkoansa käytetään näistä syistä. (Spam Laws 2023.)

Tietojenkalastelupakettien avulla hakkerit voivat luoda kopioita laillisista kirjautumissivuista ja huijata antamaan hakkereille käyttäjätunnukset ja salasanat ja joskus jopa luottokorttitiedot. Näiden sovellusten avulla lähellä istuva hakkeri voi huijata henkilön luulemaan, että hän on kirjautumassa lailliselle sivustolle (esimerkiksi hotspotille tai suosittuun online-sähköpostiin, sosiaaliseen mediaan, ostoksille tai syötä käyttäjätunnuksesi ja salasanasi uudelleen väärennettyyn portaaliin. (Cogipas 2019.)

Hakkerit ja nuuskijat käyttävät muita työkaluja, joita kutsutaan haistajiksi, tietojen keräämiseen suojaamattomien verkkojen kautta. Kun käytetään suojaamatonta Wi-Fi-yhteyttä, nämä huijarit voivat kaapata kaiken yhteyden kautta lähettämän liikenteen, mukaan lukien sähköpostin ja salasanan sekä kaikki muut lähettämät tiedot, kuten luottokorttitiedot. Tämä on yksi syistä, miksi henkilön ei pitäisi

koskaan käydä pankissa, tehdä ostoksia verkossa tai käydä verkkosivustoilla, jotka edellyttävät hänen käyttäjänimensä/salasanan suojaamattoman julkisen Wi-Fin kautta. (Cogipas 2019.)

Suojaamattomat Wi-Fi-verkot ovat nimensä mukaisesti Wi-Fi-verkkoja, joihin voidaan muodostaa yhteys ja joista puuttuu suojaus. Toisaalta suojatut verkot vaativat käyttäjiä kirjautumaan sisään sähköpostilla, hyväksymään lailliset ehdot, antamaan salasanan tai rekisteröimään tilin palveluntarjoajalle. Yritykset käyttävät usein erilaisia tietoturvatekniikoita ja -tekniikoita suojatakseen Wi-Fi-verkkojaan. Näitä ovat palomuureilla varustetut reitittimet, mukaan lukien esiohjelmoidut suojausominaisuudet, virustorjuntaohjelmistot sekä julkiset ja yksityiset kulunvalvontamenetelmät. On syytä huomata, että yhteyden muodostaminen suojaamattomaan Wi-Fi-verkkoon on kätevämpää. Käyttäjien tulee kuitenkin olla tietoisia siitä, että osa tiedoista saattaa paljastua näitä verkkoja käytettäessä. (Dr. Chaos 2022.)

Kun Wi-Fi-verkko ei ole suojattu, se voi johtaa useisiin haavoittuvuuksiin, joita hakkerit voivat hyödyntää.

Alla on joitain yleisimmistä riskeistä ja haavoittuvuuksista, jotka liittyvät sellaisten Wi-Fi-verkkojen käyttöön, joista puuttuu perusturvaominaisuudet:

- Piggybacking: Kun hakkeri voi käyttää internetyhteyttäsi, vaikka he olisivat jopa 150–300 metrin päässä. Tämä voi avata verkkosi tahattomille käyttäjille.

- Pahat kaksoishyökkäykset: Haitalliset toimijat luovat toisen verkon, jonka tarkoitus on esiintyä verkkonasi, ja kun ihmiset muodostavat yhteyden tähän väärään verkkoon, he voivat varastaa käyttäjätietoja.

- Luvaton käyttö: Hakkerit voivat päästä käsiksi tiedostoihin, jotka olet vahingossa asettanut verkkoosi yhdistävien saataville.

- Wardriving: Erityinen toimintamalli, jossa hakkerit ajavat kaupunkien läpi Wi-Fi-yhteensopivalla laitteella etsiäkseen suojaamattomia verkkoja.

- Langaton haistelu: Hakkerit käyttävät haistelutyökaluja arkaluontoisten tietojen, kuten käyttäjänimien, salasanojen ja luottokorttien numeroiden, paikantamiseen.

- ”Olkapäiden” nuuskiminen: Tämä on yksinkertainen mutta vaarallinen ongelma – hakkerit vakoilevat olkapääsi yli julkisilla alueilla varastaakseen henkilökohtaisia tai tunnistettavia tietoja.

Kaikki nämä mahdolliset ongelmat, kuten kyberhyökkäykset tai tietoturvaloukkaukset, ovat joitakin riskejä, joihin voit avata itsesi, jos et suojaa langatonta verkkoasi. (Dr. Chaos 2022.)

4 VERKKOLIIKENTEEN SEURANTA

Verkkoliikenteen valvonta on tietoverkon toimintojen seurantaa ja analysointia. Valvonta kertoo kuorman, ja analytiikka pyrkii saamaan tarkempaa tietoa liikenteen laadusta. (Noction, 2018.)

Koko verkkoliikenteen seurantaan on useita päteviä syitä. Verkkoliikenteen seurantatyökalujen tuottamaa tietoa voidaan käyttää lukuisissa IT- ja tietoturvakäyttötapauksissa. Esimerkiksi tutkitaan tietoturvaloukkauksia ja tehdään verkkoon liittyvien ongelmien vianmääritys ja analysoidaan uusien sovellusten vaikutusta koko verkkoon. Tärkeä huomautus tässä suhteessa on, että kaikki verkkoliikenteen seurantatyökalut eivät ole samanarvoisia. Yleensä ne voidaan jakaa kahteen laajaan luokkaan, syväpakettien tarkistustyökalut ja virtauspohjaiset työkalut. Kahden tyypin joukosta voit valita työkaluja, jotka eivät vaadi ohjelmistoagentteja, työkaluja. Lisäksi niiden tulisi myös tallentaa historiallisia tietoja ja työkaluja tunkeutumisen havaitsemisjärjestelmille, jotka valvovat verkkoliikennettä verkon sisällä ja verkon reunalla. (Gupta 2022.)

4.1 Lainsäädäntä

Telealan ammattilaisten ja käyttäjien on hyvä tietää, mitä verkossa voi tehdä ja mitä ei. Suomen laki asettaa selkeät rajat suomalaisille toimijoille. Voit aina tarkistaa voimassa olevan kotimaan lainsäädännön finlex.fi-palvelusta. Toimialalla on myös TIVIA:n laatima ja julkaisema eettinen säännöstö, jota kaikkien alan ammattilaisten on noudatettava. Nämä ohjeet ovat hyvin lyhyitä, ja kaikkien tulee lukea ja ymmärtää ne. (MOOC 2021.)

Televiestintään liittyviä lakeja on useita, mutta ehkä tärkein niistä on suhteellisen uusi laki sähköisistä viestintäpalveluista. Se kulkee erilaisten sähköisten palveluntarjoajien oikeuksien ja velvollisuuksien kautta. Esimerkiksi entisen Viestintäviraston (nykyinen TrafiCom) oikeus hallita .fi- ja .ax-osoitteita perustuu tähän lakiin. (MOOC 2021.)

On olemassa useita erilaisia analyysiohjelmia, joilla voidaan valvoa viestintää ja niiden protokollien toimintaa. Niitä voidaan käyttää datapakettien ja niiden sisällön seuraamiseen niiden liikkuessa tietoliikenneverkoissa. Tämäntyyppinen verkkoliikenteen seuranta ei ole laillista kaikissa tapauksissa, joten ei kannata kokeilla sitä kaikkialla. Rikosvastuu ja -vastuu on aina liikennettä seuraavilla, joten pitää

ymmärtää verkon käytön säännöt ennen liikenteen seurantaa. Esimerkiksi liikenteen seuranta tehdään tallentamalla verkkoliikenne myöhempää analysointia varten. Tätä varten käytetään usein termiä pakettien sieppaus. Sekä hyvät että pahat tekevät tällaista toimintaa. Se, mihin ryhmään liikenneanalyytikko kulloinkin kuuluu, riippuu näkökulmasta. Verkon ylläpitäjillä on oikeus valvoa verkkoliikennettä, jos käyttösäännöt sen sallivat. (MOOC 2021.)

Laki määrittelee myös menetelmät, joita tutkinnassa voidaan käyttää. Siviilitiedustelua voi Suomessa tehdä ainoastaan suojelupoliisi. Suojelupoliisin tärkein tehtävä on tiedustelu. Toisin kuin muut poliisit, rikosten ehkäisemiseen tarkoitettujen tietojen saanti ei ole poliisin suojelemisen prioriteetti. Vakavien rikosten esitutkinnasta vastaa Keskusrikospoliisi yhteistyössä Suojelupoliisin kanssa. (SUPO)

1. terrorismi
2. ulkomainen tiedustelutoiminta
3. joukkotuhoaseiden suunnittelu, valmistaminen, levittäminen ja käyttö
4. kaksikäyttötuotteiden suunnittelu, valmistaminen, levittäminen ja käyttö
5. kansanvaltaista yhteiskuntajärjestystä vakavasti uhkaava toiminta
6. suuren ihmismäärän henkeä tai terveyttä taikka yhteiskunnan elintärkeitä toimintoja uhkaava toiminta
7. vieraan valtion toiminta, joka voi aiheuttaa vahinkoa Suomen kansainvälisille suhteille tai taloudellisille tai muille tärkeille eduille
8. kansainvälistä rauhaa ja turvallisuutta uhkaava kriisi
9. kansainvälisten kriisinhallintaoperaatioiden turvallisuutta uhkaava toiminta
10. Suomen kansainvälisen avun antamisen ja muun kansainvälisen toiminnan turvallisuutta vakavasti uhkaava toiminta
11. kansanvaltaista yhteiskuntajärjestystä uhkaava kansainvälinen järjestäytynyt rikollisuus (SUPO)

Tiedustelulaki tuli voimaan kesäkuussa 2019. Sen avulla Valtion turvallisuuspoliisilla on oikeus saada tietoa tietoverkoissa tapahtuvasta tietoliikenteestä Suomen rajan yli. Se tarkoittaa teknistä tiedonkeruuta, joka perustuu tietoliikenteen automaattiseen erottamiseen ja hankittujen tietojen käsittelyyn. Oikeus päätti käyttää tietoliikennetiedustelua. (SUPO)

Suojelupoliisilla on myös oikeus saada tietoa ulkomailta. Ulkomaisen tiedustelupalvelun tarkoituksena on hankkia varhaista tietoa Suomea kohtaavista uhista, jotka ovat jo Suomen ulkopuolella. Suomen tiedustelupalvelun ainoa tavoite on suojella maata ja Suomessa asuvia ihmisiä. Kansainvälinen järjestäytynyt rikollisuus, joka uhkaa demokraattisten yhteiskuntien järjestystä. (SUPO)

Traficomin Kyberturvakeskus valvoo viestintävälittäjien verkko- ja viestintäpalvelujen turvallista toteutusta varmistaakseen, että viestinnän luottamuksellisuutta ei vaarannettu. Lisäksi keskusoppaat valvovat viestinnän välittäjiä noudattamaan lain mukaisia oikeuksiaan ja velvollisuuksiaan luottamuksellisen viestinnän käsittelyssä. Tietosuojavaltuutettu puolestaan valvoo viestintään liittyvien henkilötietojen ja sijaintitietojen eli viestintäverkoista ja päätelaitteista saatujen sijaintitietojen käsittelyä, jotka osoittavat päätelaitteen yhteyden tai maantieteellisen sijainnin. (Traficom 2021.)

Lain mukaan kommunikoivat osapuolet voivat käsitellä omia sähköisiä tietojaan ja niihin liittyviä siirtotietoja, ellei laissa toisin säädetä. Lisäksi sähköisiä viestejä ja siirrettyjä tietoja voidaan käsitellä kommunikoivan osapuolen suostumuksella tai lain edellyttämällä tavalla. Henkilö, joka on saanut tai muutoin saanut tietoa sähköisestä viestistä, radioviestinnästä tai välitetystä viestistä, joka ei ole suunnattu hänelle, ei saa ilmaista tai käyttää tällaista viestiä, välitettyä viestiä tai tällaisen viestin olemassaoloa ilman välittävän tiedon suostumusta, ellei toisin vaadita. lain mukaan. (Traficom 2021.)

Mutta laittaen eri tavalla viestinnän lähettäjä ja aiottu vastaanottaja voivat periaatteessa hoitaa keskinäisen viestinnän, mutta kukaan kolmas osapuoli ei voi käsitellä viestintää. Koska suojelupoliisilla ei tällä hetkellä ole erityisiä valtuuksia saada tietoa kansalliseen turvallisuuteen liittyvistä uhista, siviilitiedustelumääräysten tarkoituksena on parantaa suojelupoliisin mahdollisuuksia saada tietoa poliisitehtäviin liittyvistä vakavista kansainvälisistä uhista. Nämä valtuudet liittyisivät ulkomaiseen henkilöstötiedustukseen, tietojärjestelmien tiedusteluun ja tietoliikennetiedusteluihin. Salaisen tiedonhankintakeinoja ovat salakuuntelu, tiedonhankinta salakuuntelun sijasta, etävalvonta, etävalvonta puhelinosoitteen tai telepäätelaitteen omistajan suostumuksella, tukiasematietojen hankkiminen, suunniteltu salakuuntelu, salainen tiedonhankinta, tekninen salakuuntelu, tekninen katselu, tekninen valvonta, teknisten laitteiden valvonta, telepäätelaitteiden puhelinosoitteiden tai identiteettitietojen hankinta, salaiset toiminnot, väärät ostot, tietolähteiden manipulointi ja tietolähteiden valvottu käyttö sekä valvontatarkastukset. (Minilex 2020.)

Suojelupoliisilla on poliisilain viidennen luvun kolmannen §:n mukaan valtuudet rikostentorjunnan lisäksi käyttää salaisia tiedonhankintamenetelmiä seuraavien rikosten paljastamiseksi vaarantaa Suomen itsemääräämisoikeuden:

1. yllyttäminen sotaan;
2. maanpetos, maanpetos;
3. vakoilu, vakava vakoilu;
4. turvallisuussalaisuuksien paljastaminen;
5. luvaton tiedustelutoiminta;
6. Rikoslain 1 §:n 1 §:n 2–7 §:ssä tai 2 §:n 2 §:ssä tarkoitetut terroristisessa tarkoituksessa tehdyt rikokset;
7. terroristitarkoituksessa tehdyn rikoksen valmistelu;
8. johtaa terroristijärjestöä;
9. Helpotetaan terroristijärjestöjen toimintaa;
10. Tarjoaa koulutusta terrorismirikosten tekemistä varten;
11. Koulutus terroristirikosten varalta, jos teon vakavuus oikeuttaa vankeusrangaistuksen;
12. henkilöiden värväääminen terrorismirikoksiin;
13. terrorismin rahoitus;
14. terroristijärjestön rahoittaminen, jos teon vakavuus oikeuttaa vankeusrangaistuksen;
15. Matkustaminen terroristirikoksen tekemisestä, jos teon vakavuus oikeuttaa vankeusrangaistuksen.

Tiedustelutiedon käsittelyn toistuvana tilanteena on, että sillä on hankittava kansallista turvallisuutta vakavasti uhkaavasta tietoliikennetiedustelukohteiden toiminnasta tärkeitä tietoja, joita ei voida saada muilla tiedusteluvälineillä. Mikäli tietoliikennetiedustelulla hakukriteerit viittaavat vain valtion toimijoiden tai sen rinnakkaisten yksiköiden tietoliikenteeseen, tietoliikennetiedustelun avulla on hankittava tietoa tietoliikennetiedustelun kohteena olevasta toiminnasta, joka uhkaa vakavasti kansallista turvallisuutta. (Laki tietoliikennetiedustelusta siviilitiedustelussa 26.4.2019/582, § 4.)

Tietoliikennetiedustelua koskevien vaatimusten ja päätösten on koskettava:

1) tietoliikennetiedustelun kohteena oleva 3 §:ssä tarkoitettu toiminta;

2) 1 kohdassa tarkoitettua toimintaa koskevat tosiseikat;

3) tosiseikat, joihin tietoliikennetiedustelun käytön edellytykset ja tehokkuus perustuvat;

4) tietoliikennetiedustelussa käytettävät hakuehdot tai hakuehtojen luokat sekä perustelut niille;

5) rajan ylittävän viestintäverkon osa, jossa liikkuvaan tietoliikenteeseen hakuehtoja käytetään, sekä perustelut viestintäverkon osan valinnalle;

6) tietoliikennetiedustelua koskevan luvan voimassaoloaika kellonajan tarkkuudella;

7) tietoliikennetiedustelun suorittamista johtava ja valvova tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies;

8) mahdolliset tietoliikennetiedustelun rajoitukset ja ehdot.

Jos teletiedustelun tarkoitus on täytetty tai sen edellytyksiä ei enää ole, teletiedustelu on lopetettava ennen luvassa mainitun määräajan päättymistä. (Laki tietoliikennetiedustelusta siviilitiedustelussa 26.4.2019/582, § 7.)

Jos tietoliikennettä koskevia asioita ei voida viivyttää, turvallisuuspoliisin päällikkö voi päättää tietoliikennetiedustelusta, kunnes tuomioistuin ratkaisee luvan myöntämisvaatimuksen. Tämä päätös on tehtävä kirjallisesti. Asia on saatettava tuomioistuimen ratkaistavaksi mahdollisimman pian, kuitenkin viimeistään 24 tunnin kuluessa teletutkinnan alkamisesta. (Laki tietoliikennetiedustelusta siviilitiedustelussa 26.4.2019/582, § 9.)

Jos tuomioistuin toteaa, että 4 artiklan mukaiset tietoliikennetiedon edellytykset eivät täyty, sen on välittömästi lopetettava tietoliikennetiedustelun käyttö ja välittömästi tuhottava sen kautta saatu aineisto ja sen kautta saatuja tietoja koskevat muistiinpanot. Jos tuomioistuin toteaa, että 1 momentissa tarkoi-

tettu päätös on muilta osin virheellinen, tietoliikennetiedon käyttö on välittömästi lopetettava tuomioistuimen tuomion edellyttämässä laajuudessa sekä tietoliikennetiedustelun kautta saatu aineisto ja asiaa koskevat huomautukset tiedoista. saatu. Näitä tietoja voidaan kuitenkin tallentaa poliisilain henkilötietojen käsittelystä annetussa laissa tarkoitettuihin rekistereihin poliisilain 46 §:n 1 momentissa säädetyin edellytyksin. (Laki tietoliikennetiedustelusta siviilitiedustelussa 26.4.2019/582, § 9.)

Suojelupoliisi voi valtuuttaa Puolustusvoimien tiedustelupalvelun käsittelemään sotilastiedustelulain 66 §:ssä tarkoitettuja teknisiä tietoja. Puolustusvoimien tiedustelupalvelu hakee turvallisuuspoliisin puolesta sotilastiedustelulain 67 §:n mukaista lupaa teknisten tietojen käsittelyyn ja toimittaa 66 §:ssä tarkoitetun tilastollisen analyysin tulokset. Sen jälkeen toimittaa valtion turvallisuuspoliisille edellä mainitun lain 2 §:n säännökset. 7 tai 9 §:ssä säädetty Suojelupoliisin tarkoitetut päätökset toimitetaan Puolustusvoimien tiedustelupalvelulle, joka toteuttaa 5 §:n mukaiset toimenpiteet suojelupoliisin puolesta. (Laki tietoliikennetiedustelusta siviilitiedustelussa 26.4.2019/582, § 10.)

Tiedustelutiedon käytön aikana kertyneitä tietueita voi tarkastaa vain tuomioistuin tai turvallisuuspoliisin henkilöstöön kuuluva poliisi tai tiedusteluvalvontakomissaari tai hänen määräämänsä virkamies. Tallenteen voi tarkastaa myös muu virkailija, asiantuntija tai muu tiedonhankinnan toteuttamisessa avustava henkilö, poliisia suojaavan virkailijan tai tuomioistuimen määräyksestä. (Laki tietoliikennetiedustelusta siviilitiedustelussa 26.4.2019/582, § 14.)

Tietoliikennetiedon kautta saadut tiedot on tuhottava välittömästi, jos:

1) molemmat viestinnän osapuolet olivat Suomessa yhteydenottohetkellä;

2) lähettäjällä tai vastaanottajalla tai tallentajalla on velvollisuus tai oikeus kieltäytyä todistamasta 12 artiklassa mainituista asiaankuuluvista tiedoista;

3) Tietoja ei tarvita kansallisen turvallisuuden suojelemiseksi. (Laki tietoliikennetiedustelusta siviilitiedustelussa 26.4.2019/582, § 15.)

Edellä 1 momentin 3 momentissa tarkoitettuja tietoja voidaan kuitenkin poliisilain 44 §:n 5 a luvussa säädetyin edellytyksin luovuttaa rikosten ehkäisemiseksi sekä tallentaa ja tallettaa käsittelylaissa tarkoitettuun rekisteriin. henkilötietojen käsittely poliisitoiminnassa tapahtuu poliisilain 5a luvun 45 §:n 1

§:ssä säädettyjen edellytysten mukaisesti. (Laki tietoliikennetiedustelusta siviilitiedustelussa 26.4.2019/582, § 15.)

Tietojen tuhoamisesta vastaa tietoliikennetiedustelun tekninen toteuttaja, tai jos sillä on aikaa toimittaa tiedot asiakkaalle, asiakkaan vastuulla. (Laki tietoliikennetiedustelusta siviilitiedustelussa 26.4.2019/582, § 15.)

Salassapitosäännösten estämättä Suojelupoliisi voi luovuttaa tietoliikennetiedon avulla saamiaan tietoja haitallisista tietokoneohjelmista tai määräyksistä viranomaisille, yrityksille tai yhteisöille, jos luovuttaminen on välttämätöntä kansallisen turvallisuuden tai vastaanottajien etujen suojelemiseksi. Yrityksen tai yhteisön työntekijöiden salassapitovelvollisuuteen sovelletaan, mitä virkatoiminnan julkistamisesta annetun lain (621/1999) 23 §:n 2 momentissa säädetään. (Laki tietoliikennetiedustelusta siviilitiedustelussa 26.4.2019/582, § 16.)

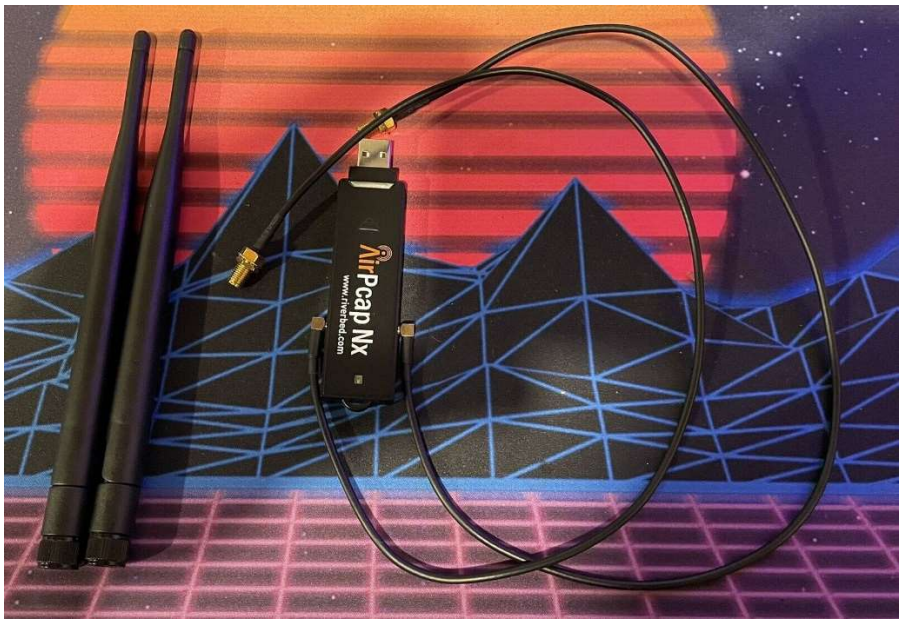
4.2 AirPcap Nx laitteen kuvas

Riverbed AirPcap -sovitin tarjoaa helpon tavan siepata ja analysoida langatonta 802.11-liikennettä ja sisältää täyden integraation suosittuun Wireshark- ja Riverbed Cascade Pilot -verkkoanalyysiin työkaluun.

AirPcap Nx on kaksikaistainen ratkaisu, joka tukee 802.11n-pakettien sieppausta ja injektiota, 802.11a/b/g vanha tila ja 4,9 GHz Yhdysvaltain yleinen turvakanava. Siinä on 2 x 2 MIMO, kaksi sisäistä antennia ja kaksi integroitua MC-korttiliitintä valinnaisille ulkoisille antenneille ja antennit, jotka parantavat suorituskykyä vaativimmissakin ympäristöissä. (Riverbed AirPcap)

AirPcap Nx tarjoaa langattoman verkon seurantatekniikkaa ja lisäominaisuuksia, kuten:

- Täysin integroitu Wiresharkin ja Cascade Pilotin kanssa täydelliseen WLAN-liikenteen analysointiin, visualisointiin, poraukseen ja raportointiin
- 802.11n liikenteen sieppaus 20 MHz ja 40 MHz kanavilla
- 802.11a, b, g pakettien sieppaus 20 MHz kanavalla
- 802.11a/b/g/n-pakettiruiskutus kaikilla nopeuksilla
- Ohjaus-, hallinta- ja datakehysten yksityiskohtainen dekoodaus
- Wireshark sisältää A-MSDU-, A-MPDU- ja HT-tiedot
- Pakettikohtaiset radiotiedot
- Mikrosekunnin aikaleiman tarkkuus
- Kaksi sisäistä antennia ja kaksi integroitua MC-korttiliitintä
- Valinnaiselle ulkoiselle antennille
- Tukee 2x2 MIMOa
- Tukee samanaikaista monikanavahankintaa yhdistettynä yhdeksi
- Yhdistetyt jäljitystiedostot käyttämällä useita AirPcap Nx -sovittimia ja ainutlaatuisia monikanavayhdistelmiä teknologiaa
- Tarjoaa AirPcap- ja WinPcap-sovellusliittymiä omien laboratoriotyökalujesi luomiseen tai laajentamiseen (Riverbed AirPcap)



KUVA 3. Riverbed AirPcap-laitteistopaketti (Ebay 2022)

Sen valmistaja Riverbed lopetti AirPcap Nx:n valmistuksen loppuvuodesta 2017. Koska tämä on Eye PA:n ensisijainen pakettien sieppauslaite, he tiesivät että heidän oli investoitava uusiin laitteisiin. AirPcap Nx:ää ei enää myydä, mutta Eye PA tukee sitä aina tulevaisuudessa. (Rich 2018.)

AirPcap Nx:n tunnettu ongelma on, että se voi aiheuttaa Blue Screen of Death (BSoD) -näytön, kun se liitetään USB 3.0 -porttiin koneessa, jossa on Windows 7 ja Intel-piirisarja. Ongelma johtuu yhteensopimattomuudesta Windows 7:n (jolla ei koskaan ollut virallista USB 3 -tukea), Intel USB 3.0 -piirisarjojen ja AirPcap Nx:n välillä. Joissakin kannettavissa tietokoneissa on sekä USB 2.0- että 3.0-portit, joten voidaan liittää AirPcap Nx:n USB 2.0 -porttiin tämän ongelman ratkaisemiseksi. Joissakin kannettavissa tietokoneissa on mahdollisuus poistaa USB 3.0 käytöstä BIOSissa ja palauttaa kaikki portit USB 2:ksi. Voidaan kokeilla käyttää koneen BIOSia nähdäksemme, onko tämä vaihtoehto käytettävissä. Tiedetään, että tämä vaihtoehto ei ole kaikkien saatavilla, mutta Windows 10 tukee alkuperäisesti USB 3:a ja toimii AirPcap Nx:n kanssa, vaikka se olisi kytketty USB 3 -porttiin. (Rich 2017.)

5 TESTAUKSET

Testausta varten, pitää asentaa jokin Linux-pohjainen virtuaalikone, koska Riverbed AirPcap Nx ei toimi oman tietokoneeni Windows 10-käyttöjärjestelmällä. AirPcap NX alkaa olla vanha laitteisto/ohjelmisto se ei toimi uudemmalla Windows 10-käyttöjärjestelmällä. Suositeltavia käyttöjärjestelmiä Riverbed AirPcap Nx paketin mukaan ovat Windows 2007/XP/Vista/7, Windows Server 2003/2008 ja Windows Server 2008 R2. Mutta kumminkin valitsin Linux-pohjaisen Kali-käyttöjärjestelmän, joka on varta vasten suunniteltu tietoliikenteen tarkkailuun. Kali-käyttöjärjestelmä tarjoaa valmiiksi asennetun Aircrack-ng-verkkoseuranta työkalun.

Aircrack on pakettien haistaja, WEP- ja WPA/WPA2-murtotyökalu, analyysityökalu ja hash-sieppaustyökalu yhdessä työkalussa. Se on työkalu Wi-Fi-hakkerointiin. Se auttaa kaappaamaan paketteja ja lukemaan niistä tiivisteitä ja jopa rikkomaan ne erilaisilla hyökkäyksillä. Se tukee lähes kaikkia uusimpia langattomia yhteyksiä.

Aircrack keskittyy pääasiassa neljään näkökohtaan:

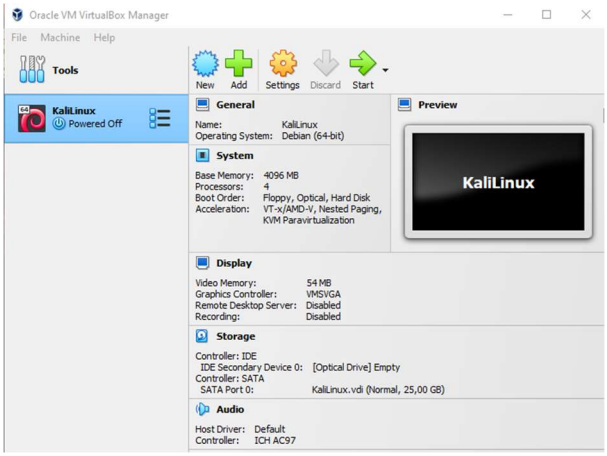
- Valvonta: sieppaa , paketteja tai hash-tiedostoja.
- Hyökkäykset: Suorita todennus tai luo väärennettyjä tukiasemia
- Testi: Tarkista Wi-Fi-kortin tai ohjaimen toiminta
- Crack: Useita suojausstandardeja, kuten WEP tai WPA PSK.

5.1 Kali-virtuaalikoneen asennus

Ensimmäiseksi pitää luoda virtuaalikone Kali-käyttöjärjestelmälle. Minä loin sen Oracle VM Virtualbox-ohjelmalla. Oracle VM Virtualbox oli minulle aikaisimmilta kursseilta tuttu työkalu ja oli valmiiksi asennettuna koneella, joten käytin sitä.

Virtualbox:ssa valitsen ja klikkaan New, joka luo uuden virtuaalikoneen. Seuraavaksi tulee ikkuna ”Nimeä ja käyttöjärjestelmä” jossa nimetään virtuaalikone ja mikä tyyppi ja sen versio. Tätä nimeä käytetään myös kaikissa tiedostonimissä (kuten kokoonpano, kiintolevyasemat ja tilannekuvat -ei ole muutettu tällä hetkellä). "Tyyppi" -sovellukselle asetin sen Linuxiksi. "Versiossa" käytin X64 -työpöytää, joten valitsin Debianin (64-bittinen). "Muistin koko" on seuraava osa, voimme määrittää käytetyn RAM-muistin määrän. Samoin mitä suurempi RAM-muisti, sitä enemmän voit avata sovelluksen ja sitä parempi sen suorituskyky. Eri työkalut Carlissa voivat vaatia resursseja. Kun tein yleisen VM: n, valitsin 4096 Mt (4 Gt) RAM-muistia.

Kohdassa ”Kiintolevy” luodaan virtuaalinen kiintolevy ja sen jälkeen kohdassa ”Kiintolevyn tiedostotyyppi”, joka on tässä tapauksessa nyt VDI (VirtualBox Disk Image). ”Tallentaminen fyysiselle kiintolevylle” ikkunassa valitaan ” Dynamically allocated”, se tarkoittaa, että on nopeampi luoda ja kasvaa suurempiin kokoihin. Kiinteän kokoiset levyt voivat olla nopeampia käyttää, mutta ne eivät voi kasvaa suurempia, kun ne täyttyvät. "Tiedoston sijainti ja koko", voin nyt määrittää kuinka suuri virtuaalinen kiintolevy on. Laitoin sen kooksi 25 Gt. Näiden jälkeen virtuaalikoneen asennus oli valmis.

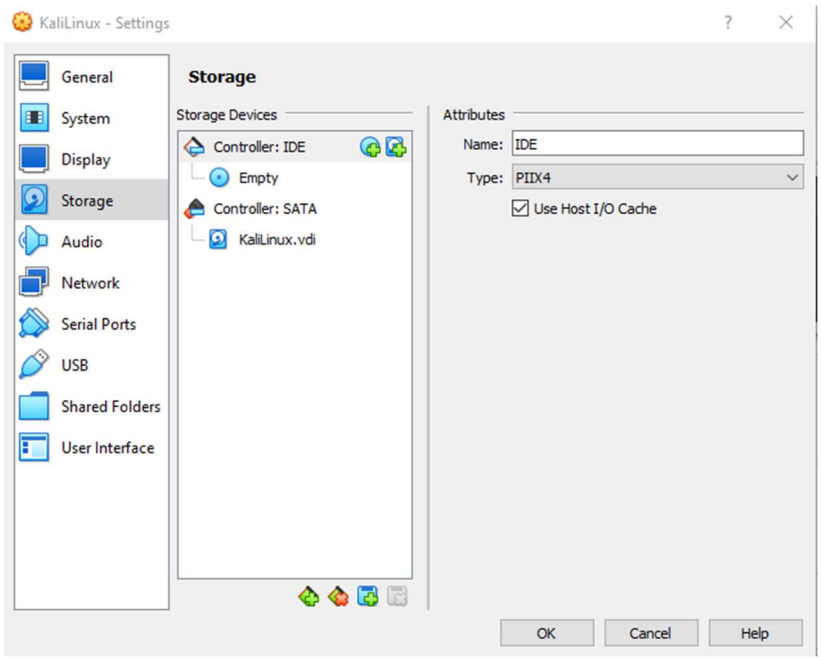


KUVA 4. Kali-virtuaalikone Oracle VM Virtualbox:ssa

Uusi ponnahdusikkuna avautuu, "Optisen levyn valitsin". Painetaan nyt "Lisää" ja siirrytään sitten ISO-sijaintiin. Kun on painettu "Avaa", tulee näkyviin, että se on lisätty, joten varmistan, että se on valittu ja paina "Valitse".

1. Aloitetaan asennus käynnistämällä valitulla asennusvälineellä. Kali Linuxin käynnistysnäyttö tulee tervetulleeksi. Valitaab joko Graafinen asennus tai Asenna (tekstitila). Tässä tilanteessa graafisen asennuksen.
2. Valitaan haluama kieli. Tätä käytetään sekä asennusprosessissa että kun käytät Kali Linuxia.
3. Määritetääb maantieteellinen sijaintisi.
4. Valitaan näppäimistöasettelu.
5. Asennus tutkii nyt verkkoliittymän, etsii DHCP-palvelun ja pyytää sitten syöttämään järjestelmän isäntänimen.
6. Voidaan valinnaisesti antaa tälle järjestelmälle oletustoimialueen nimen (arvot voidaan hakea DHCP:stä tai jos olemassa on jo olemassa oleva käyttöjärjestelmä).
7. Luodaan seuraavaksi käyttäjätili järjestelmään (koko nimi, käyttäjätunnus ja vahva salasana).
8. Asetetaan seuraavaksi aikavyöhyke.
9. Asennusohjelma tutkii nyt levyn ja tarjoaa erilaisia vaihtoehtoja asetuksista riippuen. Valitaan ohjatun - koko levyn, koska tämä on Kali Linuxin kertakäynnistysasennus, joten ei haluta muita käyttöjärjestelmiä asennettavaksi, joten pyyhitään levy. Jos levyllä on jo olemassa olevaa dataa, on olemassa ylimääräinen vaihtoehto (Opastettu - käytä suurinta jatkuvaa vapaata tilaa). Tämä ohjeistaisi asennusta olemaan muuttamatta olemassa olevia tietoja, mikä on täydellinen kaksoiskäynnistykseen toiseen käyttöjärjestelmään. Koska näin ei ole tässä esimerkissä, se ei ole näkyvissä. Jos halutaan salata Kali Linuxin, voidaan ottaa käyttöön Full Disk Encryption (FDE) -toiminnon valitsemalla Ohjattu - käytetty koko levy ja asennetaan salattu LVM. Kun tämä on valittuna, pyydetään myöhemmin asetuksissa antamaan salasana (kahdesti). On syötettävä tämä salasana joka kerta, kun käynnistetään Kali Linuxin.
10. Valitaan osioitava levy.
11. Tarpeista riippuen voidaan valita, halutaanko säilyttää kaikki tiedostosi yhdessä osiossa - oletus - tai erilliset osiot yhdelle tai useammalle ylimmän tason hakemistolle. Jos ei olla varmoja, mitä halutaan, valitaan"Kaikki tiedostot yhdessä osiossa".
12. Seuraavaksi on viimeinen mahdollisuus tarkistaa levykokoonpano ennen kuin asennusohjelma tekee peruuttamattomia muutoksia. Kun klikataan Jatka, asennusohjelma alkaa toimia ja asennus on melkein valmis.

13. Kali Linux käyttää keskusvarastoa sovellusten jakeluun. On syötettävä tarvittavat välityspalvelimen tiedot.
14. Seuraavaksi voidaan valita mitkä metapaketit halutaan asentaa. Oletusvalinnat asentavat tavallisen Kali Linux -järjestelmän, eikä tarvitse muuttaa täällä mitään.
15. Vahvistetaan seuraavaksi GRUB-käynnistyslataimen asentaminen.
16. Valitaan kiintolevy, johon halutaan asentaa GRUB-käynnistyslataimen (se ei oletuksena valitse mitään asemaa).
17. Napsauta lopuksi Jatka käynnistääksesi uudelleen uuteen Kali Linux -asennukseen.



KUVA 5. Kali-käyttöjärjestelmä asennettuna Oracle VM Virtualbox:ssa

5.2 Testaaminen

Ensimmäinen askel saada aircrack-ng toimimaan kunnolla Linux-järjestelmässä on korjata ja asentaa langattomaan korttiin oikeat ajurit. Monet kortit toimivat useiden ohjainten kanssa, joista osa tarjoaa aircrack-ng:n käyttöön tarvittavat toiminnot ja osa ei. Sanomattakin on selvää, että tarvitaan aircrack-ng-yhteensopivan langattoman kortin. Tämä on täysin yhteensopiva laitteisto, joka voi lisätä paketteja. Yhteensopivan langattoman verkkokortin avulla langaton tukiasema voidaan murtaa alle tunnissa. Katsotaan laitteiston yhteensopivuussivulta, mihin luokkaan korttisi kuuluu. Pitää muistaa: Onko langaton korttini yhteensopiva?

Tämä on lyhyt johdatus hallittuihin verkkoihin, joissa käytetään tukipisteitä. Jokainen tukiasema lähettää noin 10 ns. majakkakehystä sekunnissa. Nämä paketit sisältävät seuraavat tiedot:

- Verkon nimi (ESSID)
- Jos salausta käytetään (ja mitä salausta käytetään; huomataan, että vain koska tukiasema mainostaa, se ei välttämättä aina ole totta)
- Mitä Mbit-tiedonsiirtonopeuksia tuetaan
- mitä kanavaa verkko käyttää

Nämä tiedot näytetään sitten tähän verkkoon yhdistetyissä työkaluissa. Se tulee näkyviin, kun annetaan kortin etsiä verkkoa iwlistissa<interface> - skannaus ja suoritettaessa airodump-ng.

Jokaisella tukiasemalla on yksilöllinen MAC-osoite (48 bittiä, 6 paria heksadesimaalilukuja). Näytöt 00:01:23:4A:BC:DE. Jokaisella verkkolaitteella on tällainen osoite, ja verkkolaitteet käyttävät tätä MAC-osoitetta viestiessään keskenään. Joten se on periaatteessa kuin ainutlaatuinen nimi. MAC-osoitteet ovat ainutlaatuisia, kahdella verkkolaitteella maailmassa ei ole samaa MAC-osoitetta.

Jos halutaan muodostaa yhteys langattomaan verkkoon, on olemassa useita mahdollisuuksia. Useimmissa tapauksissa käytetään avoimen järjestelmän todennusta.

Avoimen järjestelmän sertifiointi:

- Access point vaaditaan todentamiseen.
- Access point:n vastaus: OK, olet todennettu.
- Ota yhteyttä Acess point:hen
- Access point:n vastaus: OK, olet nyt yhteydessä.

Tämä on helpoin tapaus, mutta ongelmia voi ilmetä, jos yhdistät laittomasti verkkoon:

- WPA/WPA2 on käytössä, tarvitset EAPOL-todennuksen. Access point kieltää sinut vaiheessa 2.
- Tukiasemalla on luettelo sallituista asiakkaista (MAC-osoitteet), eikä se salli kenenkään muun muodostaa yhteyttä. Tätä kutsutaan MAC-suodatukseksi.
- Tukiasemat käyttävät jaetun avaimen todennusta, ja on syötettävä oikea WEP-avain muodostaaksesi yhteyden.

Laitan Kalin monitorointitilaan seuraavasti:

1. Menen sudo su-komennolla root:iin
2. Tarkistan iwconfig-komennolla verkkoadapterit.
3. Suoritan airmon-ng listataksesi kaikki verkkoyhteydet.
4. Suoritan arimon-ng check kill lopettaaksesi häiritsevät verkkoprosessit.
5. Suoritan airmon-ng start wlan0 käynnistääksesi verkkoliittymän monitoritilassa

Kun monitoritila on käytössä, voin suorittaa airodump-ng:n sen langattoman liitännän nimellä, jota haluan käyttää, esimerkiksi airodump-ng wlan0.

Airodump-ng wlan0:n suorittaminen näyttää taulukon, jossa on tietoja langattoman sovittimen kantaman sisällä olevista langattomista tukipisteistä.

Airodump-ng:n suorittaminen voi tarjota paljon tietoa kaikista kantaman sisällä olevista langattomista laitteista. Voidaan kuitenkin suodattaa skannaukset keskittyäksesi tiettyihin verkkoihin tai laitteisiin.

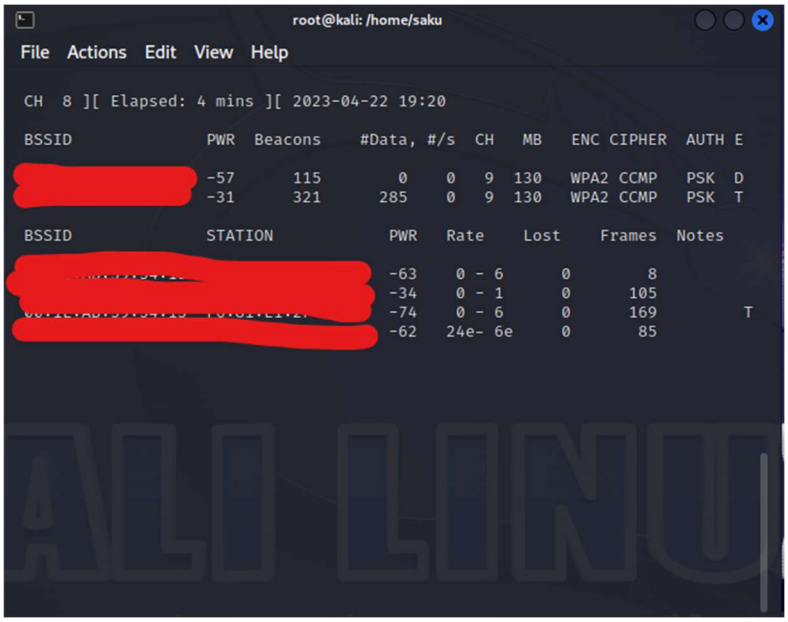
Tässä on joitain hyödyllisiä parametreja, joita voidaan käyttää airodump-ng:n kanssa lähdön suodattamiseen:

- --bssid Suodatetaan tietyn tukiaseman MAC-osoitteen mukaan.
- --channel Suodateaan tietyt kanavat. Tämä estää rowadump-ngiä ohittamasta monia kaistaa.
- --band Suodatetaan tietyt Wi-Fi-kaistat. Kirjoitin tästä lisää alla.

Komentoa --manufacturer voidaan käyttää laitteen valmistajan näyttämiseen, vaikka kaikki laitteet eivät näytä tätä tietoa.

Skannauksen aikana voidaan suodattaa näytettävää painamalla joitain interaktiivisia näppäimiä:

- Painetaan "A"-näppäintä vaihtaaksesi tukiaseman (kuten reitittimen) ja aseman (kuten kannettavan tietokoneen tai puhelimen) välillä. Tämä on hyödyllistä, jos haluat nähdä, mihin verkkoon laite on yhdistetty.
- Voidaan valita tukiaseman painamalla "TAB" ja sitten nuolinäppäimillä muita laitteita.
- Kun valitaan laite, voidaan painaa M-näppäintä korostaaksesi sen värillisenä. Vaihdetaan värien välillä pitämällä M-näppäintä painettuna. Tämä korostaa myös tukiasemaan kytketyt laitteet samalla värillä.



KUVA 6. Aircrack-ng ohjelma seuraa Riverbed AirPcap Nx:n avulla langatonta verkkoliikennettä

Ylempi tietolohko näyttää yleensä seuraavat löydetyt tukiasemat:

TAULUKKO 1. Ylemmän tietolohkon näyttämät tiedot

BSSID	AP:n MAC-osoite
RXQ	Signaalin laatu lukittuna kanavalle
PWR	Signaalin voimakkuus. Jotkut kuljettajat eivät ilmoita siitä
Beacons	Vastaanotettujen majakkakehysten määrä. Jos sinulla ei ole signaalin voimakkuutta, voit arvioida sen majakoiden lukumäärällä: mitä enemmän majakoita, sitä parempi signaalin laatu
#Data	Vastaanotettujen datakehysten määrä
#/s	Pakettien määrä sekunnissa mitataan viimeisen 10 sekunnin ajalta.
CH	Kanava, jolla AP toimii
MB	Nopeus tai AP-tila. 11 on puhdas 802.11b, 54 puhdas 802.11g. Välissä olevat arvot ovat sekoitus
ENC	Salaus: OPN: ei salausta, WEP: WEP-salaus, WPA: WPA- tai WPA2-salaus, WEP?: WEP tai WPA (en tiedä vielä)
CIPHER	Salaus havaittu. Jokin seuraavista: CCMP, WRAP, TKIP, WEP, WEP40 tai WEP104. Ei, mutta TKIP:tä käytetään yleensä WPA:n kanssa ja CCMP:tä käytetään yleensä WPA2:n kanssa. WEP40 näytetään, kun avainindeksi on suurempi kuin 0. Standardin mukaan indeksi voi olla 0–3 40 bitille ja 0 104 bitille.
AUTH	Käytettävä todennusprotokolla. Yksi seuraavista: MGT (WPA/WPA2, erillistä todennus-palvelinta käyttäen), SKA (jaettu WEP-avain), PSK (esijaettu WPA/WPA2-avain) tai OPN (WEP Open).
ESSID	Verkon nimi. Joskus piilossa

Alempi tietolohko näyttää yleensä seuraavat löydetyt asiakkaat:

TAULUKKO 2. Alemman tietolohkon näyttämät tiedot.

BSSID	Sen tukiaseman MAC, johon tämä asiakas on liitetty
STATION	Itse asiakkaan MAC
PWR	Signaalin voimakkuus. Jotkut kuljettajat eivät ilmoita siitä
Rate	Aseman vastaanottonopeus ja sitten lähetysnopeus. Jos QoS on käytössä verkossa, "e" näkyy jokaisen nopeuden jälkeen.
Lost	Viimeisten 10 sekunnin aikana kadonneiden pakettien määrä järjestysnumeron perusteella. Katso tarkempi selitys alla olevista huomautuksista.
Frames/Packets	Vastaanotettujen datakehysten määrä
Notes	Lisätietoja asiakkaasta, kuten kaapattu EAPOL tai PMKID.
Probes	Verkkonimet (ESSID), jotka tämä asiakas on tutkinut

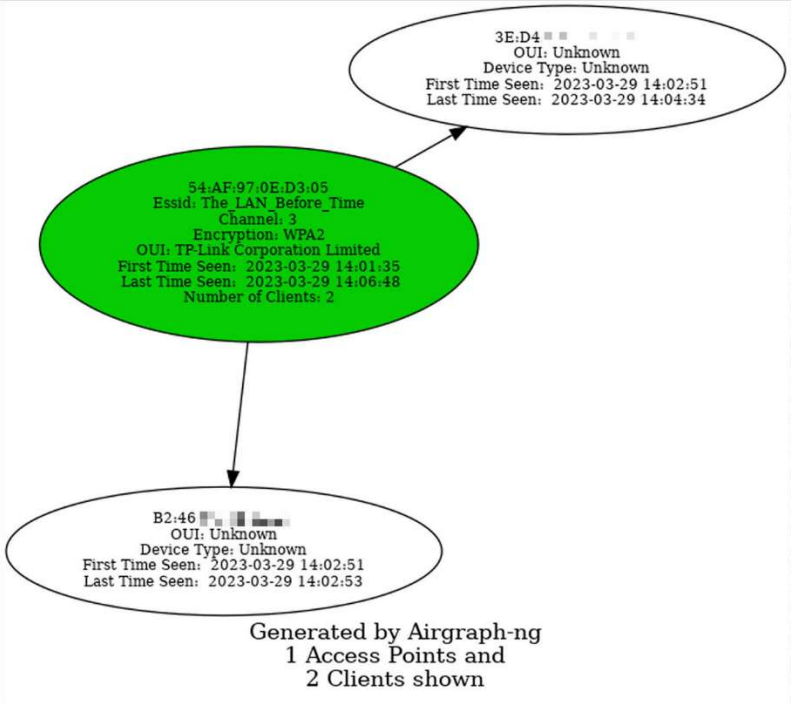
Versiosta r1648 lähtien airodump-ng voi vastaanottaa ja tulkita näppäinpainalluksia käynnissä ollessaan. Seuraavassa luettelossa kuvataan tällä hetkellä määritetyt näppäimet ja oletetut toiminnot:

- [a]: Valitse aktiiviset alueet selaamalla seuraavia näyttövaihtoehtoja: AP+STA; AP+STA+ACK; vain AP; Vain STA
- [d]: Palauta lajittelu oletusasetuksiin (virta)
- [i]: Käänteinen lajittelualgoritmi
- [m]: Merkitse valittu AP tai selaa eri värejä, jos valittu AP on jo merkitty
- [r]: (De-)Ota käyttöön reaaliaikainen lajittelu - käyttää lajittelualgoritmia aina, kun näyttö piirretään uudelleen
- [s]: Muuta saraketta lajittelemaan, joka tällä hetkellä sisältää: Ensimmäistä kertaa nähty; BSSID; PWR-taso; Majakat; Datapaketit; pakettinopeus; kanava; Max. datanopeus; Salaus; Vahvin Ciphersuite; Vahvin todennus; ESSID
- [Välilyönti]: Keskeytä näytön piirtäminen / jatka uudelleenpiirtämistä
- [TAB]: Ota käyttöön/poista käytöstä tukiasemaluettelon selaaminen
- [YLÖS]: Jos käytettävissä, valitse näytössä olevasta luettelosta tällä hetkellä merkittyä tukiasemaa edeltävä tukiasema
- [ALAS]: Valitse tukiasema tällä hetkellä merkityn AP:n jälkeen (jos saatavilla)

Aircrack-ng on kattava työkalusarja, joka on suunniteltu Wi-Fi-verkkojen auditointiin ja turvaamiseen. Sen päätarkoituksena on auttaa eettisiä hakkereita ja tietoturvaasiantuntijoita testaamaan langattomien verkkojen turvallisuutta murtamalla WEP- ja WPA-avaimia, luomalla väärennettyjä tukiasemia, sieppaamalla ja analysoimalla verkkoliikennettä sekä suorittamalla erilaisia muita verkkopohjaisia hyökkäyksiä.

Aircrack-ng-ohjelmiston avulla voi arvioida langattoman verkon suojausasennon, tunnistaa haavoittuvuudet ja testata verkon salauksen vahvuutta. Lisäksi Aircrack-ng-voidaan tunnistaa rikollisia tukiasemia, simuloida erilaisia hyökkäysskenaarioita ja suorittaa tunkeutumistestauksia.

Airgraph-ng voi luoda graafisen esityksen verkkoliikenteestä kaapatuista tiedoista ja tarjoaa visuaalisen esityksen verkon toiminnasta.



KUVA 7. Esimerkki Airgraph-Ng ohjelmasta (Cloudy Journey 2023.)

6 JOHTOPÄÄTÖKSET

Rivebed AirPcap Nx:n käyttöönotto oli aluksi mutkikas vaihe. Koska minulla on käytössä Windows 10- käyttöjärjestelmä, Riverbed AirPcap ei toiminut Wireshark-ohjelmalla. Useamman yrityksen jälkeen en saanut Riverbed:a toimimaan Wireshark:ssa. Asensin Wireshark:n useampaan kertaan ja tarvittavat USB-ajurit. Mutta lopulta tulin siihen tulokseen, ettei Riverbed toimi oman koneeni Wireshark:ssa joten päädyin käyttämään virtuaalikoneeseen asennettua Kali-käyttöjärjestelmää. Kali osoittautui myös hieman mutkikkaaksi. Asennettuani virtuaalikoneen ja Kalin, en heti saanut Aircrack-ng ohjelmaa toimimaan myöskään. Virtuaalikoneeni ei heti tunnistanut Riverbed AirPcap Nx:ää verkkoadapteriksi eikä siis löytänyt langatonta verkkoliitäntää. Mutta se pitikin vain manuaalisesti klikata USB-laitteista.

Riverbed AirPcap mahdollistaa Aircrack-ng ohjelmalla seurata eri laitteita ja access point:ja. Mutta se ei voinut seurata itse IP-pakettiliikennettä.

Haasteina oli muuan muassa aikaisemmin selitetty mutkikas Riverbed:n käyttöönotto. Riverbed muuten toimi moitteettomasti. Kun olin sitten myöhemmin tutustunut Kali-käyttöjärjestelmän ohjeisiin, oli myös sen hallinta aika helppoa. Mutta oli myös alussa haasteena oppia käyttämään ihan uutta käyttöjärjestelmää ja sen komentokehotteen komentojen oppiminen.

Rivebed AirPcap Nx voi jo omasta mielestäni kutsua ”menneen talven lumeksi”. Se ei ole enää tuettu uusimmissa Windows-käyttöjärjestelmissä ja muissa verkkoliikenteen seuraamisohjelmistoissa. Ja sen valmistaja Riverbed lopetti AirPcap Nx:n valmistuksen loppuvuodesta 2017. AirPcap Nx:ää ei enää siis myydä. Solarwind ja ManageEngine OpManager ovat esimerkiksi suositumpia langattoman verkon seuranta ohjelmia nykypäivänä.

LÄHTEET

ADI. 2020. *About WIFI.* Saatavissa: https://adi-com.co.il/en/%D7%90%D7%95%D7%93%D7%95%D7%AA-wifi/. Viitattu 20.3.2023.

Cisco Press. 2004. *Wireless System Architecture: How Wireless Works*. Saatavissa: https://www.cis-copress.com/articles/article.asp?p=344242. Viitattu 13.5.2023.

Cogipas. 2019. *Unsecured WiFi Risks: Stay Safe in Public & at Home.* Saatavissa: https://www.cogi-pas.com/unsecured-wifi-risks/. Viitattu 18.2.2023.

Dr. Chaos. 2022. *How Unsecured Wi-Fi Networks Lead to Vulnerability.* Saatavissa: https://www.drchaos.com/post/how-unsecured-wi-fi-networks-lead-to-vulnerability. Viitattu 11.2.2023.

Electronics Notes. 2023. *WiFi Standards: IEEE 802.11.* Saatavissa: https://www.electronics-no-tes.com/articles/connectivity/wifi-ieee-802-11/standards.php. Viitattu 19.2.2023.

Elprocus. 2020. *What is a WiFi Technology & How Does It Work?* Saatavissa: https://www.el-procus.com/how-does-wifi-technology-work/. Viitattu 9.2.2023.

Ervasti, E. 2015. Amnesty International. *Vapautta vai vahtimista?* Saatavissa: https://www.am-nesty.fi/vapautta-vai-vahtimista/. Viitattu 20.4.2023.

Garber, M. 2014. The Atlantic. *'Why-Fi' or 'Wiffy'? How Americans Pronounce Common Tech Terms.* Saatavissa: https://www.theatlantic.com/technology/archive/2014/06/why-fi-or-wiffy-how-americans-pronounce-techs-most-common-terms/373082/. Viitattu 15.3.2023.

Granlund, K. 2007. *Tietoliikenne*. 3 painos. Jyväskylä: Docendo.

Gupta, A. 2022. Motadata. *Verkkoliikenteen seuranta: Miksi verkonvalvojat tarvitsevat verkkoliiken-teen analysaattoria?* Saatavissa: https://www.motadata.com/fi/blog/netflow-traffic-monitoring/. Vii-tattu 9.5.2023.

ICO. 2023. *Wi-Fi security.* Saatavissa: https://ico.org.uk/for-the-public/online/wifi-security/. Viitattu 23.2.2023.

Kaspersky. 2021. *WEP, WPA, WPA2 and WPA3: Differences and explanation.* Saatavissa: https://www.kaspersky.com/resource-center/definitions/wep-vs-wpa. Viitattu 9.2.2023.

Laki tietoliikennetiedustelusta siviilitiedustelussa. 26.4.2019/582. Saatavissa: https://www.fin-lex.fi/fi/laki/ajantasa/2019/20190582#P4. Viitattu 2.3.2023.

McCurdy, P. 2009. Plant Engineering. *Understanding wireless network architecture.* Saatavissa: https://www.plantengineering.com/articles/understanding-wireless-network-architecture/. Viitattu 16.2.2023.

Minilex. 2020. *Tiedustelulait.* Saatavissa: https://www.minilex.fi/a/tiedustelulait. Viitattu 14.2.2023.

Noction. 2018. *NetFlow vs. sFlow vs. IPFIX vs. NetStream. Network Traffic Analysis and Network Traffic Monitoring.* Saatavissa: https://www.noction.com/blog/netflow-sflow-ipfix-netstream. Viitattu 9.5.2023.

Pearson. 2009. *Network+ Exam Cram: Wireless Networking*. Saatavissa: https://www.pearsonitcertification.com/articles/article.aspx?p=1329709&seqNum=4. Viitattu 10.2.2023.

Research and Markets. 2020. *Global Wi-Fi Enabled Devices Shipment Forecast.* Saatavissa: https://www.researchandmarkets.com/reports/5135535/global-wi-fi-enabled-devices-shipment-forecast. Viitattu 15.3.2023.

Rich, B. 2018. Metageek. *Introducing a new way to capture packets.* Saatavissa: https://www.metageek.com/blog/introducing-a-new-way-to-capture-packets/. Viitattu 20.2.2023.

Riverbed AirPcap. Saatavissa: http://site.microcom.us/airpcapnx.pdfhttps://www.go-wifi.co.nz/specs/DataSheet-Riverbed-AirPcap.pdf. Viitattu 13.2.2023.

Spam Laws. 2023. *Dangers of an Unsecured Wireless Network.* Saatavissa: https://www.spam-laws.com/dangers-of-an-unsecured-wireless-network.html. Viitattu 18.2.2023.

SUPO. *Suojelupoliisin työ perustuu tiedustelulainsäädäntöön.* Saatavissa: https://supo.fi/tiedustelulaki. Viitattu 12.2.2023.

Teja, R. 2021. Electronics Hub. *Wireless Communication: Introduction, Types and Applications.* Saatavissa: https://www.electronicshub.org/wireless-communication-introduction-types-applications/. Viitattu 6.2.2023.

Traficom. 2021. *Luottamuksellinen viestintä.* Saatavissa: https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/luottamuksellinen-viestinta. Viitattu 14.2.2023.

Verkon kuuntelu ja lainsäädäntö. 2021. Tietoliikenteen perusteet 2 2021. Helsingin yliopisto Saatavissa: https://tietoliikenteen-perusteet-2-21.mooc.fi/osa-2/2-laki-ja-kuuntelu. Viitattu 12.2.2023.