Elina Vaara-Sjöblom

VERKONMUODOSTUS JA -HALLINTA IEEE 802.15.4 - STANDARDIIN PERUSTUVASSA SENSORIVERKOSSA

Tietotekniikan pro gradu -tutkielma

Ohjelmistotekniikan linja

9.6.2008

Jyväskylän yliopisto

Tietotekniikan laitos

Tekijä: Elina Vaara-Sjöblom

Yhteystiedot: elina.vaara-sjoblom@chydenius.fi

Työn nimi: Verkonmuodostus ja -hallinta IEEE 802.15.4 -standardiin perustuvassa sensoriverkossa

Title in English: Network formation and management in IEEE 802.15.4 sensor network.

Työ: Pro gradu -tutkielma

Sivumäärä: 82

Linja: Ohjelmistotekniikka.

Teettäjä: Jyväskylän yliopisto, tietotekniikan laitos

Avainsanat: langaton sensoriverkko, 802.15.4, LR-WPAN, klusterointi, HEED, verkonmuodostus, verkonhallinta,

Keywords: Wireless sensor network, 802.15.4, LR-WPAN, clustering, HEED, network formation, network management,

Tiivistelmä: Langattomaan sensoriverkkoteknologiaan perustuvien sovellusten odotetaan lähitulevaisuudessa räjähdysmäisesti kasvavan. Sovellusalueita löytyy lukemattomia teollisuudesta ja ympäristön monitoroinnista kotitalouksia hyödyttäviin sovelluksiin. Laitteiden rajallisten resurssien takia tarvitaan useita erikoistuneita menetelmiä ja protokollia määrittämään sensoriverkon muodostamisen ja -hallinnan yksityiskohtia IEEE 802.15.4 -standardin lisäksi. Näiden protokollien avulla pyritään saavuttamaan sensoriverkolle toivotut ominaisuudet, kuten matala ja tasainen energiankulutus ja siten mahdollisimman pitkä elinkaari. Käytännön esimerkkinä näistä menetelmistä on esitelty HEED-algoritmi ja sen soveltuvuus standardin mukaisiin sensoriverkkoihin.

Abstract: Wireless sensor networks are envisioned to be very potential sphere of interest to computing platforms in the near future. They offer a wide range of applications to be

exploited in industry and environmental monitoring as well as in domestic domains. There is a need for specialised protocols for the network formation and management in addition to IEEE 802.15.4 standard for wireless sensor networks, due to the nature of limited resources of network devices. The goal of these methods is to achieve desired properties for the network, such as low and equal power consumption between devices and thus prolonged network life cycle. As an example of these methods HEED-algorithm and its applicability to the standard is analysed.

Esipuhe

Tämän työn tekeminen oli hieno ja opettavainen matka. Haluan kiittää kaikkia niitä henkilöitä, jotka ovat mahdollistaneet opiskeluni ja myötävaikuttaneet tämän työn syntymiseen. Erityinen kiitos kuuluu ohjaajalleni professori Ismo Hakalalle saamastani tuesta ja ohjauksesta. Kiitos myös Merja Tikkakoskelle ja Jukka Määttälälle kannustuksesta ja yhteisistä pohdinnoista.

Kiitoksen ansaitsee myös läheiseni, Kaj, joka piti kodin kasassa opiskeluni aikana, Siri ja Walter, jotka antoivat äidin uppoutua ”kouluhommiin” sekä Leena- ja Taimi-mummot, jotka auttoivat lastenhoidossa tentti- ja kirjoitusrupeamien aikana.

”Asioilla on tapana järjestyä”

Elina Vaara-Sjöblom

Termiluettelo

AMRP	Average Minimum Reachability Power
ASK	Amplitude-Shift Keying
BPSK	Binary Phase Shift Keying
CAP	Contention Access Period
CCR	Critical Coverage Range
CFP	Contention-Free Period
CID	Cluster Identification
CSMA-CA	Carrier Sense Multiple Access-Collision Avoidance,
CTR	Critical Transmitting Range
DSSS	Direct Sequence Spread Spectrum
ED	Energy Detection.
FFD	Full Function Device
GTS	Guaranteed Time Slot
HEED	Hybrid Energy-Efficient Distributed Clustering
HR-WPAN	High Rate Wireless Personal Area Network
IEEE	Institute of Electrical and Electronics Engineers
IEEE 802.15.4	IEEE:n julkaisema standardi koskien langattomia sensoriverkkoja
IETF	Internet Engineering Task Force

LLC	Logical Link Control
LR-WPAN	Low Rate Wireless Personal Area Network
MCPS	MAC Common Part Sublayer
MCPS-SAP	MAC Common Part Sublayer -Service Access Point
MIC	Message Integrity Code
MLME	MAC Sublayer Management Entity
MLME-SAP	MAC Sublayer Management Entity -Service Access Point
MPDU	MAC Protocol Data Unit
MR-WPAN	Medium Rate Wireless Personal Area Network
MSDU	MAC Service Data Unit
NESCOM	IEEE:n New Standards Committee
O-QPSK	Offset Quadrature Phase Shift Keying
PAN	Personal Area Network
PAN-koordinaattori	Sensoriverkon hallintaa hoitava laite
PDA-laite	Personal Digital Assistant
PD-SAP	Physical layer Data Service Access Point
PIB	Pan Information Base
PLME	PHY Layer Management Entity
PLME-SAP	PHY Layer Management Entity Service Access Point

PN	Pseudo Noise
POS	Personal Operating Space
PPDU	PHY Protocol Data Unit
PSDU	PHY Service Data Unit
PSSS	Parallel Sequence Spread Spectrum
QoS	Quality of Service
RA-ongelma	Range Assignment -ongelma
RF	Radio Frequency
RFD	Reduced Funcion Device
RSSI	Received Signal Strength Indication
SAP	Service Access Point
SINK	Verkon hallintalaite, PAN-koordinaattori, joka toimii verkon tiedonkeruuyksikkönä
6loWPAN WG	IPv6 over Low-Power WPAN Work Group
SSCS	Service Specific Convergence Sublayer
WLAN	Wireless Local Area Network
WPAN	Wireless Personal Area Network

Sisältö

1 Johdanto

Sensoriverkot, erityisesti langattomat sensoriverkot, ovat lupaava ja nopeasti kasvava tutkimus- ja tuotekehityskohde. Niiden käytön odotetaan nousevan räjähdysmäisesti laitteiden halpenemisen myötä. Sovellusalueita yhteiskunnasta löytyy lukemattomia ympäristön monitoroinnista kotitalouksia hyödyttäviin sovelluksiin. Langattoman sensoriverkon erityispiirteenä on sen matala energiankulutus ja laitteiden itseorganisoituvuus. Verkon laitteita ei yleensä valvota niiden sijoittamisen jälkeen, ja kun laitteesta loppuu paristo tai se rikkoutuu, sitä voi olla sijainnista johtuen vaikeaa tai mahdotonta korjata. Tavoite on luoda mahdollisimman pitkäikäisiä verkkoja, joten matala energiankulutus ja verkon tehokas organisoiminen asettavat haasteita langattoman sensoriverkon muodostamiselle ja -hallinnalle. Tässä työssä sensoriverkolla tarkoitetaan erityisesti lyhyen kantaman langattomia sensoriverkkoja.

IEEE Standards Association julkaisi vuonna 2003 langattomien sensoriverkkojen 802.15.4 -standardin, joka määrittelee laitteiden fyysisen ja MAC-kerroksen. Standardi ei määrittele verkonmuodostuksen yksityiskohtia vaan ainoastaan MAC-kerroksen tuen sille. Standardin jatkeeksi sensoriverkoille on kehitetty viime aikoina lukuisia protokollia, joiden tavoitteena on luoda energiatehokkaita ja pitkäikäisiä langattomia sensoriverkkoja Tässä työssä tutkitaan erityisesti näitä langattoman sensoriverkon muodostukseen ja hallintaan liittyviä asioita.

Luvussa kaksi luodaan yleiskatsaus lyhyen kantaman langattomiin sensoriverkkoihin ja niiden käyttökohteisiin. Luvussa kerrotaan myös langattomien sensoriverkkojen yleisimmistä verkkotopologioista sekä tarkastellaan haasteita, joita langaton sensoriverkkotekniikka kohtaa. Kolmannessa luvussa keskitytään erityisesti langattomille sensoriverkoille luotuun standardiin IEEE 802.15.4. Neljäs luku tarkastelee verkonmuodostamiseen ja -hallintaan liittyviä asioita, kuten topologian hallintaa, reititystä ja klusterointia. Luku pyrkii antamaan kokonaisvaltaisen käsityksen siitä, mitä pitää ottaa huomioon langatonta sensoriverkkosovellusta suunniteltaessa. Luvussa viisi tarkastellaan yhtä klusterointiprotokollaa, HEED-algoritmia ja sen sopivuutta langattomiin sensoriverkkoihin. HEED-protokolla on klusterointiprotokolla, joka toimii täysin

hajautetusti tavoitteenaan langattoman sensoriverkon elinkaaren pidentäminen. Lopuksi on pohdittu standardin ja HEED-protokollan yhteensopivuutta langattomissa sensoriverkkosovelluksissa.

2 Langattomat sensoriverkot

Elektronisten laitteiden ja langattoman teknologian nopea kehitys viime vuosina on luonut mahdollisuuden kehittää pienikokoisia, halpoja, yksinkertaisia ja vähän energiaa kuluttavia monitoimisia sensorilaitteita, jotka viestivät keskenään pienellä etäisyydellä toisistaan. Nämä pienet laitteet, joissa on vaatimattomia mittaus-, tiedonkäsittely ja kommunikaatio-ominaisuuksia, muodostavat langattoman sensoriverkon. Langattomat sensoriverkot ovat siis teollisuuteen tai muuhun ympäristöön tarkoitettuja tiedonkeruujärjestelmiä, ja niistä käytetään myös nimeä anturiverkko. Laitteiden edullisuus mahdollistaa tiheät ja laajat sensoriverkkosovellukset, mikä puolestaan on avannut ennennäkemättömät mahdollisuudet ja välineet kotien, kaupunkien ja ympäristöjen tutkimiseen. [7] [1] Tässä työssä sensoriverkolla tarkoitetaan nimenomaan näitä lyhyen kantaman langattomia sensoriverkkoja.

Langattomuuden puolesta puhuvat useat tekijät sensoriverkoissa. Vaikka laitteiden kappalehinta saataisiin alhaiseksi, lankaverkon kaapelointikustannukset pysyvät suurina. Kaapelit voivat katkeilla tai irrota, joten niiden ylläpitäminen ja korjaaminen on myös kallista. Mitä enemmän tietoa keräämiä sensoreita ympäristössä on, sitä runsaammin saadaan myös tietoa hyödynnettäväksi, fyysiset kaapeloinnit olisivat erittäin epäkäytännöllisiä tällaisissa tiheissä verkoissa. Langattomuus mahdollistaa myös sensoreiden liikkuvuuden, olisi hankalaa tai mahdotonta kiinnittää kaapeloitua sensoria esimerkiksi pyörivään kohteeseen. [4]

Langallisten verkkojen häiriöttömyys ja tietoturvallisuus ovat kuitenkin omaa luokkaansa verrattuna langattomiin versioihin, niinpä näiden yhdistelmä onkin paras vaihtoehto. Langattomia vaihtoehtoja käytetään siellä, missä se on tarpeellista tai antaa lisäarvoa – fyysisen verkon laajennuksina. [4]

2.1 Langattomien sensoriverkkojen käyttökohteita

Langattomat sensoriverkot voidaan luokitella Barretin *ym.* [4] mukaan seuraavasti:

- Sovellukset, joissa langattomat paristokäyttöiset lähettimet keräävät ja lähettävät mittaustietoa kohdeympäristöstä.

- Sovellukset, jotka voivat toimia ainoastaan langattoman yhteyden välityksellä, esimerkiksi renkaan ilmanpaineen mittaaminen.

- Sovellukset, joissa langaton silta toimii yhdyskäytävänä langallisen verkon ja langattoman verkon välillä.

- Sovellukset, joissa fyysinen kaapelointi olisi hankalaa.

Sensoriverkot tarjoavat muita langattomia teknologioita matalaenergiaisemman ja halvemman vaihtoehdon langattomaan tiedonsiirtoon erityisesti sovellusalueille, joissa tiedonsiirtokapasiteetista voidaan tinkiä [ST03, s.20]. Samoin siinä, missä WLAN ja Bluetooth -standardit luotiin tarkasti määritellyille sovellusalueille, langattomien sensoriverkkojen sovellusalueet vaihtelevat suuresti [4].

2.1.1 Valvonta teollisuudessa ja kaupallisella sektorilla

Teollisuuden ja kaupan aloilla langattomat sensoriverkot tuovat kustannussäästöjä esimerkiksi kaapelointitarvetta vähentämällä. Valvottavalle alueelle voidaan sijoittaa suuri määrä sensoreita tietoa keräämään. Niiden avulla voidaan hankkia reaaliaikaista informaatiota tapahtumista ja tiloista, ja siten ennakoida esimerkiksi huollon ja kunnossapidon tarvetta. Sensoriverkot voivat valvoa ja jäljittää omaisuutta tai ohjata ja automatisoida toimintaa. Sensoriverkot voidaan myös linkittää yrityksen muihin tietokantoihin päätöksenteon tueksi. [4]

2.1.2 Kotiautomaatio

Erityisesti kotiautomaatiosovelluksista ennustetaan kasvavaa alaa tulevina vuosina, joten se on erittäin potentiaalinen sovellusalue langattomille sensoriverkoille. Lyhyen kantaman langattomille sensoriverkoille luodun LR-WPAN (Low Rate Wireless Personal Area Network) IEEE 802.15.4 -standardin tiedonsiirtokapasiteetin yläraja on määritelty juuri

analysoimalla kotiautomaation sovelluksia. Kotiautomaation piiriin kuuluvat esimerkiksi [4]:

- kodin elektroniikka – esimerkiksi henkilökohtaiset, vuorovaikutteiset kaukosäätimet
- mikrotietokoneitten lisälaitteistot – esimerkiksi langattomat hiiret, näppäimistöt ja ohjaussauvat
- taloautomaatio, kuten lämmitys, valaistus, ilmastointi – esimerkiksi langattomat termostaatit, verhojen säätö valoisuuden mukaan ja langattomat valokatkaisijat
- turvallisuus ja vartiointi – sensoreitten asentaminen on helpompaa ja virrankulutus alhaisempaa käytettäessä sensoriverkkoja kuin langallisia tai bluetooth -sovelluksia
- henkilökohtainen terveydenhoito – esimerkiksi henkilökohtaisten terveystietojen säännöllinen automaattinen mittaaminen ja mittaustulosten siirtäminen seurantajärjestelmiin
- lelut ja pelit – merkittävä sovellusalue, koska lelut ja pelit ovat erityisen kustannusherkkiä.

2.1.3 Automaatio kulkuneuvoissa

Langattomat palvelut ovat lisääntymässä myös kulkuneuvoissa sitä mukaa, kun ajomukavuus lisääntyy ja kulkuneuvon hallintaan tarjotaan lisäominaisuuksia. Nykyautoissa käytetään runsaasti erilaisia sensoreita ilmaisemassa esimerkiksi polttoaineen määrää, renkaiden ilmanpainetta, öljynpainetta ja nesteiden määrää. Kulkuneuvon kunnon ilmaisemisen lisäksi sensoriverkot voivat viestiä ympäristön ja muiden kulkuneuvojen kanssa optimoimalla esimerkiksi reittejä tai antamalla reaaliaikaista informaatiota liikenneolosuhteista. [4]

2.1.4 Maatalous

Maataloudessa, erityisesti täsmäviljelyssä, on tarve sensoriverkkosovelluksille ympäristöolosuhteiden mittaamisessa. Täsmäviljely on ympäristöystävällinen järjestelmä, jonka avulla pyritään optimoimaan tuotteiden laatu ja määrä mahdollisimman pienin kustannuksin, vähällä työmäärällä sekä minimoimalla luonnonolosuhteitten vaihtelun vaikutus. Tiheillä sensoriverkoilla voidaan kerätä tietoa esimerkiksi maaperän kosteudesta, PH-arvoista, ilman lämpötilasta, sademääristä sekä muista viljelijälle tärkeistä asioista. [4]

2.1.5 Muita sovellusalueita

Sovellusalueita on rajattomasti ja LR-WPAN-tekniikkaa pidetäänkin tulevaisuuden tekniikkana. Muita sovellusalueita löytyy esimerkiksi lääketieteen, sotatieteen, biologian ja maantieteen aloilta. Biologit voivat esimerkiksi tutkia jonkin eläinpopulaation levinneisyyttä häiritsemättä itse populaatiota, tai sensoriverkkojen avulla voidaan ilmaista metsäpaloja tai tutkia tornadojen liikkeitä. Armeija voi tutkia vihollisen liikkeitä tai päätellä, onko tietyllä alueella vaarallisia kemikaaleja tai muita myrkkyjä vaarantamatta ihmishenkiä. Liikennesuunnittelussa takseihin voidaan kiinnittää sensoreita ilmaisemaan liikenneolosuhteita tai parkkipaikoilla voi olla sensoreita ilmaisemassa autoille vapaita parkkiruutuja. [ST03 s.20]

2.2 Langattomien sensoriverkkojen haasteita

Suurimmat haasteet langattomien sensoriverkkojen toteuttamisessa koskevat laitesuunnittelua ja tiedonsiirtoprotokollia. Tavoitteena on saavuttaa mahdollisimman pitkä sensoriverkon elinikä, ja samalla luotettavasti ja kannattavasti kerätä virheetöntä, oikea-aikaista tietoa sovelluskohteesta.

2.2.1 Valmistuskustannukset

Langattoman sensoriverkon laitteiden suuren määrän vuoksi yksittäisen laitteen valmistuskustannukset ovat merkittävä kustannustekijä [1]. Sensorilaitteita valmistavien yritysten olisikin huomattavasti tuottoisampaa myydä kokonaisia sovelluksia halpojen laitteiden sijaan. Helposti myytävien sovellusten puute aiheuttaa kuitenkin haasteita alan

yrityksille. Sovelluskohteet ovat hyvin pitkälle erikoistuneita, eikä ole kannattavaa suunnitella sellaista sovellusta, jonka potentiaalinen asiakaskunta ei ole laaja. [34]

2.2.2 Laiterajoitukset

Langattomaan sensoriverkkoon suunniteltu laite koostuu yleensä mittauslaitteesta, prosessorista, vastaanottimesta, lähettimestä sekä virtalähteestä. Mikäli sensoriverkon laitteelta vaaditaan tarkkaa sijaintitietoa, laitteessa täytyy olla myös paikannusjärjestelmä. Sovelluksesta riippuen laite voi olla liikkuva tai siinä voi olla muita erikoisominaisuuksia. Laitteen tulisi kuitenkin olla pieni kooltaan, kuluttaa erittäin vähän virtaa, olla helposti korvattava, toimia itsenäisesti, sopeutua toimintaympäristöön ja olla edullinen valmistaa. [1]

Laitteiden muisti- ja tiedonkäsittelykapasiteetti pyritään pitämään mahdollisimman vaatimattomana, jotta hinta pysyy alhaisena. Verkon suunnittelussa täytyy siis huomioida, että keskeiset toiminnot, kuten esimerkiksi reititystaulut, tietoturva ja datan käsittely, ovat mahdollisimman yksinkertaisia. Joissakin tilanteissa voi olla tarpeellista yhdistellä eri sensoreitten välittämää tietoa halutun informaation saamiseksi kohteesta. Osa laitteista, esimerkiksi klusteriverkon hallintasolmut, voivat siten olla hiukan älykkäämpiä pystyen esimerkiksi kokoamaan dataa ja lähettämään yhteenvetoja eteenpäin. Tämä osaltaan helpottaa myös verkon ruuhkaisuutta [28].

Langattoman sensoriverkon ympäristöolosuhteet voivat olla hyvinkin haasteellisia, mikä tekee laitteista käytännössä kertakäyttöisiä [1]. Huolto- ja korjaustoimenpiteitä voi olla mahdotonta suorittaa, mikäli tutkittava kohde sijaitsee esimerkiksi koneen sisällä, sodankäyntialueilla tai vesistössä, kuten IBM:n [17] suunnittelema sensoriverkko Hudson River -jokeen.

2.2.3 Virrankulutus

Sensorilaite käyttää virtaa mittaamiseen, viestintään ja datan prosessointiin. Sensoriverkoissa virran loppuminen laitteesta saattaa aiheuttaa merkittäviä muutoksia topologiaan ja johtaa reititysmuutoksiin, jopa koko verkon organisointiin uudelleen.

Useissa sovelluksissa laitteiden huoltaminen, esimerkiksi pariston vaihto, on hankalaa tai jopa mahdotonta. Laitteen käyttöikä on usein sama kuin pariston kesto. Laitteiden matala energiankulutus ja virransäästöominaisuuksien kehittäminen on siten kriittinen asia langattomissa sensoriverkkosovelluksissa, koska tavoitteena on myös mahdollisimman pitkäikäinen verkko. [28] [1]

2.2.4 Skaalautuvuus ja virheensietokyky

Langattomassa sensoriverkossa voi olla jopa tuhansia laitteita sovelluskohteesta riippuen ja ne voivat sijaita hyvin tiheästi alueella. Uusien laitteiden liittyminen verkkoon sekä vanhojen poistuminen on tavallista verkon elinkaaren aikana. Lisäsensoreitten sijoittaminen täytyy usein olla mahdollista koko verkon elinkaaren ajan korvaamaan toimimattomia sensoreita tai suorittamaan lisätehtäviä. Osa sensoriverkon laitteista voi lakata toimimasta tai joutua kuuluvuusalueen ulkopuolelle virran loppumisen tai ympäristöolosuhteiden muutoksen vuoksi. Yksittäisten laitteiden poistuminen ei kuitenkaan saa häiritä verkon yleistä toimintaa, ja verkon kaiken toiminnan täytyy pystyä sopeutumaan ko. muutoksiin. [1]

2.2.5 Topologian suunnittelu ja hallinta

Sensoriverkossa sensorilaitteet voivat sijaita hyvinkin tiheästi pienellä alueella, siksi verkon topologian suunnitteluun ja hallintaan täytyy kiinnittää erityistä huomiota. Topologiaan vaikuttaa muun muassa se, kuinka sensorilaitteet sijoitetaan alueelle, yksi kerrallaan vai esimerkiksi lentokoneesta kylväen. Sijoittamisen jälkeen topologia on altis jatkuville muutoksille, koska sensorilaitteiden paikka, saavutettavuus, toiminta ja tehtävät saattavat muuttua. Tiheissä verkoissa datan ruuhkautumisen ja kehysten törmäämisen vaara on suuri. Niinpä kehysten samanaikaista lähettämistä on rajattava toistensa kuuluvuusalueella olevissa laitteissa. [28] [1]

2.2.6 Tiedonsiirtomedia

Sensoreiden välisen yhteyden voi rakentaa radiotien, infrapunan tai optisen median avulla. Globaaleissa sovelluksissa täytyy ottaa huomioon, että mediaa täytyy olla mahdollista

käyttää kaikkialla maapallolla. Suurin osa sensorilaitteiden tiedonsiirrosta perustuu RF-tekniikkaan (Radio frequency). [1]

2.2.7 Itseorganisoituvuus

Langattoman sensoriverkon itseorganisoituvuus on välttämätön ominaisuus laajoissa verkoissa, koska niitä voidaan käyttää alueilla, joihin pääsy on hankalaa tai mahdotonta (esimerkiksi luonnonmullistukset, terrori-iskut tai muuten vihamieliset ympäristöt). Olosuhteet, joissa sensoriverkkosovelluksia käytetään, voivat myös olla äärimmäisen vaativia esimerkiksi sään suhteen. Lisäksi suuren solmumäärän käsinkonfigurointi on mahdotonta. Uusien laitteiden liittyminen verkkoon täytyy olla mahdollista, koska laitteet ovat häiriöherkkiä ja yksittäiset sensorilaitteet voivat lopettaa toimimisen vaikkapa pariston loppumisen myötä. Verkon täytyy pystyä sopeutumaan näihin muutoksiin. Verkon topologia vaihtelee myös jatkuvasti, koska viestinnässä käytetään radiolähetystä ja kuuluvuusalue on herkkä muutoksille, vaikka itse laitteet pysyisivätkin paikallaan. Verkon eheys ei kuitenkaan saa vahingoittua topologiamuutoksista tai yksittäisten laitteiden poistumisesta tai liittymisestä [28]. Sensoriverkkosovellukset joutuvatkin pinnistelemään säilyttääkseen halutun QoS (Quality of Service) -tason verraten vähäisillä resursseilla. [34]

2.2.8 Yhtenäiset protokollat

Krishnamachari [23] nostaa esiin haasteet sensoriverkkojen protokollien kehityksen yhteistyössä. Huolimatta laitteiden nopeasta kehityksestä, on todennäköistä, että yksittäisen laitteen kapasiteetti pysyy tulevaisuudessakin rajoitettuna. Tavoiteltavaa onkin suunnitella synergisiä protokollia, jotta sovelluksen kapasiteetti on suurempi kuin osiensa summa tiedon varastoinnin, tiedon käsittelyn ja viestinnän resurssien suhteen.

2.3 Verkkotopologiat

Langattoman sensoriverkon laajuuden ja tiheyden lisäksi verkkotopologian valintaan vaikuttaa käytettävä sovellus ja sen vaatimukset esimerkiksi viiveen, ylläpidon, skaalautuvuuden ja laitteistojen osalta. Taulukossa 1 [4] on kerrottu yleisimpien

topologioitten joitakin vahvuuksia ja heikkouksia sekä esitelty mahdollisia sovelluksia, joihin kukin topologia voisi sopia.

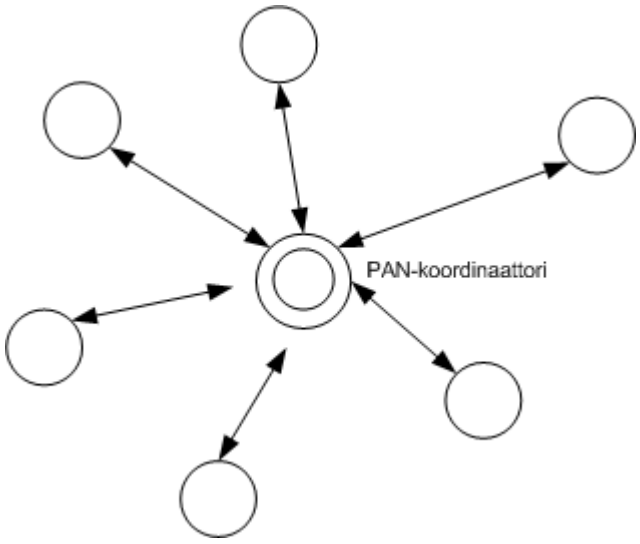
Topologia	Vahvuudet	Heikkoudet	Mahdolliset sovellusalueet
Tähti	Matala viive keskitetty verkon ohjaus	Toiminta-alue suppea vain singlehop viestin välitys	Kotiautomaatio, PC oheislaitteet
Peer-to-peer	Laaja toiminta-alue multihop viestin välityksessä	Korkeampi viive	Langattomat sensoriverkot, teollisuus, ympäristö- mittaukset
-Tasainen Mesh-verkko	Yksinkertaiset laitteet	Ongelmia skaalautu- vuudessa, kun laitteiden määrä kasvaa	Yksinkertaiset suppeat langattomat sensoriverkot
-Klusteriverkko	Mahdollistaa suuren määrän laitteita	Epätasainen virrankulutus laitteiden välillä	Kotiautomaatio (LVI)
-Klusteripuu-verkko	Mahdollistaa laajat verkot	Verkon hallinnan moni- mutkaisuus	Teollisuus, ympäristö- mittaukset, laajan alueen langattomat sensoriverkot

Taulukko 1. Topologian soveltuvuus eri kohdealueisiin [4].

2.3.1 Tähtitopologia

Tähtitopologia (Star topology) on hyvä valinta sovelluksiin, joiden täytyy kattaa tietty suppea alue ja joissa yhden laitteen täytyy olla yhteydessä kaikkiin muihin. Lelut, pelit, kotiautomaatiosovellukset sekä pc-oheislaitteet käyttävät usein tähtitopologiaa. Tähtitopologiassa keskussolmu toimii verkon hallintasolmuna eli PAN-koordinaattorina ja laitteet keskustelevat pelkästään sen kanssa. PAN-koordinaattorista käytetään yleisesti myös nimeä sink. Tämä kuvassa 1 esitetty topologia sopii hyvin sovelluksiin, joissa ei ole tarvetta solmujen keskinäiseen viestintään, vaan keskussolmu toimii tiedonkeruupisteenä. Keskussolmu on myös luonteva liityntäpiste kahden järjestelmän välillä. Topologia mahdollistaa myös muiden kuin keskussolmun yksinkertaisemman toteutuksen. Tähtiverkossa kaikki data kulkee PAN-koordinaattorin kautta, näin ollen pakettien

reititystä ei tarvita. Tähtiverkon reititys voidaankin määritellä MAC-kerroksella, toisin kuin peer-to-peer-verkon, jossa reitityksestä huolehtii verkkokerros. Tämä osaltaan yksinkertaistaa laitesuunnittelua, koska ylempiä protokollakerroksia ei tarvitse reitityksessä huomioida. Huonona puolena on verkon haavoittuvuus. Jos keskussolmun toiminta häiriintyy, koko verkko on toimintakyvytön. Usein langattomissa sensoriverkoissa on tarve tiedonsiirtoon myös laitteiden välillä, silloin peer-to-peer-topologia on järkevämpi valinta. [18]

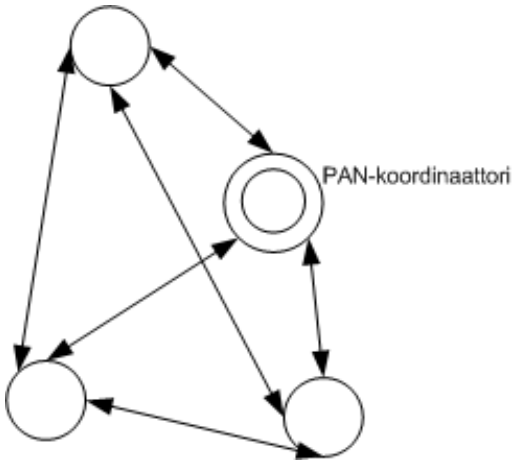


Kuva 1. Esimerkki tähtitopologian mukaisesta verkosta.

2.3.2 Peer-to-peer-topologia

Peer-to-peer-topologiassa kaikki verkon laitteet voivat viestiä keskenään kuuluvuusalueellaan. Siten se mahdollistaa monimutkaisempia verkon toteutuksia, joissa tieto kulkee suoraan solmusta toiseen. Peer-to-peer-topologian verkot voivat olla itseorganisoituvia, itsekorjautuvia sekä ad hoc -verkkoja. Itseorganisoituvassa verkossa kuuluvuusalueelle tuleva laite kuuntelee radioyhteyttä ja muodostaa itsenäisesti yhteyden PAN-koordinaattorin kanssa. Itsekorjautuvassa verkossa yhden laitteen poistuminen tai rikkoutuminen ei vaikuta verkon toimintaan. Ad hoc -verkoissa jokainen solmu voi toimia myös reitittimenä, niinpä peer-to-peer-verkossa tietoa voidaan siirtää myös multihop-menetelmällä, missä sanoma kulkee lähettäjältä vastaanottajalle muiden solmujen kautta.

Kuvassa 2 on esitetty täydellinen peer-to-peer-topologia, missä jokaisesta solmusta on linkki jokaiseen muuhun solmuun. [18]



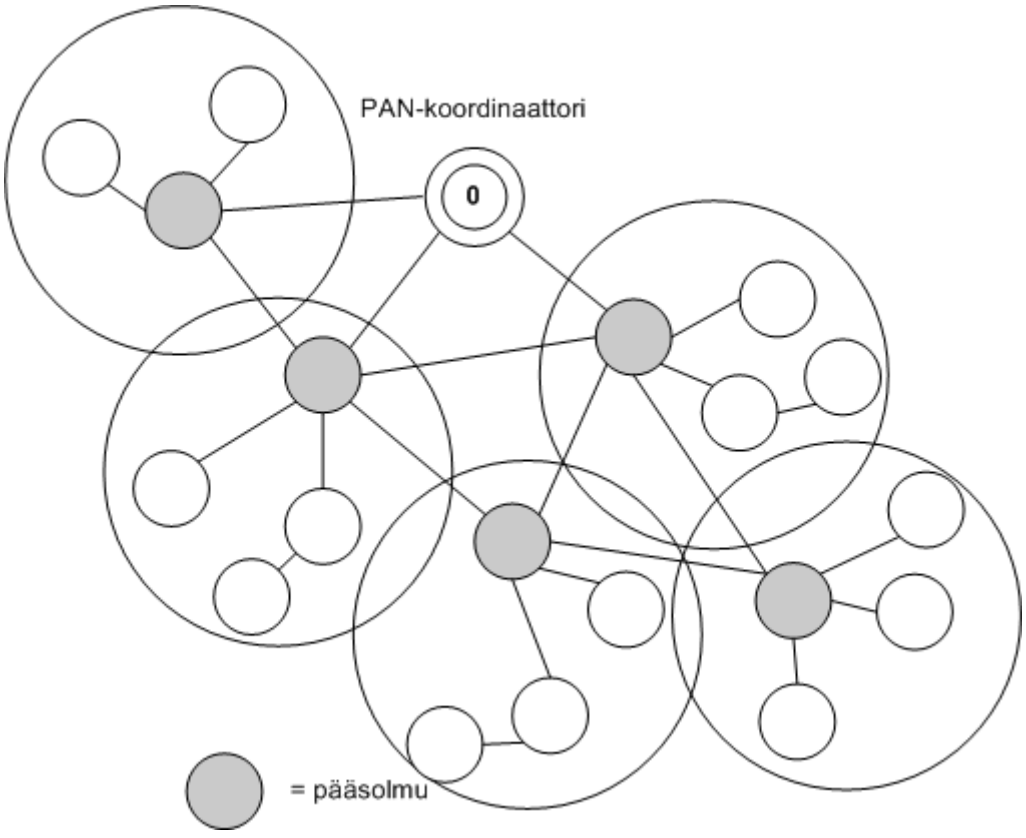
Kuva 2. Esimerkki täydellisestä peer-to-peer-topologian mukaisesta verkosta.

2.3.2.1 Mesh-verkko

Mesh-verkot voidaan jakaa kolmeen erilaiseen topologiaan. Yksinkertaisin näistä on tasainen mesh-verkko, missä laitteet toimivat sekä verkon solmuina että reitittiminä ja ovat keskenään lähes tasa-arvoisia toiminnoiltaan. Siinä laite voi olla suoraan yhteydessä kaikkiin naapureihinsa kuuluvuusalueellaan. Tasaisen mesh-verkon suurin etu on sen toteuttamisen yksinkertaisuus, mutta suuren haasteen aiheuttaa osoitteenhaku ja reititys. Yksittäisen laitteen sijainti voi olla hankala selvittää, koska laitteet eivät ole ryhmissä tai hierarkkisesti järjestäytyneitä. Hankala osoitteenhaku vaikeuttaa suuresti esimerkiksi verkon skaalautuvuutta. Hierarkkisessa mesh-verkossa laitteet ovat erikoistuneita eri tehtäviin, vain osa laitteista huolehtii reitityksestä ja muodostaa tukirangan, jota pitkin tietoa siirretään verkossa ja johon muut solmut ovat yhteydessä. Hybridi mesh-verkko on hierarkkisen mesh-verkon erikoistapaus ja se voi hyödyntää ja yhdistellä useita muita langattomia teknologioita sekä tukirangassa että tiedonkeruussa. [16]

2.3.2.2 Klusteri-verkko

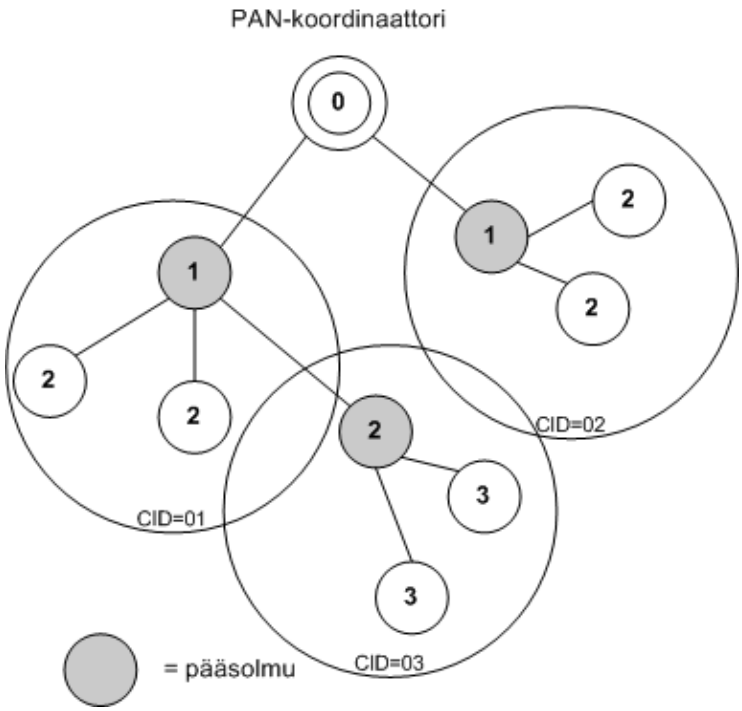
Peer-to-peer-verkon reititysongelmia helpottaa muun muassa klusterointi, missä laitteet kuvan 3 mukaisesti asettuvat sensoriverkkoon hierarkkisesti lapsi-vanhempi -tapaan. Uusi laite asettuu verkkoon aina jonkun lapseksi. Klusterissa on aina yksi pääsolmu (Cluster head, CLH), joka on klusterin juurisolmu ja huolehtii yhteydenpidosta muihin ryhmiin. Pääsolmut voivat muodostaa keskenään mesh-rakenteen. Yhdellä solmulla voi olla useita lapsia ja lapsenlapsia, mutta vain yksi vanhempi. PAN-koordinaattori voi säännöllisesti tarkistaa verkon tilan lähettämällä esimerkiksi kyselyitä lapsisolmuille, jotka eivät ole kenenkään vanhempia. Paluuviestien avulla laitteet saavat ymmärryksen oman lähiympäristönsä laitteiden organisoitumisesta ja yhteyksistä. [4]



Kuva 3. Esimerkki klusteriverkosta.

2.3.2.3 Klusteripuuverkko (Cluster tree)

Peer-to-peer-verkkojen erikoistapaus on kuvassa 4 [8] esitetty hierarkkinen klusteripuuverkko, missä solmujen numerot esittävät sen tasoa PAN-koordinaattorin ollessa tasolla 0. Klusteripuutopologian avulla saavutetaan yksinkertaisempi reititys ja huomattavasti pienempi määrä yhteyksiä verrattuna täydelliseen peer-to-peer-topologiaan. Haittapuolena voi olla suurempi viive liikennöinnissä. Verkon laitteet ovat jaoteltu hierarkkisiin ryhmiin. Jokaisessa ryhmässä on yksi laite, joka toimii pääsolmuna ja huolehtii yhteydenpidosta muihin ryhmiin. Ryhmän muut laitteet muodostavat hierarkkisen puun pääsolmuun nähden. Erona klusteri-verkkoon, myös pääsolmut ovat hierarkkisesti järjestäytyneet PAN-koordinaattoriin nähden. Jokaisella ryhmällä on oma ryhmätunnus (Cluster identification, CID). Klusteripuuverkossakin on vain yksi PAN-koordinaattori, joka voi toimia myös oman ryhmänsä pääsolmuna. PAN-koordinaattoriksi voidaan valita solmu, jolla on kyky parempaan tietojenkäsittelyyn, kyky muodostaa yhteys muihin verkkoprotokolliin tai se voi olla ensimmäinen mahdollinen laite PAN-koordinaattoriksi verkkoa muodostettaessa. PAN-koordinaattoria ja sen valintaa käsitellään tarkemmin luvussa 3.2.1. [4] [18]



Kuva 4. Esimerkki klusteripuuverkosta [8].

2.4 Langattomien verkkojen standardiperhe

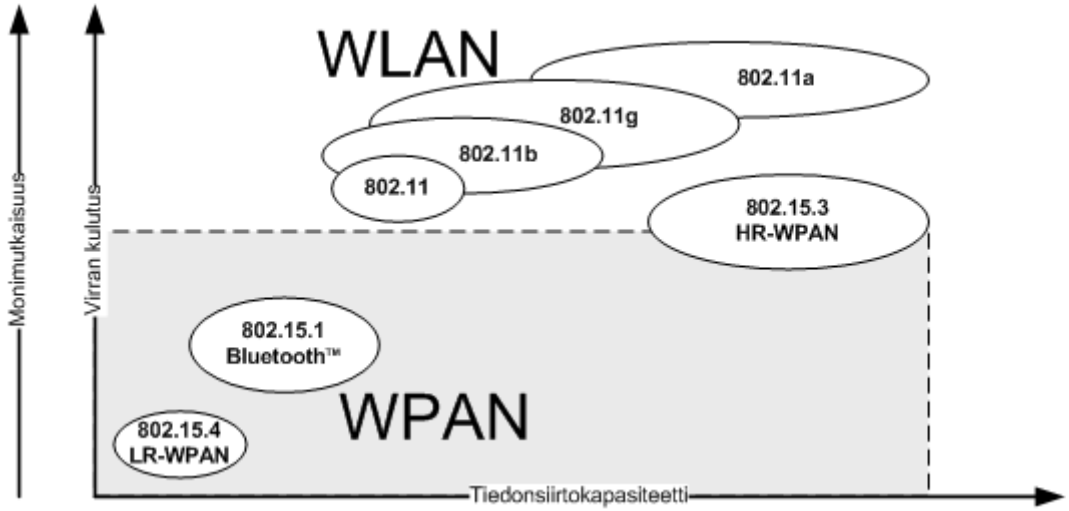
Siinä missä langattomat lähiverkot (WLAN) luotiin suuren toimintasäteen ja suuren laitekannan, saumattoman liikkumisen ja viestien välityksen tekniikaksi, langattomien PAN-verkkojen (WPAN) toimintasäde on ainoastaan muutamia kymmeniä metrejä liikkuvan tai paikallaan olevan kohteen ympärillä [4]. Nopea laitekehitys tosin mahdollistaa jo suuremmat kantamat myös WPAN-laitteille, laitevalmistajat lupaavat uusille laitteille jopa kilometrien kantaman lähetystehon lähestyessä sataa millivattia [21]. Taulukossa 2 [4] on vertailtu kolmea yleisintä langatonta tekniikkaa keskenään.

	802.11b WLAN	**802.15.1 Bluetooth™**	**802.15.4 L-R WPAN**
Toimintasäde	~100 m	~10 -100 m	10 m
Tiedonsiirtokapasiteetti	~2-11 Mb/s	1 Mb/s	≤ 0,25 Mb/s
Virran kulutus	keskiverto	matala	erittäin matala
Koko	laaja	pienempi	pienin
Hinta/ monimutkaisuus	korkea	keskiverto	erittäin matala

Taulukko 2. Langattomien verkkojen ominaisuuksia [4].

IEEE 802.15 Working Group jakaa WPAN-verkot kolmeen luokkaan tiedonsiirtokapasiteetin, pariston kulutuksen ja QoS (Quality of Service) -ominaisuuksien mukaan. IEEE 802.15.3 on korkeimman tason HR-WPAN-verkko (High Rate Wireless Personal Area Network) ja sopii multimediasovelluksille, jotka vaativat myös korkeat QoS-ominaisuudet. Keskitason MR-WPAN-verkko (Medium Rate Wireless Personal Area Network) on suunniteltu korvaamaan fyysisiä kaapeliyhteyksiä elektronisten laitteiden välillä. Tästä tuttu esimerkki on IEEE 802.15.1 -standardi eli Bluetooth™, joka on suunniteltu puhelinten ja PDA-laitteiden väliseen kommunikaatioon ja siksi äänensiirto on keskeinen QoS-ominaisuus. Matalimman tason LR-WPAN-verkot palvelevat yksinkertaisia sovelluksia, joilla on matala energiankulutus ja edulliset kustannukset. Näitä verkkoja edustaa standardi IEEE 802.15.4. Kuvassa 5 [4] on esitelty joitakin standardiperheeseen kuuluvia langattomia verkkoja virrankulutuksen, monimutkaisuuden

ja tiedonsiirtokapasiteetin osalta. Harmaalla pohjalla on kuvattu WPAN-standardeja ja vaalealla pohjalla on vertailun vuoksi WLAN-standardeja. [4]



Kuva 5. WLAN ja WPAN standardien toiminta-alueet [4].

3 IEEE 802.15.4 -standardi

Joulukuussa 2000 IEEE:n New Standards Committee (NesCom) antoi luvan aloittaa Low-Rate Wireless Personal Area Networks (LR-WPANs) -standardin kehitystyön. Tavoitteena oli määritellä standardi erittäin yksinkertaisten, edullisten ja virrankulutukseltaan vähäisten langattomien verkkojen tekemiseen halpojen, kannettavien ja liikkuvien laitteiden välille. Erityisesti kehitystyön kohteena olivat langattomat sensoriverkot. Keskeisenä ajatuksena koko kehitystyössä oli yksinkertaisuus. Kehitystyön tuloksena julkaistiin IEEE 802.15.4 -standardi marraskuussa 2003 [4]. Standardista julkaistiin päivitetty versio IEEE 802.15.4-2006 syyskuussa 2006 [19]. Vuoden 2006 standardi on alaspäin yhteensopiva alkuperäisen version kanssa [18].

3.1 Tehonkulutus IEEE 802.15.4 -standardissa

IEEE 802.15.4 -standardin keskeinen ominaisuus on lyhyen kantaman palvelut ilman tukiasemia ja kyky tukea myös hyvin laajoja verkkoja. Pieni tehonkulutus on sen tärkeimpiä ominaisuuksia, koska sensoriverkon laitteen ikä on usein sama kuin sen pariston kesto. Niinpä sen täytyy tukea äärimmäisen matalaa virrankulutusta sekä lähetys- että vastaanottotoiminnoissa. Standardi tukee laitteiden matalaa virrankulutusta sallimalla lähettimien ja vastaanottimien olevan suurimman osan toiminta-ajastaan virransäästötilassa. [4]

3.2 Verkon komponentit

Standardin mukainen LR-WPAN-verkko muodostuu vähintään yhdestä verkon koordinaattorilaitteesta sekä vähintään yhdestä tavallisesta verkon laitteesta, jotka toimivat samalla POS-alueella (Personal Operating Space). Täsmälleen yksi verkon koordinaattorilaite toimii PAN-koordinaattorina. PAN-koordinaattori on erikoistunut verkon koordinaattorilaite, joka voi olla toiminnoiltaan muita laitteita monipuolisempi. Oman sovelluksensa lisäksi sen tehtäviin kuuluu verkon muiden laitteiden ohjaus. [18]

Standardi määrittelee kahden tyyppisiä laitteita, FFD- (Full Funcion Device) ja RFD- (Reduced Funcion Device) -laitteita. FFD-laitteet voivat toimia verkon koordinaattoreina,

PAN-koordinaattoreina ja tavallisina verkon laitteina. RFD-laitteet voivat toimia ainoastaan verkon tavallisina laitteina. FFD-laitteet voivat viestiä keskenään tai RFD-laitteiden kanssa, RFD-laitteet voivat viestiä ainoastaan FFD-laitteiden kanssa, eivät siis keskenään. RFD-laitteet on tarkoitettu siis yksinkertaisiksi laitteiksi, esimerkiksi valokatkaisijoiksi. Niiden ei tarvitse lähettää suuria tietomääriä ja ne kommunikoivat vain yhden FFD-laitteen kanssa kerrallaan. Pienten resurssien ja vaatimattoman muistikapasiteetin ansiosta niiden valmistuskustannukset saadaan hyvin alhaisiksi. [18]

Standardi tukee sekä tähti- että yleistä peer-to-peer-topologiaa, johon sisältyy suuri kirjo erilaisia rakennevaihtoehtoja, joita käsiteltiin luvussa 2.3.2. Jokaisella laitteella topologiasta riippumatta on 64 bitin yksilöllinen osoite. PAN-koordinaattori voi tarvittaessa luoda kuuluvuusalueen laitteille myös 16 bitin lyhytosoitteita. Verkon laitteet ovat useimmiten paristokäyttöisiä, mutta PAN-koordinaattori toimii yleensä verkkovirralla. [18]

3.2.1 PAN-koordinaattorin valinta

Verkonmuodostuksen ensimmäinen askel on PAN-koordinaattorin valinta. Laite asettuu PAN-koordinaattoriksi, kun ylemmät protokollakerrokset lähettävät sitä koskevan komennon (MLME-START.request) laitteen MAC-kerrokselle. Sovelluksessa voidaan määritellä PAN-koordinaattorin valinta esimerkiksi seuraavilla tavoilla [4]:

- PAN-koordinaattori voidaan valita laitteen tehtävän perusteella. Joissakin sovelluksissa yhden laitteen täytyy toimia yhdyskäytävänä verkon ulkopuolelle. Tällöin on luontevaa valita tuo laite myös PAN-koordinaattoriksi.

- Sovelluksissa, joissa mikä tahansa laite voi hallita verkkoa, PAN-koordinaattori voi määräytyä toimintoperusteisesti eli jonkin ulkoisen toiminnon perusteella, esimerkiksi käyttäjän painamasta napista.

- Sovelluksissa, joissa ei ole merkitystä mikä laite on PAN-koordinaattori, voidaan antaa laitteiden itse määrätä asia. Verkon ensimmäinen laite, joka saa negatiivisen tuloksen aktiivisesta kanavaskannauksesta (käsitellään luvussa 3.6.3), eli PAN-

koordinaattoria ei vielä ole, saa luvan ylemmiltä kerroksilta toimia sellaisena. Mikäli kanavaskannauksen tuloksena saadaan beacon-sanoma useammalta PAN-koordinaattorilta, siis samalla kuuluvuusalueella on useampia LR-WPAN-verkkoja, täytyy FFD-laite ohjeistaa, kuinka toimia tällaisessa tapauksessa. Etukäteen voi olla jo 64-bittisen laiteosoitteen avulla määritelty, mihin PAN-koordinaattoriin uuden laitteen tulee liittyä.

3.3 Tiedonsiirto LR-WPAN –verkossa

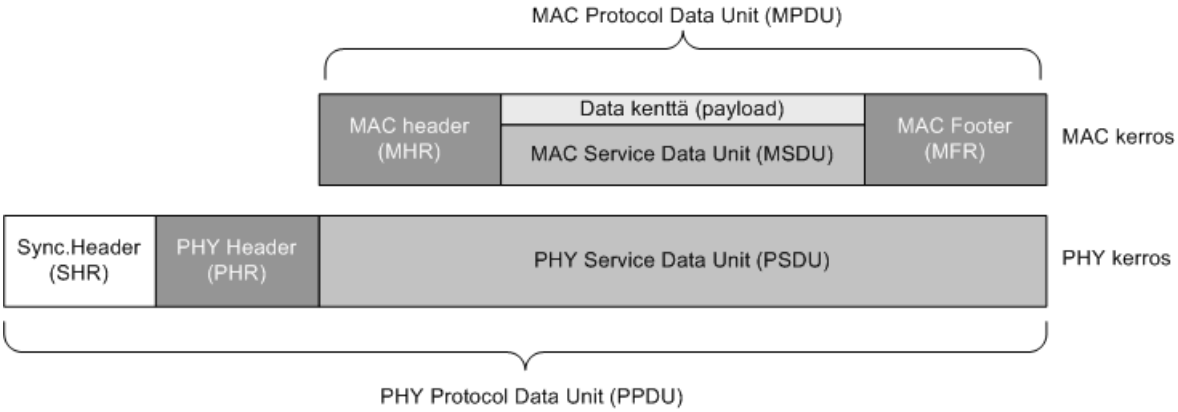
LR-WPAN-verkoissa tapahtuu kolmenlaista tiedonsiirtoa: viestejä laitteelta PAN-koordinaattorille, viestejä PAN-koordinaattorilta laitteelle sekä kahden laitteen keskinäistä tiedonsiirtoa. Tähtitopologiassa ainoastaan kaksi ensin mainittua ovat mahdollisia, koska siinä on sallittu vain laitteen ja PAN-koordinaatorin välinen kommunikointi. Verkkotopologian lisäksi standardissa on määritelty muitakin tiedonsiirtoon vaikuttavia ominaisuuksia. Tiedonsiirtoon vaikuttavat muun muassa erilaiset signaloinnit ja kanavanvarausjärjestelmä. LR-WPAN-verkon kehysrakenne on suunniteltu mahdollisimman yksinkertaiseksi, mutta toisaalta riittävän luotettavaksi häiriöiselläkin siirtotiellä. IEEE 802.15.4 -standardi määrittelee neljä erilaista tiedonsiirtokehystä [18]:

- beacon-kehys, jota koordinaattori käyttää lähettäessään verkon laitteille beacon-sanomia,
- datakehys, jota käytetään tiedonsiirrossa,
- kuittauskehys, jolla vahvistetaan sanoman perille saapuminen sekä
- MAC-komentokehys ohjaussanomia varten.

3.3.1 Kehysrakenne

Tiedonsiirtokehysten kehysrakenne on samankaltainen, suurin ero on niiden datakuormassa. Radiotielle lähetettävät kehykset ovat PPDU (PHY Protocol Data Unit) -paketteja, jotka koostuvat fyysisen kerroksen lisäämistä otsikkokentistä (synkronointi ja PHY) sekä PSDU:sta (PHY Service Data Unit). PSDU puolestaan sisältää MAC-

kerrokselta saadun MPDU:n (MAC Protocol Data Unit). Kuvassa 6 [4] näkyy PPDU:n ja MPDU:n rakenne. MSDU (MAC Service Data Unit) sisältää kehyksen MAC-kerroksen tarjoamia palveluja kuten esimerkiksi superframen tunnistetiedot, sekvenssitietoja, osoite- ja reititystietoja sekä mahdollisesti ylempien kerrosten lisäämiä otsikkotietoja. Kuittausviestien rakenne poikkeaa kuvassa 6 näkyvästä MPDU:sta, se ei sisällä MSDU:ta lainkaan. [4]



Kuva 6. Kehysrakenne [4].

3.3.2 Beacon-kehys

Beacon-kehysten lähettäminen eli majakkasignalointi on mahdollista ainoastaan verkon FFD-laitteille, RFD-laitteet pystyvät vain kuulemaan ja reagoimaan beacon-sanomiin. Verkon koordinaattori lähettää beacon-sanomia säännöllisin väliajoin ja niiden avulla verkon laitteet voivat tahdistaa toimintansa. Tarvittaessa beacon-sanomilla on useita muitakin tehtäviä. Ne voivat sisältää esimerkiksi ohjausta koskien liittymistä verkon laitteeksi. Ne myös rajaavat superframet, joita käytetään tiedonsiirrossa laitteiden välillä. Pakollista beacon-kehysten käyttö on ainoastaan uusien laitteiden houkuttelemisessa verkon laitteiksi. [4] [18]

3.3.3 Datakehys

Fyysinen kerros saa MAC-kerrokselta datakehyksen, jonka se lähettää radiotietä pitkin toisen laitteen fyysiselle kerrokselle, mistä kehys siirtyy kohdelaitteen ylemmille

protokollakerroksille. Datakehykset sallitaan kaikille verkon laitteille topologiasta riippumatta. [4]

3.3.4 Kuittauskehys

Täyttääkseen luotettavan tiedonsiirron kriteerit, täytyy sensoriverkon tarjota jokin menetelmä, jolla varmistetaan tiedon perillepääsy. Kuittauskehysten avulla vastaanottava laite ilmoittaa, että sanoma on saapunut perille. Mikäli kuittausta ei tule, lähettäjä olettaa, että sanomaa ei ole vastaanotettu ja voi yrittää lähettää sitä muutaman kerran uudelleen tai keskeyttää lähetyksen. Kaikissa viesteissä ei ole kuittauskäskyä, jolloin lähettäjä olettaa viestin saapuneen perille myös ilman kuittausta. Kuittauskehykset sallitaan myös kaikille verkon laitteille riippumatta topologiasta. [18]

3.3.5 MAC-komentokehys

MAC-komentokehyksen avulla lähetetään laitteille erilaisia ohjaussanomia, jotka voivat liittyä esimerkiksi verkonmuodostukseen tai ylläpitoon. Komentokehykset sallitaan myös kaikille verkon laitteille. [4]

3.3.6 Kanavanvaraus

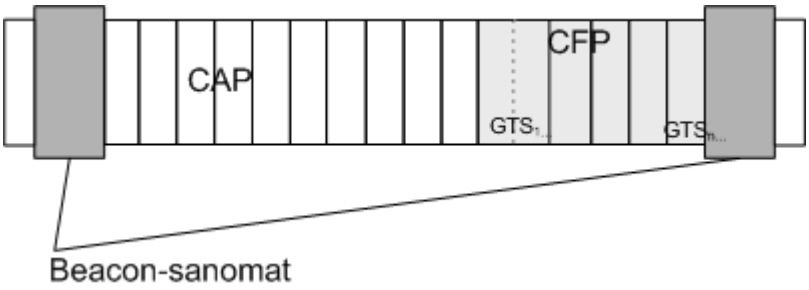
Sensoriverkkojen laitteet joutuvat usein jakamaan yhteisiä resursseja. Mikäli samalla radiotiellä on kaksi tai useampi lähetys yhtä aikaa, ne häiritsevät toisiaan ja yhteentörmäyksen riski kasvaa. Todennäköisyys kehysten perillepääsyyn laskee, joten jonkinlainen kanavanvarausjärjestelmä on tarpeen.

3.3.6.1 CSMA-CA –protokolla

CSMA-CA-kilpavarausmenetelmän avulla pyritään tunnistamaan liikenne kuuntelemalla ensin radiotietä ja lähettämällä kehys vasta sitten kun tie on vapaa. Lähettävä laite kuuntelee radiotietä ja havaittuaan sen olevan vapaa, se odottaa vielä satunnaisen ajan ennen lähettämistä. Menetelmää käytetään ainoastaan komento- ja dataviesteille, kuittausviestit ja beacon-viestit lähetetään ilman CSMA-CA-protokollaa. [4]

3.3.6.2 Superframe

Superframe-rakenne on tiedonsiirtomenetelmä, jota hallinnoi verkon PAN-koordinaattori. Superframe-kehys alkaa ja päättyy beacon-sanomiin ja sitä käytetään laitteen ja PAN-koordinaattorin väliseen kommunikointiin. Superframen käyttö edellyttää myös laitteiden keskinäistä tahdistamista, joka tehdään superframen aloittavan beacon-sanoman avulla. Beacon-sanomien avulla myös identifioidaan PAN-koordinaattori ja kuvataan superframen rakenne. Superframe on jaettu 16 samanpituiseen aikaväliin, jotka ovat beacon-sanomien välissä. Beacon-sanomien välisen ajan jakaa CAP (Contention Access Period) ja valinnainen CFP (Contention-Free Period). Laitteet, jotka haluavat viestiä PAN-koordinaattorin kanssa CAP:n aikana, käyttävät CSMA-CA-kilpavarausmenetelmää. CFP muodostuu GTS:istä (Guaranteed Time Slots), joiden avulla PAN-koordinaattori voi myöntää superframe-aikaa tietylle laitteelle. Tänä aikana radiotie on varattu pelkästään laitteen ja PAN-koordinaattorin väliseen liikenteeseen. GTS:t sijaitsevat kuvan 7 mukaisesti CAP:n ja superframen päättävän beacon-sanoman välissä. PAN-koordinaattori voi myöntää enintään seitsemän GTS:ää, kuitenkin niin, että CAP:n pituudeksi jää vähintään 440 symbolia. Yksi GTS voi sisältää yhden tai useamman aikavälin (timeslot). [4] [18]

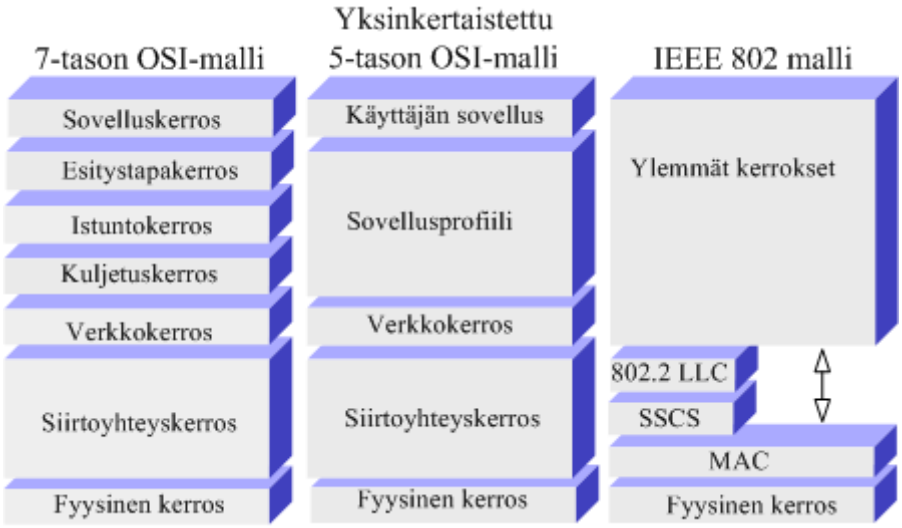


Kuva 7. Superframe-kehyksen rakenne käyttäen GTS:ää.

3.4 IEEE 802.15.4 -verkon arkkitehtuuri

Zimmermanin [38] OSI-malli kuvaa tiedonsiirtoprotokollat seitsemässä tasossa. IEEE 802 -malli määrittelee standardeissaan ainoastaan kaksi alimmaista kerrosta, siirtoyhteyskerroksen ja fyysisen kerroksen. Muiden kerrosten määrittelyistä vastaavat

yleensä alan yritysten muodostamat yhteisöt, jotka tuotteissaan käyttävät IEEE 802 -standardeja. IEEE 802.15.4 -standardin osalta ylempien kerrosten määrittelyitä tekevät muun muassa Zigbee™ Allianssi, joka käyttää kuvassa 8 esitettyä yksinkertaistettua 5-tason OSI mallia, sekä IETF:n 6loWPAN WG (IPv6 over Low power WPAN Work Group) [20]. [4]



Kuva 8. OSI-malli ja IEEE 802 malli.

Kuvasta 8 näkyy myös IEEE 802 -mallin siirtoyhteyskerros, joka on jaettu LLC-kerrokseen ja MAC-kerrokseen. LLC-kerros on määritelty IEEE 802.2 -standardissa. IEEE 802.15.4 -standardissa määritellään fyysisen kerroksen ja MAC-kerroksen lisäksi SSCS-alikerros (the Service Specific Convergence Sublayer), joka luo yhteyden MAC-kerroksen ja IEEE 802.2 -standardin LLC-kerroksen välille. IEEE 802.15.4 -standardissa MAC-kerrokseen on sisällytetty kuitenkin useita sellaisia toimintoja, jotka tavallisesti on määritelty LLC-kerrokselle, joten se pystyy liittymään myös verkkokerrokselle suoraan. Tämä mahdollistaa langattomien laitteiden yksinkertaisemman toteutuksen. [4]

3.5 Fyysinen kerros (Physical layer, PHY)

Fyysinen kerros on OSI-mallin protokollapinon alimmainen kerros ja se määrittelee siirtoyhteyden mekaaniset, fyysiset ja toiminnalliset ominaisuudet [13]. Fyysinen kerros on vastuussa radiolähettimen ja -vastaanottimen ohjauksesta (aktivoinnista ja passivoinnista),

käytetyn kanavan energian ja yhteyden laadun mittaamisesta, vapaan kanavan valinnasta ja kanavanvarauksesta sekä sanomien lähettämisestä radiotielle ja niiden vastaanottamisesta ja välittämisestä ylemmälle protokollakerrokselle (MAC-kerrokselle). [4]

3.5.1 Taajuusalueet ja kanavajako

LR-WPAN-verkot toimivat lisenssivapailla, maksuttomilla taajuuksilla, joten lähetystehon täytyy pysyä niiden rajojen sisällä, jotka viranomaiset ovat määritelleet. Taulukossa 3 [18] on esitelty LR-WPAN-verkkojen taajuusalueet, kanavat ja niihin liittyvät parametrit. Kanavanvalinnan ei pitäisi vaikuttaa kahden laitteen väliseen kuuluvuuteen, kuitenkin uusimpien tutkimusten mukaan myös kanavanvalinnalla on merkitystä [5].

Kaista mhZ	Taajuusalue MHz	Hajaspektritekniikan parametrit		Dataparametrit		
		Chip siirto-nopeus kchips/s	Modulaatio	Tiedonsiirto-nopeus kb/s	Symbolin siirtonopeus ksymbols/s	Symboli
868/915	868-868,6	300	BPSK	20	20	Binary
	902-928	600	BPSK	40	40	Binary
868/915 (valinnainen)	868-868,6	400	ASK	250	12,5	20-bit PSSS
	902-928	1600	ASK	250	50	5-bit PSSS
868/915 (valinnainen)	868-868,6	400	O-QPSK	100	25	16-ary orthogonal
	902-928	1000	O-QPSK	250	62,5	16-ary orthogonal
2,4 GHz	2,4-2,4835 Ghz	2000	O-QPSK	250	62,5	20-bit PSSS

Taulukko 3. Lisenssivapaat kaistat ja niiden ominaisuuksia [18].

Euroopassa käytetään 868 MHz:n taajuutta, Pohjois-Amerikassa, Uusi-Seelannissa ja osassa Etelä-Amerikkaa 902–928 MHz:n taajuutta, ja 2,4 GHz:n taajuus on maailmanlaajuinen. Maailmanlaajuisesta 2,4 GHz:n kaistasta on erityisen suuri hyöty laitevalmistajille, koska samaa tuotetta voidaan myydä räätälöimättä kaikkiin maihin ja tämä tietysti osaltaan alentaa valmistuskustannuksia. Toisaalta tämä taajuus saattaa juuri siitä syystä ruuhkautua joissain tilanteissa. Niinpä laitevalmistajien kannattaakin käyttää

sovelluksissaan IEEE 802.15.4 -standardin tarjoamia alempia taajuusvaihtoehtoja erityisesti alueellisissa sovelluksissa. [4]

Standardin alkuperäisessä, vuoden 2003 versiossa, kanavia eri taajuuksilla oli yhteensä 27 kappaletta. Päivitetyssä standardissa kanavia on lisätty valinnaisten taajuuksien vuoksi ja kanavajako määritellään kanavanumeroitten ja kanavasivujen yhdistelmänä. Kanavasivuja on yhteensä 32, joista sivut 3–31 on varattu tulevaisuutta varten. Kanavasivu 0 tukee vuoden 2003 kanavajakoa, missä 868 MHz:n taajuudelle on varattu 1 kanava (kanavanumero 0), 902–968 MHz:n taajuudelle 10 kanavaa (kanavanumerot 1–10) ja 2,4 GHz:n taajuudelle 16 kanavaa (kanavanumerot 11–26). Kanavasivuilla 1 ja 2 on tarjolla 11 kanavaa valinnaisille taajuusalueille, 10 kanavaa 915 MHz:n taajuudelle ja yksi 868 MHz:n taajuudelle. [18]

3.5.2 Tiedonsiirto

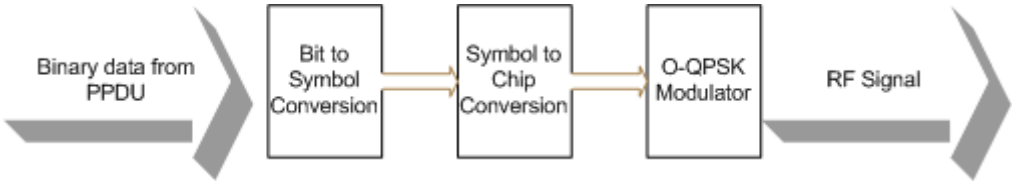
Fyysisen kerroksen vastuu tiedonsiirron osalta on radiotieyhteyden perustaminen kahden laitteen välille. Samoin se huolehtii bittien moduloinnista ja demoduloinnista, lähettimen ja vastaanottimen tahdistamisesta sekä pakettien synkronoinnista [4]. Sen ensisijainen tehtävä on siis bittitiedon siirtäminen mahdollisimman virheettömästi. Fyysisen kerroksen tehtäviin ei kuitenkaan kuulu virheettömyyden tutkiminen, se on ylempien kerrosten tehtävä [36]. Tiedonsiirtomenetelmänä standardi käyttää hajaspektritekniikkaa, joka toteutetaan suorasekvenssimenettelynä (Direct Sequence Spread Spectrum, DSSS) tai rinnakkaissekvenssimenettelynä (Parallel Sequence Spread Spectrum, PSSS) [18]. Hajaspektritekniikka poikkeaa perinteisestä siirtotekniikasta. Perinteiset järjestelmät käyttävät tiedonsiirtoa varten yhden kapean taajuusalueen, jolla ne liikennöivät. Hajaspektritekniikassa taajuusalue jaetaan useaan alitaajuuteen, joilla lähetetään samanaikaisesti tai vuorotellen. Tiedonsiirtolaite käyttää siis suuren taajuusalueen, jolle lähetys jaetaan. Hajaspektritekniikka parantaa lähetyksen häiriöttömyyttä ja tietoturvaa, mutta tarvitsee suuremman taajuuskaistan [31]. [13]

Suorasekvenssimenettelyssä lähetykseen lisätään bittejä kertomalla jokainen lähetettävän tiedon bitti 11 bitin näennäissatunnaisella kohinalla, joka lisää signaaliin tekokohinaa

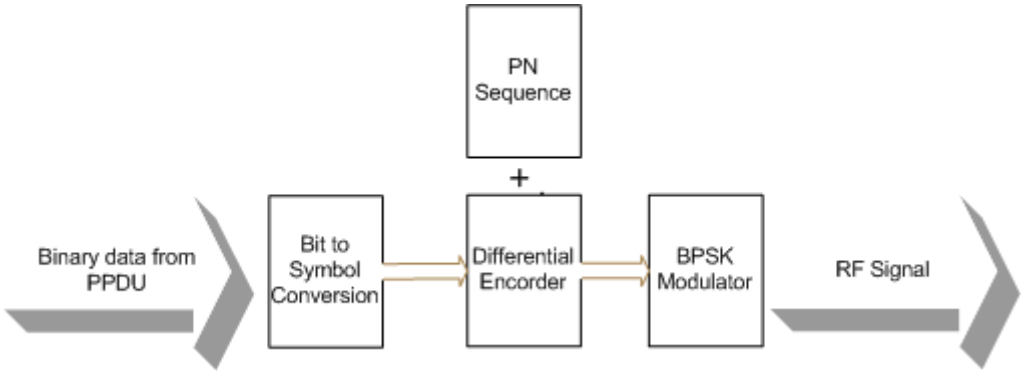
(Pseudo noise, PN). Lähetettävän signaalin spektri on alkuperäistä leveämpi, mutta kunkin alitaajuuden lähetysteho ei ole juuri normaalia taustakohinaa suurempi [31]. Siten tietoturva paranee, koska signaalia on vaikea havaita taustakohinan seasta. Rinnakkaissekvenssimenettelyssä lähetettävä viesti jaetaan k-bitin jaksoihin, käsitellään rinnakkain [35].

Moduloinnissa 868 MHz:n ja 915 MHz:n taajuuksilla käytetään BPSK-menetelmää (Binary Phase Shift Keying). Valinnaisilla taajuuksilla voidaan käyttää myös ASK-modulointia (Amplitude-Shift Keying) sekä O-QPSK-modulointimenetelmää (Offset Quadrature Phase Shift Keying). 2,4 GHz:n taajuuskaistalla käytetään O-QPSK-modulointimenetelmää.

ASK-moduloinnissa amplitudia muutetaan moduloivan digitaalisen ohjauksen mukaan, missä 1-bittiä vastaa maksimiamplitudi ja 0-bittiä 0-amplitudi [25]. O-QPSK-menetelmässä alkuperäinen data muutetaan kuvan 9 [4] mukaisesti neljän bitin jaksoissa 32 bitin lastuiksi (chip) ja käsitellään O-QPSK-modulaattorilla ennen radiotielle lähettämistä. BPSK-menetelmässä 1-bittiä kuvaa symboli, joka muodostetaan yksittäisestä bitistä ja differentiaalikooderin avulla tehdystä 15-bittisestä PN (pseudo random) -hajoituskoodista. Hajoituskoodin käänteiskoodia käytetään kuvaamaan 0-bittiä. Lopuksi nämä moduloidaan BPSK-modulaattorilla kuvan 10 mukaisesti. [4]



Kuva 9. Bittien muunnos radiotielle 2,4 GHz:n taajuudella [4].



Kuva 10. Bittien muunnos radiotielle 868 / 915 GHz:n taajuuksilla.

3.5.3 Lähetysteho

Standardin mukaan verkon laitteesta täytyy löytyä vähintään -3 dBm:n lähetysteho, mikä vastaa 0,5 mW lähetystehoa. Maksimitehon puolestaan määrittelevät viranomaiset. Esimerkiksi Yhdysvalloissa 2,4 GHz:n kaistalle sallitaan jopa 1 Watin lähetysteho käytettäessä hajaspektritekniikkaa, kun taas Euroopassa raja on tälle kaistalle 100 milliwattia [4]. Suomessa viestintävirasto [37] määrittelee maksimilähetystehoksi 100mW 2,4 GHz:n kaistalle ja 25 mW 868 MHz:n kaistalle.

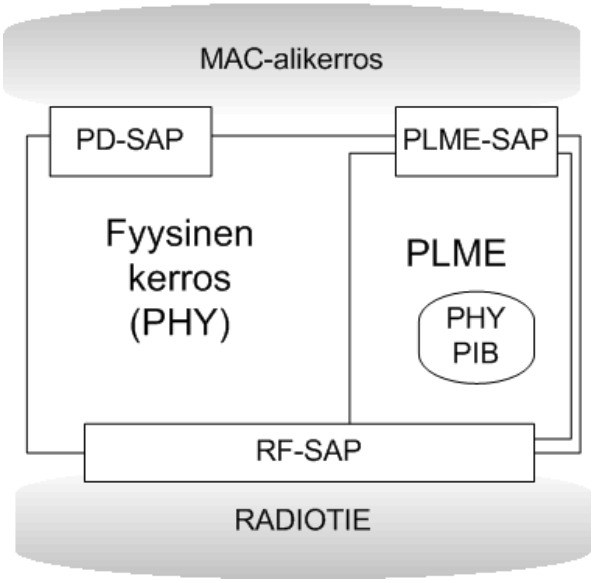
IEEE 802.15.4 -standardi määrittelee myös herkkyysvaatimukset laitteille. Laitteen täytyy pystyä vastaanottamaan sanoma oikein vielä -85 dBm:n lähetysteholla 2,4 GHz:n taajuudella ja alemmilla taajuuksilla -92 dBm:n teholla. [4]

3.5.4 Kanavan viritysterävyys

Taajuuskaistalla 915 MHz on 10 ja taajuuskaistalla 2,4 GHz 16 kanavaa. Standardin mukaan laitteen täytyy näillä kaistoilla pystyä torjumaan yhden vierekkäisen kanavan häiritsevä signaali, jonka lähetysteho on sama kuin samanaikainen käytettävän kanavan liikenne. Koska LR-WPAN-verkkojen liikenteen oletetaan olevan kohtuullisen harvaa, standardissa on katsottu yhden vierekkäisen signaalin torjuminen riittäväksi. Lisäksi laitteen täytyy pystyä torjumaan yli 30 dB:n liikenne, joka tulee jommankumman vierekkäisen kanavan kahdesta seuraavasta kanavasta. Tässäkin riittää kyky yhden häiritsevän signaalin torjumiseen kerrallaan. [4]

3.5.5 Palvelut MAC-kerrokselle

Fyysinen kerros tarjoaa liittymän fyysisen radiotien ja MAC-alikerroksen välille ohjaus- ja datapalvelulla. Fyysisen kerroksen ohjausyksikön, PLME:n (PHY layer management entity), avulla kutsutaan kerroksen ohjauspalveluita PLME-SAP-rajapinnan (PLME-Service Access Point) kautta. PLME pitää yllä myös tietokantaa objekteista, jotka ovat tekemisissä fyysisen kerroksen kanssa. Tästä tietokannasta käytetään nimitystä PHY PIB (PHY Pan Information Base). Fyysisen kerroksen datapalveluita kutsutaan PD-SAP:n kautta (PHY layer Data Service Access Point). Kuvassa 11 on havainnollistettu näitä käsitteitä. [18]



Kuva 11. Fyysisen kerroksen rakennemalli ja rajapinnat [18].

Datapalvelut sisältävät kolme primitiiviä, joiden avulla viestitään MAC-alikerroksen kanssa [18]:

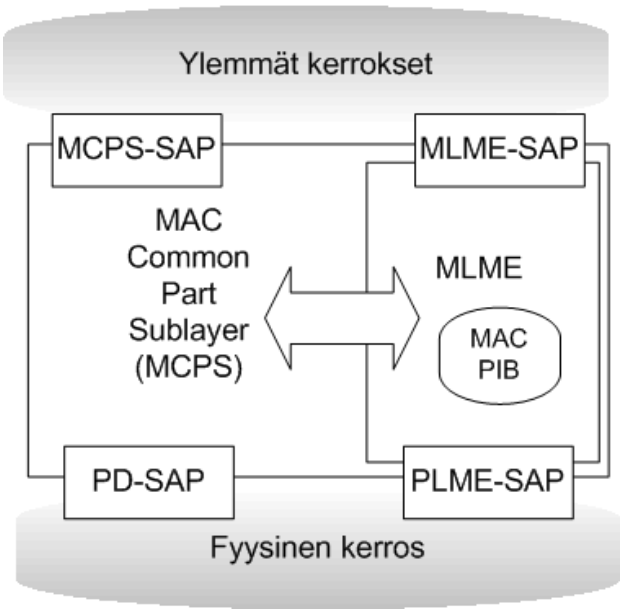
- PD-DATA.request, jonka lähettää kutsuva MAC-kerros paikalliselle PHY:lle aloittaakseen MPDU:n siirron
- PD-DATA.indication, jonka avulla PHY ilmoittaa MAC-kerrokselle datasiirron aloittamisesta.
- PD-DATA.confirm, joka vahvistaa datasiirron, joko ehjänä tai virheellisenä.

Ohjauspalveluiden PLME-primitiivejä on viisi: GET, SET, SET-TRX-STATE, CCA ja ED ja niitä käytetään seuraavasti [4]:

- PLME-GET ja PLME-SET -primitiivejä käytetään PIB-tietokannan ylläpidossa.
- Radiolähetin avataan ja suljetaan PLME-SET-TRX-STATE-primitiivin avulla. Tämän palvelun avulla mahdollistetaan matala virrankulutus.
- PLMA-CCA-primitiivin avulla toteutetaan CCA-toimintoa (vapaan kanavan valinta).
- PLME-ED-primitiiviä käytetään energianmittaukseen käytössä olevasta kanavasta.

3.6 MAC kerros

MAC-kerroksen tärkeimmät tehtävät ovat verkon infrastruktuurin luominen sekä yhteysresurssien tehokas ja oikeudenmukainen jakaminen laitteiden välillä [1]. MAC-kerros tarjoaa kahdenlaisia palveluita: MCPS-datapalveluita (MAC Common Part Sublayer), jotka huolehtivat MPDU:jen lähettämisestä ja vastaanottamisesta sekä datasiirroista ylempien kerrosten kanssa, ja MLME-ohjauspalveluita (MAC sublayer Management Entity). MLME huolehtii myös tietokannan ylläpidosta (MAC PIB). Kuvasta 12 näkyy MAC-kerroksen eri rajapinnat, SAP:t, joiden kautta palveluita voidaan kutsua. Ylemmät kerrokset kutsuvat ohjauspalveluita MLME-SAP:n kautta ja datapalveluita MCPS-SAP:n kautta. Lisäksi on olemassa yhteys MLME:n ja MCPS:n välillä, jonka kautta MLME voi käyttää MCPS:n datapalveluita. [18]



Kuva 12. MAC-alikerroksen rakennemalli ja rajapinnat [18].

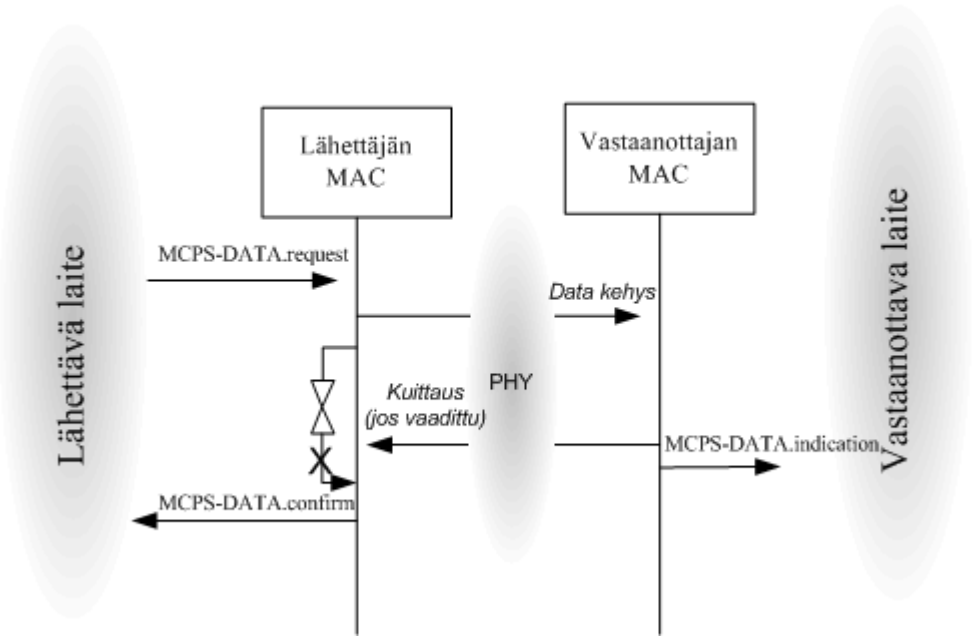
MAC-kerroksen kautta kulkevat kaikki sanomat fyysiselle kerrokselle ja sillä on lukuisia tehtäviä vastuullaan [18]:

- Luotettavan tiedonsiirron tarjoaminen kahden laitteen MAC-kerrosten välillä.
- Laitteen assosiaation, eli verkkoon liittymisen, sekä disassosiaation, eli yhteyden katkaisun ohjaaminen, ylempien kerrosten pyynnöstä.
- GTS-palvelun (jonka avulla varataan laitteelle yhteysaikaa superframessa) toteuttaminen ja ylläpitäminen.
- Verkkolaitteen tahdistaminen beacon-sanomien avulla.
- Beacon-sanomien generointi, jos laite on koordinaattori.
- Laitteen tietoturvan tukeminen.
- CSMA-CA-menetelmän toteuttaminen kanavanvarauksessa.

3.6.1 Tiedonsiirto

Langaton tiedonsiirto on usein altis häiriöille. Tarvitaankin mekanismi varmistamaan, että viestit ovat menneet perille. Mikäli lähetetyssä paketissa on virheitä, voi olla että se ei koskaan saavu vastaanottavan laitteen MAC-kerrokselle, koska fyysinen kerros ei pysty sitä vastaanottamaan (kuulemaan) tai välittämään. Kolme skenaariota on mahdollista kuittausta vaativissa tiedonsiirtotapahtumissa: Onnistunut tiedonsiirto (data ja kuittaus), epäonnistunut datan siirto tai epäonnistunut kuittaus. Kahdessa viimeksi mainitussa tapauksessa MAC-kerros ei saa kuittausta onnistuneesta tiedonsiirrosta ja niinpä MCPS yrittää lähettää sanomaa uudelleen useita kertoja. Jatkuvien epäonnistumisten jälkeen se informoi ylempiä kerroksia epäonnistuneesta tiedonsiirrosta. [4]

MAC-datapalvelu tarjoaa kolmenlaisia primitiivejä kuten PHY-datapalvelukin: data.request, data.confirm ja data.indication. Neljättä data.response-primitiiviä ei vaadita, koska datapalvelun luonne on tahdistamaton. Näiden käyttötarkoitus näkyy myös kuvassa 13. [4]



Kuva 13. Sekvenssikaavio onnistuneesta tiedonsiirrosta MAC-kerroksilla [4].

MLME tukee komentoja, joilla ohjataan sanoma-asetuksia, radiota sekä verkon toimintaa. MLME-ohjausprimitiivivalikoima on laajempi kuin fyysisen kerroksen, johtuen MAC-

kerroksen laajasta tehtävänkuvasta. Koska standardissa on haluttu varmistaa mahdollisimman yksinkertaisten laitteiden toteuttaminen, kaikki primitiivit eivät ole pakollisia. Valinnaiset primitiivit liittyvät lähinnä tähtitopologian tukemiseen. Taulukossa 4 [4] on esitelty MLME-ohjausprimitiivit ja niiden käyttöyhteys.

			Käytettävät Datapalveluprimitiivit			
Primitiivi	**Kategoria**	**Kuvaus**	Request	Confirm	Response	Indication
GET	Sanoma-asetukset	MAC PIB hallinta	x	x		
SET			x	x		
RESET			x	x		
RX-ENABLE	Radion ohjaus	Radio on/off	x	x		
SCAN		Radiokanavien skannaus	x	x		
ASSOCIATE	Verkon ohjaus	Verkkoon yhdistyminen / yhteyden katkaisu	x	x	x	x
DISASSOCIATE			x	x		x
GTS*		GTS hallinta	x	x		x
ORPHAN*		Orvon laitteen hallinta			x	x
SYNC		Tahdistuksen hallinta				
SYNC-LOSS			x			x
START*		Beacon-sanomien hallinta	x	x		
BEACON-NOTIFY						x
POLL		Tahdistus ilman beacon-sanomia	x	x		
COMM-STATUS		Sanomien tila				x

*=valinnainen

Taulukko 4. MAC-kerroksen MLME-ohjausprimitiivit [4].

3.6.2 Assosiaatio ja disassosiaatio

Assosiaatiolla tarkoitetaan yksittäisen laitteen liittämistä verkkoon. LR-WPAN-verkossa assosiaatiota käytetään tähtitopologiassa. Laite, joka haluaa liittyä tähtiverkkoon, kuuntelee ensin PAN-koordinaattorin lähettämiä beacon-sanomia. Vastaanotettuaan sellaisen, laite lähettää assosiaatiopyynnön (MLME.ASSOCIATE.request) PAN-koordinaattorille. PAN-koordinaattorilla on valta hyväksyä tai hylätä laite. Assosiaation yhteydessä laitteella on mahdollista anoa PAN-koordinaattorilta 16-bittistä lyhytosoitetta käyttöönsä korvaamaan 64-bittinen yksilöllinen osoite. Lyhytosoitteen ansiosta sanomapakettien pituus lyhenee ja se osaltaan parantaa kaistanleveyden käyttöastetta. Aloitteen yhteyden purkamiseen eli disassosiaation voi tehdä laite tai PAN-koordinaattori käyttämällä MLME-DISASSOCIATE-primitiivejä. Mikäli yhteys katkeaa vahingossa eli laite jää orvoksi, se

voidaan rakentaa uudelleen MLME-SCAN- ja MLME-ORPHAN -primitiivien avulla. Peer-to-peer-topologia mahdollistaa monimutkaisemman verkonmuodostuksen ja standardi ei määrittele verkonmuodostuksen yksityiskohtia, ainoastaan MAC-kerroksen toiminnot sen tukemiseen, kuten kanavaskannauksen ja tahdistamisen, joita käsitellään seuraavissa luvuissa. [4]

3.6.3 Kanavaskannaus

Standardi tarjoaa kanavaskannaukseen neljä eri menetelmää, joiden avulla laite voi muun muassa määrittää oman ja muiden laitteiden paikat toiminta-alueellaan. [4]

- Passiivisen kanavaskannauksen avulla FFD- ja RFD-laitteet kuuntelevat beacon-sanomia haluamiltaan kanavilta.

- Orpo FFD- tai RFD-laite voi yrittää päästä uudelleen yhteyteen koordinaattorin kanssa Orphan-kanavaskannauksen avulla.

- Aktiivisen kanavaskannauksen avulla FFD-laite etsii muiden laitteiden lähettämiä beacon-sanomia kuuluvuusalueellaan. Erona passiiviseen, laite lähettää haluamilleen kanaville Beacon Request -käskyn, johon koordinaattori vastaa lähettämällä beacon-sanoman.

- FFD-laite voi suorittaa kanavan energiamittausta ED (Energy Detection) -skannauksen avulla. Energiamittauksessa haluttuja kanavia kuunnellaan ja jokaiselta mitataan suurin signaaliteho. Mittauksen perusteella laite voi esimerkiksi päättää yrittääkö liittyä osaksi jo olemassa olevaa verkkoa vai alkaako se PAN-koordinaattorina muodostaa omaa verkkoaan [8].

3.6.4 Tahdistaminen

Tahdistamisessa käytetään MLME-SYNC- ja MLME-SYNC-LOSS-primitiivejä, joiden avulla etsitään beacon-sanomia esimerkiksi tiedonsiirron aloittamista varten. Tahdistaminen voi olla kertaluonteista tai jatkuvaa ja se tapahtuu aktivoimalla radiovastaanotin tietyksi ajaksi beacon-sanoman vastaanottamista varten. Standardi sallii

tahdistamisen myös ilman beacon-sanomia. Tällöin laite ilmoittautuu PAN-koordinaattorille saatuaan MLME-POLL.request-primitiivin ylemmältä protokollakerrokselta. [4] [18]

3.6.5 Beacon-sanomat

Beacon-sanomia käytetään tahdistamaan kaksi eri laitetta keskenään tiedonsiirtoa varten ja niiden avulla merkitään myös superframen alkaminen ja päättyminen. Beacon-sanomista hyötyvät myös sellaiset sovellukset, jotka haluavat vähentää viestien viivettä koordinaattorin ja verkkolaitteen välillä. Verkkolaite voi tarkistaa jo beacon-kehyksen pending-kentästä, onko sille tulossa sanomia.

Joissakin sovelluksissa beacon-sanomat voivat kuitenkin rasittaa verkkoa. Esimerkiksi sellaisissa verkoissa, joissa on hyvin vähän liikennettä verkkolaitteen ja koordinaattorin välillä, beacon-sanomat aiheuttavat turhaa virrankulutusta sekä verkkolaitteessa että koordinaattorissa. Parempi vaihtoehto on olla käyttämättä beacon-sanomia ja antaa verkkolaitteen lähettää CSMA-CA-kilpavarausmenetelmää käyttäen dataa sitä mukaa, kun sillä (harvakseltaan) on lähetettävää. Beacon-sanomat ovat kuitenkin välttämättömiä verkonmuodostamisessa. IEEE 802.15.4 -standardi tukee myös niitä sovelluksia, joissa beacon-sanomia ei muuten käytetä.

Kun verkkolaitteen MAC-kerros vastaanottaa PAN-koordinaattorin generoiman beacon-sanoman, se tarkistaa löytyykö sen laiteosoite beacon-kehyksen osoitekentästä. Mikäli laitteen osoite on listattu, se lähettää data.request-pyynnön PAN-koordinaattorille. FFD-laitteet peer-to-peer-verkossa voivat myös generoida beacon-viestejä naapurilaitteille. Niiden avulla ilmaistaan laitteen olemassaolo naapurille, jonka jälkeen voidaan vaihtaa tarvittavat parametrit laitteiden välillä esimerkiksi verkonmuodostusta varten. [4]

3.6.6 Tietoturva

Keskeinen asia tietoturvan kannalta on kehysten turvallisuus, mitä hallinnoi MAC-kerroksella MAC PIB. Barretin *ym.* [4] mukaan MAC-kerros tarjoaa ylemmille kerroksille useita tietoturvaan liittyviä palveluita:

- Laitetunnistus, laitteella on MAC-kerroksellaan tieto, kenen kanssa sillä on lupa viestiä.

- Tiedon salaus, missä salaus perustuu symmetrisen salausavaimen käyttöön. Siten vain ne laitteet, joilla on avain pääsevät käsiksi verkossa liikkuvaan dataan. Salaus koskee beacon-, komento- ja datakehyksiä. Muut viestit lähetetään salaamatta (esimerkiksi kuittausviestit).

- Tiedon eheys, vastaanottava laite pystyy varmistamaan salauskoodin (Message Integrity Code, MIC) avulla, että vieras laite ei ole muuttanut viestiä. Samalla se varmistuu siitä, että sanoma tulee salausavaimen omistavalta laitteelta. Tämän oletetaan olevan yksi eniten käytettyjä tietoturvaan liittyviä asetuksia LR-WPAN-verkoissa. Näissä verkoissa kulkeva tieto ei useinkaan ole salaista, sen sijaan on tärkeää pystyä varmistamaan, että tieto tulee oikeasta lähteestä, eikä ole matkalla luvattomasti muuttunut.

- Identtisten päällekkäisten viestien estäminen, MAC-kerroksella pystytään seuraamaan sanomia myös sekvenssinumeron mukaan. Uudelleenlähetystapauksissa voidaan näin hylätä jo kertaalleen lähetetyt identtiset sanomat.

IEEE 802.15.4 -standardi tasapainoilee tietoturvan määrityksissä pitääkseen tietoturvan riittävällä tasolla, mutta samalla sovellusten toteuttamisen riittävän yksikertaisena. Niinpä se tarjoaa sovelluksille kolme erilaista tietoturvaluokkaa, joista ne voivat valita omiin tarpeisiinsa soveltuvimman. Unsecured Mode -luokka on tarkoitettu sovelluksille, jotka eivät tarvitse mitään yllämainituista tietoturvapalveluista. ACL (Access Control List) -luokka on tunnistuspalvelu, missä MAC ylläpitää tietoja laitteista, joiden kanssa se saa viestiä. Se vertaa saapuneiden viestien osoitekenttää tähän listaan ja välittää viestin mukana ylemmille kerroksille tiedon lähettäjän statuksesta. Ylemmät kerrokset päättävät, hylkäävätkö viestit, jotka saapuvat listaan kuulumattomilta lähettäjiltä. Lähettäjän osoite on kyllä mahdollista väärentää, koska viestit kulkevat salaamatta. Secured Mode -luokassa

voidaan käyttää kaikkia yllämainittuja neljää tietoturvamekanismia erilaisina yhdistelminä. [4]

4 Verkonmuodostus ja -hallinta

Kuten edellisessä luvussa todettiin, IEEE 802.15.4 -standardi ei määrittele verkonmuodostuksen yksityiskohtia, ainoastaan MAC-kerroksen tuen sille. Verkonmuodostus tapahtuu MAC-kerroksen yläpuolisilla tasoilla ja tässä luvussa tuodaan esiin niitä standardin ulkopuolisia asioita, jotka suunnittelijan on otettava huomioon muodostettaessa ja hallitessa IEEE 802.15.4 -standardin mukaista sensoriverkkoa.

Langaton sensoriverkko on tyypillisesti sovellus, jossa verkon solmuina eli noodeina toimivat laitteet keräävät mittaustietoa, mahdollisesti käsittelevät sitä kevyesti ja lähettävät sen eteenpäin PAN-koordinaattorille eli tukiasemalle radiotietä pitkin. PAN-koordinaattori kerää lähetetyn tiedon, analysoi sitä ja tekee yhteenvetoja ja päätelmiä verkon mittaamasta kohteesta. Useimmiten langattoman sensoriverkon luonteeseen kuuluu myös tiedonsiirto monelta laitteelta yhdelle laitteelle. Tämä johtaakin laitteiden epätasaiseen rasitukseen ja energiankulutukseen. [30]

Ad hoc -verkko koostuu laitteista, jotka osaavat viestiä langattomasti toistensa kanssa. Ad hoc -verkosta puuttuu kiinteä rakenne ja linkitykset. Solmut etsivät dynaamisesti reittejä ja solmuja, joiden kanssa ja kautta ne voivat viestiä. Avainoletus ad hoc -verkossa on se, että kaikki solmut eivät voi suoraan keskustella toistensa kanssa, siten yksittäisen solmun vastuulle kuuluu myös toisten solmujen viestien välittäminen. Keskeinen ominaisuus ad hoc -verkoille on solmujen liikkumisesta ja lähetystehon vaihteluista johtuvat nopeat muutokset topologiassa sekä linkkien ja yhteyksien ominaisuuksissa. Ad hoc -verkon tyypillinen sovellus voisi olla esimerkiksi liikkuvien kannettavien tietokoneitten, pda-laitteiden ja/tai älypuhelimien muodostama verkko, jossa laitteet voivat keskustella keskenään ilman kiinteää infrastruktuuria. [32]

Osittaisesta samankaltaisuudesta huolimatta ad hoc -verkoilla ja sensoriverkoilla on joitakin keskeisiä eroja. Laitteiden määrä sensoriverkossa voi olla aivan eri suuruusluokkaa, kuin ad hoc -verkoissa ja laitteet voivat olla myös hyvin tiheään sijoiteltuja. Näin ollen kaikilla sensoriverkon laitteilla ei ole välttämättä omaa globaalia ID-tunnistetta. Sensoriverkon laitteiden paristonkesto sekä tiedonkäsittely- ja muistikapasiteetti ovat rajattuja ja toteutuksessa on varauduttava siihen, että verkon

topologia voi muuttua jatkuvasti laitteiden poistumisen ja uusien liittymisen myötä. Laitteet kuitenkin pysyvät yleensä paikoillaan, kun taas ad hoc -verkon laitteet ovat usein liikkuvia. Sensoriverkot viestivät useimmiten yleislähetyksen (broadcasting) avulla. Liikennöinti voi olla hyvinkin harvaa pitkän aikaa, mutta jokin tapahtuma voi laukaista erittäin vilkkaan liikenteen. Tämä ilmiö tunnetaan ”tapahtumasuihkuna” tai ”hälytysmyrskynä” [22]. Ad hoc -verkot käyttävät enemmän point-to-point-viestintää. Keskeisin ero ad hoc- ja sensoriverkoilla on sensoriverkkojen resurssien vähyys ja laitteiden yksinkertaisuus. Verkonhallintaprotokollat ovat yleensä tehty järeämmille laitteille kuin sensoriverkossa käytetään. Niinpä langattomiin ad hoc -verkkoihin suunnitellut tekniikat ja protokollat eivät välttämättä sovellu langattomiin sensoriverkkoihin sellaisenaan. [1] [34]

Tähtimäisessä verkossa IEEE 802.15.4 -standardi määrittelee laitteiden liittymisen verkkoon assosiaation avulla [4]. Reititysongelmia ei tähtiverkossa myöskään ole, koska data liikkuu aina yhden laitteen ja sinkin eli PAN-koordinaattorin välillä. Superframe-rakenteen avulla PAN-koordinaattorin on mahdollista hallinnoida tiedonsiirtoa laitteiden ja itsensä välillä. Peer-to-peer-verkon suunnitteluprosessissa joudutaan kiinnittämään erityistä huomiota muun muassa topologian hallintaan, tiedonkulkuun ja tiedonkäsittelyyn.

Langattomien sensoriverkkojen muodostamiseen ja hallintaan liittyviä menetelmiä on viime vuosina esitelty lukuisia. Klusterointi-, reititys- ja datansiirtomenetelmien avulla pyritään mahdollisimman pitkäikäiseen verkkoon pitämällä verkon topologia hallittuna sekä laitteiden energiankulutus mahdollisimman alhaisena ja tasaisena laitteiden kesken. Samoin pyritään luotettavaan ja mahdollisimman häiriöttömään tiedonsiirtoon laitteiden välillä. Menetelmien valintaan vaikuttavat esimerkiksi verkon laitteiden ominaisuudet, ovatko laitteet keskenään samanlaisia vai erilaisia, sensoriverkon maantieteellinen laajuus ja laitteiden lukumäärä verkossa sekä sovelluksen asettamat vaatimukset ja sovellusympäristö.

4.1 Topologian hallinta

Langattoman sensoriverkon tiheän rakenteen avulla saadaan tutkittava alue hyvin katettua ja verkon toimintavarmuus on korkeampi, koska rikkoutuneille solmuille löytyy helposti korvaaja. Tiheä rakenne kuitenkin myös korostaa joitakin sensoriverkoille tyypillisiä ongelmia. Solmun asteen kasvaessa tiedonkulun häiriöt lisääntyvät. Solmun asteeksi kutsutaan solmun naapureiden määrää tietyllä alueella. Laitteet joutuvat käyttämään tarpeettoman paljon energiaa keskustellessaan kaukaisempien solmujen kanssa tuhlaten samalla käytettävissä olevaa kaistanleveyttä. Reititys monimutkaistuu mahdollisten reittien lisääntyessä ja reitit joudutaan laskemaan uudelleen, mikäli yksittäisessä solmussa tapahtuu pienikin muutos. Joitakin näistä ongelmista pystytään vähentämään topologian hallinnan avulla, missä tarkoituksella rajoitetaan aktiivisten solmujen ja linkkien toimintaa. [22]

Santin [34] mukaan sensoriverkon topologian hallinnan tavoitteena on saada sensoriverkkoon halutut ominaisuudet koordinoimalla solmujen toiminta-alueita (Transmitting Range), samalla vähentäen solmujen virrankulutusta ja/tai nostaen verkon tiedonsiirtokapasiteettia.

Karl *ym.* [22] esittelee kolme vaihtoehtoa topologian hallintaan:

1. Aktiivisten solmujen määrää vähennetään esimerkiksi sammuttamalla osaksi aikaa virta laitteista, joilla on matala energiavarasto ja aktivoimalla saman alueen muita solmuja hyödyntäen näin laitteiden tiheää sijoittelua.

2. Aktiivisten linkkien ja aktiivisten naapureiden määrää rajoitetaan ja ohjataan viestintä vain tietyille naapureille ja tietyille linkeille. Tasaisessa verkossa, missä kaikki laitteet ovat samanarvoisia, rajoitetaan viestintää naapureiden kanssa esimerkiksi säätämällä lähetystehoa tai mukauttamalla modulointimenetelmiä (nopeammat modulointimenetelmät ovat mahdollisia vain lyhyillä etäisyyksillä).

3. Aktiiviset solmut ja linkit voidaan järjestää hierarkkisesti, jolloin joillakin solmuilla on erityisrooli. Osa solmuista voidaan valita esimerkiksi verkon rangaksi ja muille solmuille sallitaan linkit ainoastaan rankaan kuuluviin solmuihin. Toinen esimerkki hierarkkisesta rakenteesta on klusterointi, jota on käsitellään luvussa 4.3.

Santi [34] jakaa topologian hallintamenetelmät yhtenäisiin (homogeneous) ja epäyhtenäisiin (nonhomogeneous) riippuen siitä pystyvätkö verkon laitteet itse vaikuttamaan toiminta-alueeseensa. Yhtenäisissä menetelmissä kaikkien verkon solmujen toiminta-alue on samankokoinen, kun taas epäyhtenäisissä menetelmissä verkon laitteille on sallittu toiminta-alueen mukauttaminen sallituissa rajoissa.

4.1.1 Yhtenäinen toiminta-alue

Mikäli verkon kaikilla laitteilla on yhtä suuri toiminta-alue, nousee keskeisimmäksi kysymykseksi se, mikä on laitteen pienin mahdollinen toiminta-alue, jotta sensoriverkko säilyy yhtenäisenä. Tästä käytetään nimeä CTR (Critical Transmitting Range). Sensoriverkon laitteet voidaan levittää myös satunnaisesti tietylle alueelle. Tällöin CCR (Critical Coverage Range) määrittelee pienimmän mahdollisen solmun toiminta-alueen, mikä tarvitaan kattamaan tämä alue. CCR:ää voidaan käyttää myös käänteisesti, eli arvioidaan, montako laitetta tietylle alueelle täytyy levittää, jotta alue on kokonaan katettu. [34]

4.1.2 Epäyhtenäinen toiminta-alue

Sensoriverkon solmut pystyvät usein vaikuttamaan omaan toiminta-alueeseensa lähetystehon säätelyllä. Tällaisessa verkossa on tärkeää miettiä solmujen käyttämä optimaalinen energiataso toiminta-alueen määrittämisessä suhteessa verkon yhtenäisyyden säilymiseen. Tätä ongelmaa kutsutaan RA-ongelmaksi (Range Assignment -ongelma). Mikäli sinkillä on tieto solmujen sijainnista, voi se laskea solmuille optimaalisen toiminta-alueen. Käytännön sensoriverkkosovelluksissa keskitetty tieto solmun sijainnista ei kuitenkaan ole itsestäänselvyys. Santi [34] esittelee kolme eri lähestymistapaa verkon solmujen sijainnin ylläpitoon: sijaintiin perustuvat (location-based) protokollat, suuntaan perustuvat (direction-based) protokollat sekä naapureihin perustuvat (neighbor-based) protokollat. Sijaintiin perustuvissa protokollissa jokainen solmu tietää oman sijaintinsa. Suuntaan perustuvissa protokollissa solmut eivät tunne omaa sijaintiaan, mutta pystyvät arvioimaan suunnan naapurisolmuun. Naapurimenetelmissä solmu tietää ainoastaan naapureidensa tunnisteet ja lukumäärän.

4.1.3 Hyvän topologianhallintaprotokollan ominaisuuksia

Koska verkon keskitetty hallinta usein puuttuu langattomista sensoriverkoista, hyvän topologianhallintaprotokollan tulee olla täysin hajautettua eli solmu pystyy rakentamaan tarvitsemansa tiedon verkon topologiasta täysin paikallisesti, käyttämällä hyväkseen muutamasta naapurisolmusta saamiansa tietoja. Paikallisuuden hyväksikäyttäminen on välttämätön ratkaisu esimerkiksi laajoissa verkoissa. Se myös helpottaa verkon uudelleenmuodostamista solmujen liittyessä verkkoon tai erotessa verkosta. Samoin pienet muutokset yksittäisten solmujen polkujen kohdalla eivät saisi heijastua koko verkkoon. Hyvä topologianhallintaprotokolla säilyttää verkon yhtenäisyyden sekä solmujen välisten linkkien kaksisuuntaisuuden, jota edellyttää myös useat standardit, kuten IEEE 802.15.4. Edelleen hyvä topologianhallinta luo ja säilyttää topologian, jossa solmujen asteet ovat pienet häiriöttömän tiedonkulun edistämiseksi. Sen täytyy myös olla hyvin kevyt toteuttaa, jotta se ei itsessään rasita verkkoa. [34] [22]

Verkon topologian muuttuessa linkkien vähentäminen lisää todennäköisesti polun pituutta verkossa joidenkin solmujen välillä. Hop stretch factor määrittelee polun pituuden lisäyksen kahden solmun välillä pahimman tapauksen mukaan. Vastaavasti energy stretch factor määrittelee polun energiankulutuksen lisäyksen kahden solmun välillä pahimman tapauksen mukaan. Tavoiteltavaa onkin siis pitää molemmat stretch factorit alhaisena. Sensoriverkon täytyy myös pystyä ylläpitämään samansuuruista liikennettä linkkien vähenemisen jälkeenkin. [22]

Solmujen käyttämän tiedon laatu voidaan jakaa kolmeen tasoon: korkealaatuiseen (esimerkiksi informaatio naapurisolun sijainnista), keskilaatuiseen (esimerkiksi informaatio naapureiden etäisyyksistä ja suunnista) sekä matalalaatuiseen (naapurisolmujen tunniste ja lukumäärä). Tiedon laadun taso on käänteisesti suhteessa tiedonkäsittelyn energiakulutukseen, mitä korkeampi laatu, sen matalampi energiankulutus. Säästö energiankulutuksessa täytyy kuitenkin olla merkittävä ennen kuin sitä kannattaa suosia, koska korkeampilaatuinen tieto edellyttää laitteelta monimutkaisempaa tiedonkäsittelykykyä ja/tai mahdollisesti lisälaitteita, esimerkiksi GPS-antennia, ja siten nostaa yksittäisen laitteen hintaa. Matalalaatuista informaatiota käyttäviä protokollia voidaan myös hyödyntää laajemmin kuin korkeampilaatuista käyttäviä. Esimerkiksi

sijaintiin perustuvat tekniikat eivät sovellu sisätiloihin johtuen radiosignaalin vaikeasti ennustettavasta leviämisestä. Yleisesti suositellaankin matalalaatuisen informaation hyödyntämistä topologianhallintaprotokollissa. [34] [22]

4.2 Datansiirtomenetelmät

Peer-to-peer-verkoissa voidaan datan siirtoon käyttää singlehop-menetelmää, jossa laite kommunikoi suoraan kohdelaitteen kanssa tai multihop-menetelmää, jossa data kulkee lähteestä kohteeseen muiden verkon laitteiden kautta. Santin [34] mukaan tiedonsiirto käyttäen multihop-polkuja on energiatehokkaampaa kuin yksi pitkä singlehop-polku. Tyypillisesti sensoriverkkosovellukseen valitaan jompikumpi tiedonsiirto-menetelmä, mutta myös näiden yhdistelmä on mahdollinen. Sensoriverkossa täytyy myös määritellä lähettävätkö solmut tietoa sinkille säännöllisin väliajoin vai tapahtumaperusteisesti eli vain silloin, kun tapahtuu jotain. [29]

4.2.1 Singlehop -menetelmä

Singlehop-menetelmässä on selvää, että kaikkien niiden laitteiden, jotka kommunikoivat keskenään, on oltava samalla kuuluvuusalueella. Klusteriverkossa laitteet voivat lähettää tiedon ryhmänsä pääsolmulle (cluster head) singlehop-menetelmällä ja pääsolmu puolestaan välittää viestin sinkille samoin singlehop-menetelmää käyttäen. Mikäli verkon laitteet ovat samanlaisia, voi pääsolmun roolia kierrättää ryhmän sisällä, jolloin minkään ryhmän laitteen energiankulutus ei nouse liian suureksi kuten Bhardwaj *ym.* [6] ovat esittäneet. Tällöin tietysti kaikkien laitteiden täytyy pystyä toimimaan pääsolmuina, mikä osaltaan voi nostaa laitekustannuksia. [29]

4.2.2 Multihop-menetelmä

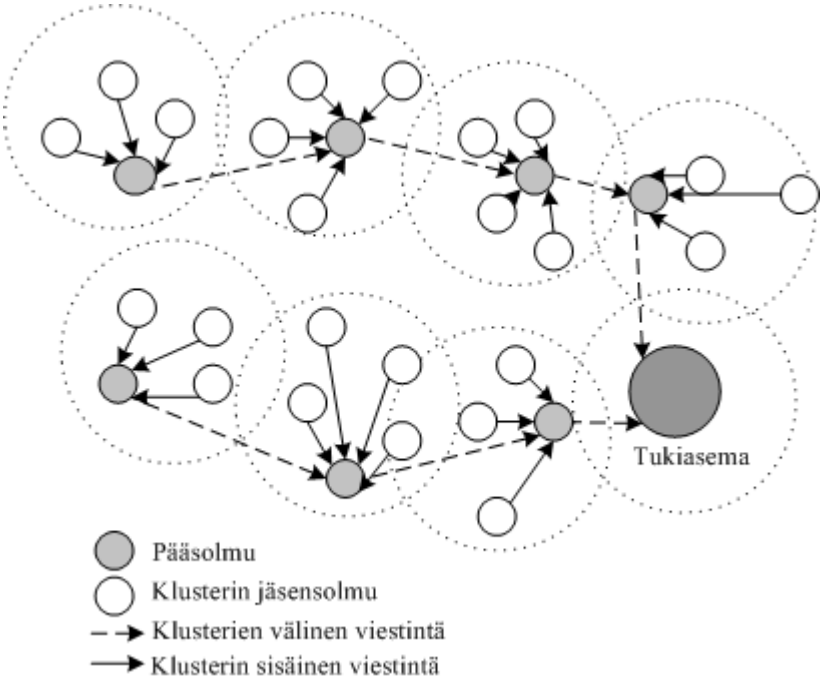
Multihop-menetelmässä tieto kulkee lähdelaitteelta pääsolmulle muiden laitteiden kautta. Multihop-verkossa suurimman rasituksen kohteena ovat sinkkiä lähinnä olevat laitteet, koska kaikkien muiden kauempana sijaitsevien laitteiden lähettämä tieto kulkee niiden kautta. Samoin tällainen verkko on haavoittuva, jos sinkkiä lähinnä olevat laitteet rikkoutuvat, on koko verkko toimintakyvytön. [29]

4.2.3 Yhdistelmä

Mhatre ja Rosenberg [29] esittelevät hybridimallin, jonka avulla voidaan optimoida energiankulutus ja kustannukset datansiirtoon liittyen. Siinä datan siirto vaihtelee singlehop- ja multihop -menetelmien välillä. PAN-koordinaattori lähettää säännöllisesti beacon-sanoman verkon solmuille ja määrää vaihtamaan datansiirtomallin. Siirryttäessä singlehop-menetelmästä multihop-menetelmään, kaukana sinkistä sijaitsevat solmut vapautetaan pitkistä datan lähetysmatkoista. Siirryttäessä takaisin singlehop-menetelmään lähellä sinkkiä sijaitsevat solmut vapautuvat datan välitysvelvollisuudestaan.

4.3 Klusterointi

Useissa sensoriverkkosovelluksissa riittää, että tukiasemalle siirretään vain tarpeellinen tieto, ei kaikkea kerättyä tietoa. Esimerkiksi mitattaessa alueen radioaktiivisuutta, riittää mitattu maksimiarvo. Jossain toisessa sovelluksessa tärkein tieto voi olla mittauksien keskiarvo. Kaiken tiedon siirtäminen ja tiedonkäsittely vasta tukiasemassa ruuhkauttaa turhaan sensoriverkkoa ja lisää energiankulutusta lyhentäen näin sensoriverkon elinkaarta. Verkon solmut kannattaakin jakaa ryhmiin, klustereihin, joissa tietoa voidaan tehokkaasti käsitellä ja mittaustuloksia yhdistellä ennen sen lähettämistä tukiasemalle. Ryhmän pääsolmu kerää datan klusterin muilta jäsensolmuilta, käsittelee sen ja lähettää käsitellyn tiedon tukiasemalle suoraan tai muiden pääsolmujen kautta. Pääsolmu voi käsitellä ja yhdistää jäseniltä saamiinsa tietoihin myös muilta pääsolmuilta saadut tiedot kuvan 14 mukaisesti. Koska pääsolmut kuluttavat enemmän energiaa verrattuna verkon muihin solmuihin, kannattaa sensoriverkko klusteroida uudelleen säännöllisesti, jolloin pääsolmuiksi valitaan sellaiset laitteet, joiden energiataso on korkea. Klusterointi vähentää myös ruuhkaa ja pakettien törmäyksiä radiotiellä, joten se on varsin tehokas tapa organisoida sensoriverkko. [24]



Kuva 14. Tiedonsiirto klusteriverkossa.

4.3.1 Klusterointitekniikat

Langattomien sensoriverkkojen klusteroinnissa on paljon haasteita, kuten kuinka varmistetaan yhteyden säilyminen kaikissa tilanteissa, kuinka usein pääsolmun roolia tulisi kierrättää, mikä on klusterin ihannekoko sekä klusteroinnin tapahtuminen solmun aktiivisen ajan (duty cyclen) aikana.

Klusterointitekniikkaa valittaessa täytyy ottaa huomioon sensoriverkkojen erityispiirteet kuten [24]

- laitteiden tiheä sijoittelu ja suuri määrä,
- laitteet eivät välttämättä ole tietoisia sijainnistaan, joten klusterointiprotokollan tarvitseman sijainnin määrityksen täytyy perustua laitteen naapurustoon,
- sensoriverkkojen energiakulutus on usein kriittinen asia, joten klusteroinnin täytyy tapahtua pienellä energiamäärällä,

- uudelleenklusterointi on skaalautuvuuden kannalta välttämätöntä. Sensoriverkossa laitteet saattavat lakata toimimasta tai uusia laitteita voi liittyä verkkoon. Klusteroinnin perusteena käytettävät parametrit kuten energian määrä tai solmun aste ovat myös muuttuvia.

4.3.2 Pääsolmun valinta

Klusteroinnissa verkon solmut jaetaan siis ryhmiin ja jokaiselle ryhmälle valitaan pääsolmu, cluster head. Klusterin kaikkien jäsenten täytyy pystyä kommunikoimaan pääsolmunsa kanssa ja pääsolmun täytyy pystyä lähettämään käsittelemänsä data tukiasemalle, ainakin muiden pääsolmujen kautta. Artikkeli [24] jakaa pääsolmujen valintaperusteet neljään luokkaan.

1. Pääsolmujen valintaperuste voi olla satunnainen, esimerkiksi solmujen ID-tunnukseen perustuva. Pääsolmuksi voidaan suosia esimerkiksi pienen ID-tunnuksen omaavia solmuja. Tämän tyyppistä menetelmää käytettäessä edellytetään tietysti, että jokaisella solmulla on globaali ID ja että ID-tunnukset on jaettu tasaisesti verkossa. Tällaiset menetelmät eivät sovellu hyvin sensoriverkkosovelluksiin, jotka ovat kriittisiä energiankulutuksen suhteen, koska pääsolmun valinnassa ei huomioida solmun energiamäärää.

2. Solmun aste voi olla määräävä parametri pääsolmun valinnassa. Tämän menetelmän haittapuolena on suuriasteisten solmujen suuri energiakulutus. Tasoittamalla klustereitten koot vähennetään pääsolmun rasitusta, mutta samalla klustereitten määrä lisääntyy ja reititys monimutkaistuu.

3. Pääsolmu voidaan valita myös tietyn parametrin arvon mukaan tai useiden parametrien yhdistelmällä. Näitä parametreja voivat olla esimerkiksi jäljellä olevan energian määrä solmussa, solmun aste tai keskimääräinen etäisyys naapureista.

4. Pääsolmun valinnassa voidaan hyödyntää solmujen runsautta samalla alueella. Muut solmut nukkuvat, kun yksi ryhmän solmu hoitaa reitityksen

vuorollaan omalla alueellaan. Tämä edellyttää tietysti sitä, että jokainen solmu *u* alueella A pystyy kommunikoimaan viereisen B-alueen jokaisen solmun *v* kanssa. Vaikka tämäntyyppiset menetelmät eivät ole varsinaisia klusterointimenetelmiä, niiden vaikutus verkon topologiaan on samankaltainen.

4.3.3 Klusterin koko ja niiden määrä

Pääsolmun valinnan lisäksi täytyy päättää klustereitten määrä verkossa ja siten klustereitten koko. Tämä voidaan hoitaa keskitetysti esimerkiksi tukiaseman koordinoimana, tai vastuu klusterin koosta voi olla jaettu solmuille itselleen. Mikäli tukiasema päättää klusteroinnista, täytyy sillä olla globaali tieto verkon topologiasta. Keskitetyssä klusteroinnissa voidaan käyttää esimerkiksi klassista MacQueenin [27] K-means-algoritmia, mikäli solmujen sijainti on tiedossa ja klustereitten määrä voidaan päättää ennalta. K-means-algoritmissa klusterikeskukset arvotaan verkkoon tasaisesti ja solmut liittyvät lähimpään klusterikeskukseen. Sitten klusterikeskus siirretään klusterin keskelle ja solmujen lähimmät klusterikeskukset tarkistetaan uudelleen. Kun klustereitten rakenne ei enää muutu, algoritmi lopetetaan. Suurissa verkoissa keskitetty klusterointi ei ole tehokasta, koska se vie paljon aikaa ja energiaa. Niissä kannattaakin usein suosia hajautettua klusterointia, missä solmut itse päättävät klusteriin liittymisestään paikallisen informaation perusteella. [24]

Hajautetut klusterointimenetelmät voidaan jakaa luonteeltaan joko iteratiivisiin tai satunnaisiin. Iteratiivisissa menetelmissä solmut odottavat tiettyä tapahtumaa, ennen kuin päättävät omasta klusteristaan. Ne voivat esimerkiksi antaa naapurisolmun päättää asiasta ensin, mikäli sen paino on suurempi. Solmun painolla tarkoitetaan tässä tietyn parametrin arvoa, esimerkiksi energiatasoa. Iteratiivisten menetelmien haasteena on klusteroinnin nopeuden riippuminen verkon halkaisijasta, eli pisimmästä polusta, sekä herkkyys virheille. Esimerkiksi jos solmu *u* odottaa painavamman naapurisolmun *v* päätöstä ja solmu *v* lopettaa toimimisen heti, kun on ilmoittanut painonsa solmulle *u*, solmu *u* voi jäädä odottamaan määrittelemättömäksi ajaksi. Satunnaisissa menetelmissä jokainen solmu päättää itsenäisesti liittymisestään klusteriin. Tämän menetelmän avulla klustereitten koot

saadaan tasaiseksi ja klusterointi voi olla nopeaa, koska klusteroinnissa saatetaan selvitä vain yhdellä iterointikierroksella. Luvussa 5 esitellään HEED-protokolla esimerkkinä satunnaisesta klusterointimenetelmästä. [24]

4.4 Homogeeninen vs. heterogeeninen verkko

Homogeeninen verkko koostuu energiankulutukseltaan ja monimutkaisuudeltaan keskenään identtisistä laitteista, kun taas heterogeenisessä verkossa voi olla kahden tai useamman tyyppisiä laitteita. IEEE 802.15.4 -standardin mukaisissa toteutuksissa homogeenisissä verkoissa on ainoastaan FFD-laitteita ja heterogeenisissä voi olla mukana myös RFD-laitteita. [30]

Homogeenisessa verkossa klusterin pääsolmu voidaan äänestää ja pääsolmun rooli voi olla myös kiertävä ryhmän laitteiden välillä. Kierrättämällä pääsolmun roolia päästään tasaisempaan energiankulutukseen laitteiden välillä, mutta täytyy huomioida, että energiaa kuluu myös pääsolmuäänestykseen. Staattisessa homogeenisessa verkossa pääsolmu pysyy samana koko verkon elinkaaren ajan. [30]

Heterogeeninen verkko muodostuu energiankulutukseltaan ja monimutkaisuudeltaan vähintään kahdentyyppisistä laitteista: yksinkertaisista sensorilaitteista ja pääsolmuiksi kelpaavista monimutkaisemmista laitteista. Koska pääsolmun ominaisuudet ja korkeampi energiankulutus keskitetään tietyille laitteille, saadaan laitekustannukset alhaisemmiksi verkon muissa laitteissa. Äänestysprotokollaa ei myöskään tarvita pääsolmun valitsemiseksi, koska pääsolmua ei kierrätetä. Mikäli heterogeenisessä verkossa käytetään singlehop-menetelmää, kauimpana pääsolmusta sijaitsevien laitteiden energiankulutus kasvaa, koska niiden täytyy käyttää suurempaa lähetystehoa. Multihop-menetelmää käytettäessä pääsolmua lähinnä olevien laitteiden energiankulutus kasvaa siitä syystä, että ne joutuvat välittämään enemmän dataa pääsolmulle kuin kauempana sijaitsevat laitteet. Verkon laitteiden energiankulutusta ei siis koskaan saada täysin tasaiseksi. [30]

Langattoman sensoriverkon kaksi suurinta haastetta ovat siis madaltaa laitekustannuksia ja saada laitteiden energiankulutus alhaiseksi ja keskenään samantasoiseksi. Heterogeenisen verkon avulla voidaan madaltaa laitekustannuksia ja homogeeninen verkko puolestaan

tukee tasaisempaa energiankulutusta [30]. Krishnamacharin [23] mukaan heterogeenisten verkkojen haasteena on usein löytää laitteiden optimaalinen kombinaatio, jotta muut verkolle asetetut vaatimukset täyttyvät.

4.5 Reititys sensoriverkoissa

Multihop-menetelmää käyttävässä sensoriverkossa tieto kulkee lähettäjältä vastaanottajalle usean välittäjäsolmun kautta. Välittäjäsolmun täytyy päättää, kenelle se viestin välittää, mikäli se itse ei ole vastaanottaja. Reititykseen vaikuttaa myös se onko paketin vastaanottajaksi määritelty yksittäinen solmu, ryhmä solmuja vai kaikki verkon solmut. Tietoa naapurisolmujen sopivuudesta seuraavaksi välittäjäsolmuksi ylläpidetään reititystauluissa. Reititysprotokollan tärkein tehtävä onkin näiden taulujen rakentaminen ja ylläpitäminen. Karl *ym.* [22] pitää yleisimpänä haasteena kaikissa reititysprotokollissa ohjausviestien runsautta verkon topologian tutkimisessa ja kohteiden löytämisessä.

Luotettavuuden, oikeudenmukaisuuden, vakauden ja optimaalisuuden lisäksi Hać:n [14] mukaan langattoman sensoriverkon hyvä reititysprotokolla käyttää vähän energiaa, on skaalautuva solmujen lukumäärän ja verkon topologian suhteen sekä sietää hyvin solmujen toimintatilan muutoksia. Reititysprotokollan tulee osaltaan varmistaa myös se, että verkon toimintakyky säilyy mahdollisimman pitkään. Mikäli reititysprotokolla keskittyy vain optimaalisen polun löytämiseen, kuluttaa se energiaa eniten näiden polkujen varrella ja vaarantaa verkon säilymisen yhtenäisenä. Siten on usein tarpeen etsiä useampia mahdollisia reittejä vastaanottajalle. Matala ja tasainen virrankulutus on siis myös hyvän reititysprotokollan keskeisin ominaisuus. Reititysprotokollaa suunniteltaessa on pidettävä mielessä myös sensoriverkon laitteiden rajallinen muistikapasiteetti, taulut eivät saa paisua liian suuriksi. Luonnollisesti reititysprotokollaa suunniteltaessa täytyy muistaa, että sensoriverkot käyttävät radiolähetystä, joten protokollan täytyy toimia luotettavasti ja tehokkaasti vaikka lähetysolosuhteet ja -ympäristö ovat jatkuvassa muutoksessa. Hyvä reititysprotokolla vähentää myös osaltaan verkon kuormitusta rajaamalla esimerkiksi uudelleenlähetyksiä. [16]

Hu *ym.* [16] jakaa reititysprotokollat topologiaperusteisiksi tai sijaintiperusteisiksi. Topologiaperusteiset protokollat valitsevat reitin perustuen topologiseen informaatioon kuten solmujen välisiin linkkeihin. Sijaintiperusteiset perustavat reitinvalinnan maantieteellisen informaatioon. On myös reititysprotokollia, jotka yhdistävät em. informaationlähteet. Topologiaperusteiset protokollat voidaan edelleen jakaa Royerin *ym.* [33] mukaan proaktiivisiin eli taulukkopohjaisiin (table-driven) ja reaktiivisiin eli dynaamisiin (on-demand) protokolliin. Proaktiiviset protokollat pitävät reititystauluja yllä koko ajan eli jokaisessa solmussa on ajantasainen reititystieto kaikkiin verkon solmuihin. Reaktiiviset protokollat laskevat sopivia reittejä vain tarvittaessa, kun kohteelle ei ole reititystietoja saatavilla. Reaktiivisten menetelmien vahvuus on ohjausviestien väheneminen, koska reititystauluja ei tarvitse ylläpitää koko ajan. Toisaalta menetelmä aiheuttaa viivettä uutta reittiä laskettaessa. Proaktiviisissa menetelmissä viivettä ei esiinny, mutta käyttämättömien reittien ylläpito reititystauluissa kuormittaa turhaan. On olemassa myös protokollia, jotka poimivat molempien menetelmien hyödyt. Nämä hybridiprotokollat pitävät reititystietoja yllä lähellä sijaitseviin solmuihin sekä usein käytetyillä poluilla. Kauempana sijaitseviin tai harvoin käytettäviin kohteisiin lasketaan reitit tarvittaessa.

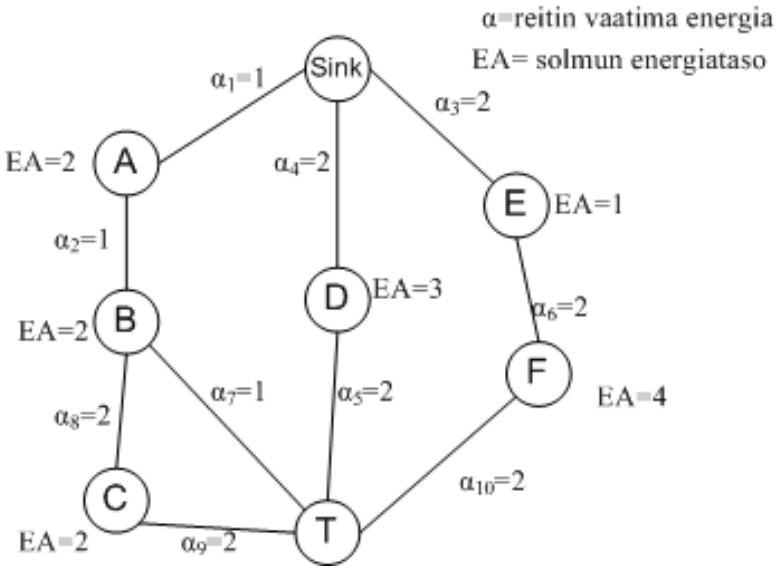
Estrin *ym.* [11] luokittelee reititysmenetelmät osoitekeskeisiin (address-centric) ja datakeskeisiin (data-centric) menetelmiin. Osoitekeskeisissä menetelmissä lähettäjä lähettää paketin vastaanottajalle itsenäisesti lyhintä reittiä pitkin. Datakeskeisissä menetelmissä reitin varrella olevien solmujen on mahdollista tutkia lähetettävää dataa ja tarvittaessa yhdistellä tietoja eri lähteistä ennen välittämistä eteenpäin. Langattomien sensoriverkkojen sovellukset ovat usein kiinnostuneita ilmiöistä yksittäisten tietojen sijaan. Esimerkiksi alueet, joissa radioaktiivisuus nousee yli sallitun, on kiinnostavampi tieto kuin yksittäisten sensoreiden mittaustulokset. Niinpä langattomissa sensoriverkoissa datakeskeinen lähestymistapa on usein mielekkäämpää [1]. Datakeskeisyyteen liittyy Estrinin *ym.* [10] esittelemä Directed diffusion, joka on enemmän suunnittelufilosofia kuin varsinainen reititysprotokolla. PAN-koordinaattori ilmaisee kiinnostuksensa eli julkaisee kyselyn (interestin) tietynlaiseen nimettyyn dataan. Kun solmu vastaanottaa kyselyn, se tallentaa sen tietyksi ajaksi välimuistiinsa ja suuntaa gradientin takaisinlähetystä varten.

Mikäli solmu havaitsee dataa, joka vastaa kyselyä, se lähettää datan gradienttia pitkin takaisin.

Reititysprotokollia voidaan luokitella myös useilla muilla tavoilla, kuten esimerkiksi tasainen verkko - hierarkkinen verkko, linkin etäisyys - linkin tila, kohdeperusteinen - naapuriperusteinen tai yksipolkuinen - monipolkuinen reititysmenetelmä. Protokollat voidaan luokitella myös verkon käyttökohteen mukaan. [16]

4.5.1 Reititysstrategioita

Tulviva reititys (flooding) lienee alkeellisin pakettien välitysstrategia. Siinä välittäjäsolmu lähettää viestin kaikille naapureilleen ja jossain vaiheessa viesti saavuttaa vastaanottajasolmun. Toinen alkeellinen strategia on satunnainen välitystapa (gossiping), missä välittäjäsolmu lähettää viestin satunnaiselle naapurille ja viesti toivottavasti joskus päätyy vastaanottajalle. Välittäjäsolmu välittää eteenpäin vain ne paketit, joita ei ole vielä aikaisemmin sen kautta kulkenut. Näin estetään paketin loputon kulkeminen verkossa. Useimmiten paketteihin merkitään myös voimassaoloaika, minkä kuluessa vastaanottajan täytyy olla tavoitettu. Esimerkiksi niitä tapauksia varten, kun vastaanottajasolmu ei ole saavutettavissa. Kiinteä strategia määrittelee kiinteät reitit solmuparien välille. Mikään näistä välitystavoista ei sellaisenaan ota huomioon naapurin senhetkistä sopivuutta viestin välittäjäksi. Useimmiten langaton sensoriverkko tarvitseekin mukautuvaa välitysstrategiaa, joka huomioi muun muassa topologian, ruuhkat, vikatilanteet ja naapurisolmujen energiatason [22]. Kuvassa 15 [1] on esimerkki multihop-verkosta ja taulukko 5 esittää esimerkin siihen liittyvästä reititystaulusta. Reititystauluun on merkitty kustannukset energiakulutuksen (α), solmujen energiatasojen (EA) ja hyppyjen määrän näkökulmista T-solmun ollessa lähettävänä solmuna.



Kuva 15. Yksinkertainen multihop-verkko [1].

Esimerkki solmun T reititystaulusta

Kohde	Seuraava solmu	Total EA	Total α	Hyppyjä
C	C	2	2	1
C	B	4	3	2
B	B	2	1	1
B	C	4	4	2
D	D	3	2	1
F	F	4	2	1
E	F	5	4	2
A	C	6	5	3
A	B	4	2	2
Sink	C	6	6	4
Sink	B	4	3	3
Sink	D	3	4	2
Sink	F	5	6	3

Taulukko 5. Esimerkki kuvan 15 verkon reititystaulusta.

4.5.2 Energiatehokas yksittäislähetys

Yksittäislähetyksestä (unicasting) puhutaan, kun tieto kulkee yksittäisten laitteiden välillä. Vastaanottajana on siis yksi yksittäinen solmu. Hyvän reititysprotokollan eräs tavoite onkin löytää sellainen polku näiden kahden laitteen välille, joka on energiatehokas. Polun löytäminen ei aina kuitenkaan ole yksikäsitteistä, koska energiatehokkuutta voidaan mitata usealla eri tavalla [1]:

- Maksimi-energiatason reitti on polku, jossa suositaan välittäjiksi niitä solmuja, joiden yhteenlaskettu energiataso on korkein. Tärkeää on kuitenkin eliminoida ne reitit, jotka pidentävät polkua turhaan. Kuvassa 15 maksimi-energiatason reitti solmusta T PAN-koordinaattoriin (Sink) olisi C–B–A–Sink. PAN-koordinaattoriin pääsee myös myös reittiä B–A–Sink, joten maksimienergiatason reitti ei ole tässä tehokkain, koska kulku solmun C kautta pidentää reittiä turhaan ja se on eliminoitava. Maksimi-energiatason reitiksi valikoituu siten F–E–Sink.

- Vähiten energiaa kuluttava reitti on polku, jonka varrella hypyt kuluttavat vähiten energiaa. Tämä voi johtaa epätasaiseen energiankulutukseen solmujen välillä. Kuvassa 15 vähiten energiaa solmusta T PAN-koordinaattoriin kuluttaa reitti B–A–Sink.

- Valintakriteerinä voi olla myös hyppyjen määrä reitillä eli valitaan polku, jossa on vähiten hyppyjä. Kuvassa 15 solmusta T PAN-koordinaattoriin vähiten hyppyjä on reitillä D–Sink.

- Reitti voidaan valita myös välttämällä pienen energiatason solmuja. Tällöin valitaan reitti, jossa pienin solmun energiataso on korkeampi, kuin muiden reittien pienin solmun energiataso. Tällä vältetään kuluttamasta liikaa yksittäistä laitetta vain sen takia, että sen ympärillä olevilla laitteilla on korkea energiataso. Kuvan 15 esimerkissä solmusta T PAN-koordinaattoriin tämän kriteerin täyttää parhaiten reitti D–Sink.

Yksittäislähetyksissä voi olla hyödyllistä laskea useita mahdollisia reittejä lähteen ja kohteen välille yhden parhaan reitin laskemisen sijaan. Puhutaan monipolkuisesta

reitittämisestä (multipath unicast routing). Tasapainoileminen tiedonsiirron vaatiman energian ja solmujen energiatason tasaisena pitämisen kanssa on helpompaa, kun reiteissä on valinnanvaraa. Lisäksi vaihtoehtoisille reiteille voi siirtyä nopeasti, mikäli solmu tai linkki jostain syystä rikkoutuu. Tavoitteena monipolkuisen reitityksen rakentamisessa on se, että reiteillä ei ole kohteen ja lähteen lisäksi yhteisiä solmuja tai linkkejä. Reittien perustamisen jälkeen seuraava vaihe on valita paras olemassa olevista reiteistä muut optimaalisen reitityksen vaatimukset huomioiden. [22]

4.5.3 Energiatehokas monilähetys

Monilähetyksessä voi vastaanottajana olla kaikki verkon laitteet (broadcasting) tai ryhmä laitteita (multicasting) esimerkiksi jollain maantieteellisellä alueella. Monilähetys on hyvin yleinen operaatio useimmissa langattomissa sensoriverkoissa. Keskeinen kysymys monilähetyksen reitittämisessä on se, kuinka rajata tietoa välittävien solmujen määrä mahdollisimman pieneksi siten, että kaikki kohdesolmut saavat tiedon. Mahdollisten reititysrakenteiden valikoima on laaja, seuraavaksi on esitelty muutamia esimerkkejä [22]:

- Puurakenteessa, jossa lähdesolmu toimii puun juurisolmuna, jokaiselle lähdesolmulle rakennetaan puu, joka sisältää kaikki kohdesolmut. Yleensä vaihtoehtoja on siis useita, mitä puurakennetta pitkin tietoa lähetetään. Tavoitteena on valita optimaalinen puu. Optimaalinen puu voi olla esimerkiksi sellainen, jossa kaikkien linkkien kustannusten summa on pienin (Steinerin pienin virittävä puu) tai jokaiselle kohteelle valitaan erikseen halvin polku. Ensimmäinen vaihtoehto on NP-täydellinen ongelma, jälkimmäinen on yksinkertaisemmin ratkaistavissa.

- Jaetussa puurakenteessa käytetään vain yhtä puuta, jonka kaikki lähdesolmut jakavat. Puun juurisolmuksi valitaan jokin verkon solmu ja puurakenne sisältää kaikki lähde- ja kohdesolmut. Verkon kuormitus on pienempi, koska usean puun sijasta ylläpidetään vain yhtä puuta, mutta luonnollisesti polut voivat pidetä. Optimaalisen juurisolmun löytäminen on jälleen NP-täydellinen ongelma.

- Mesh-rakenne syntyy, kun puurakenteeseen lisätään vaihtoehtoisia linkkejä esimerkiksi estämään puun rikkoutumista. Puumaisen rakenteen keskeinen

ominaisuus, silmukoiden puuttuminen, muuttuu. Mesh-rakenne on skaalautuvampi eikä häiriöille niin herkkä kuin puurakenne. Mesh-rakenne tarjoaa lyhyempiä polkuja kuin jaettu puurakenne, mutta se vaatii monimutkaisempia välitysalgoritmeja, ettei tieto tulvi koko mesh-rakenteeseen.

4.6 Datan kokoaminen sensoriverkossa (Data Aggregation)

Langattomassa sensoriverkossa on tyypillistä, että ollaan kiinnostuneita informaatiosta, jota sensorit mittavat, enemmän kuin tiedon lähteestä. Samalla alueella voi olla myös useita sensoreita, jotka tarkkailevat aluetta vuoronperään toisten ollessa lepotilassa. Yksittäisen sensorin osoite, josta data on lähtöisin, on siis toisarvoinen tieto. Samoin tietoa mittaavan sensorin toimintaan ei vaikuta se, kenelle tai kuinka monelle vastaanottajalle tietoa lähetetään. Langatonta sensoriverkkoa voikin luonnehtia datakeskeiseksi. [22]

Langattoman sensoriverkon resurssien rajallisuus muistaen tarvitaan tekniikoita estämään verkon ruuhkautumista ja tukkeutumista. Näitä tekniikoita kutsutaan datan kokoamistekniikoiksi. Datan kokoamisella pyritään estämään datan imploosio ja päällekkäisyys. Imploosiolla tarkoitetaan sitä, että sama tieto menee eteenpäin eri reittejä pitkin. Päällekkäisyys tarkoittaa sitä, että naapurisensorilaitteet havaitsevat saman ilmiön yhtä aikaa ja lähettävät sen eri tietoina eteenpäin. Datan kokoamista käsiteltiin jo hiukan klusteroinnin yhteydessä luvussa 4.3. Datan kokoamiseen liittyy myös eri sensoreista saatavien tietojen yhdistely ja mahdollisesti myös tietojen käsittely tarkoituksenmukaiseksi informaatioksi ennen sen välittämistä eteenpäin, tätä kutsutaan datafuusioksi. Datan kokoamisessa tulee kuitenkin yleensä säilyttää raportoivien solujen sijaintitiedot, koska useimmat sovellukset tarvitsevat mitattavan ilmiön sijaintitietoja. Yksinkertaisimpia esimerkkejä datan kokoamisesta ovat esimerkiksi suurimman/pienimmän arvon tai keskiarvon laskeminen ja tämän tiedon lähettäminen eteenpäin. Monimutkaisempaa datan kokoamista vaatii esimerkiksi tietyn alueen ääriviivojen tai kahden alueen rajaviivan arvioiminen saatujen arvojen perusteella. [22] [1]

Datan kokoamismekanismissa täytyy huomioida halutun tarkkuustason muuttuminen. Tietyn alueen solmuilta voidaan haluta joissakin tilanteissa tarkempaa tietoa kuin

normaalisti. Tietoja kokoavan solmun täytyy siis pystyä tuottamaan tietoa vaihtelevilla tarkkuusasteilla. [34]

4.6.1 Datan kokoamispisteen sijoittaminen

Tietoa kootaan sinkille yleensä puurakennetta pitkin. Tietoa kokoavien solmujen sijainti on syytä miettiä tarkkaan, jotta kokoamisella saavutetaan mahdollisimman suuri hyöty. Tiedon kokoamisen tulisi tapahtua mahdollisimman aikaisessa vaiheessa ja lähellä lähettäviä solmuja. [22]

Artikkeli [11] esittelee kolme tarkoitukseen sopivaa puurakennetta: Center at Nearest Source (CNS), Shortest Paths Tree (SPT) ja Greedy Incremental Tree (GIT). CNS-puurakenteessa solmut lähettävät tietonsa sinkkiä lähinnä olevalle lähettävälle solmulle, joka kokoaa tiedon ja lähettää sen edelleen sinkille. SPT-puukenteessa solmut lähettävät tiedon Sinkille kukin lyhintä reittiä pitkin ja päällekkäiset polut muodostavat kokoavan puun. GIT-puurakenne rakentuu vaiheittaisesti. Ensimmäisessä vaiheessa PAN-koordinaattori ja lähin lähettävä solmu muodostavat puun ja seuraavissa vaiheissa muut lähettävät solmut liittyvät lähimpään puuhun.

4.6.2 Datan kokoamisen tehokkuuden arviointi

Datan kokoamisen tuloksia voidaan arvioida useilla tavoilla. Kootun tiedon tarkkuus on ehkäpä tärkein arviointialue eli kuinka paljon vastaanottajan saamat arvot poikkeavat alkuperäisistä arvoista. Kiinnostava tieto on myös informaation täydellisyys eli kuinka suuri osa alkuperäisistä mittaustiedoista sisältyy lopulliseen koottuun informaatioon sekä kuinka suuren viiveen tiedon kokoaminen aiheutti. Energiankulutuksen vähentäminen ja siten verkon elinkaaren pidentäminen on datan kokoamisen päätavoite, joten viestien määrän väheneminen on myös tärkeä arviointialue. [22]

5 HEED-klusterointiprotokolla

Kokkolan yliopistokeskus Chydeniuksen tietoliikennelaboratorissa on jo vuodesta 2002 tehty tutkimusta koskien langattomia sensoriverkkoja ja kehitetty niihin hallintamenetelmiä. Esimerkiksi testausta, datansiirtomenetelmiä ja reititystä on kehitetty ja kehitetään muissa tutkimuksissa ja yhtenä kiinnostavana tutkimuskohteena on verkon organisoiminen klusteroinnin avulla. Siksi se valittiin tässä tutkimuksessa tarkastelukohteeksi.

Keskeinen tavoiteltava ominaisuus sensoriverkolle on energiatehokkuus, koska sen vaikutus verkon elinkaareen ja skaalautuvuuteen on merkittävä. Sensoriverkolle on myös tyypillistä, että sen mittaama data voidaan koota ja yhdistellä paikallisesti ja lähettää käsiteltynä eteenpäin sinkille. Klusterointi on siis hyvin perusteltua useissa sensoriverkoissa, sitä pidetään tehokkaana tapana organisoida verkko. Viime vuosina on kehitetty useita klusterointiprotokollia myös langattomille sensoriverkoille. Esimerkiksi LEACH-menetelmässä (Low-Energy Adaptive Clustering Hierarchy) [3] pääsolmun tehtävää kierrätetään ja klusterointi vaatii vain yhden iterointikierroksen. LEACH on sovellussidonnainen ja suunniteltu singlehop-verkkoihin. Se olettaa pääsolmujen energiankulutuksen olevan yhdenmukainen. DECA-menetelmä (Distributed Efficient Clustering Approach) [26] on suunniteltu erityisesti mobiileihin langattomiin verkkoihin, jotka viestivät multihop-menetelmää käyttäen. EELTC (An Energy-Efficient Level-based and Time-based Clustering algorithm for Wireless Sensor Networks) [15] on klusterointimenetelmä täysin tahdistettuihin verkkoihin, missä pääsolmujen valintaperusteena on solmujen etäisyys sinkistä ja solmujen jäljellä oleva energiamäärä.

Tässä luvussa käsitellään HEED-protokollaa (Hybrid Energy-Efficient Distributed Clustering), joka on Fahmyn ja Youniksen [12] esittelemä energiatehokas klusterointimenetelmä sensoriverkoille. HEED valittiin tarkasteltavaksi, koska se on täysin hajautettu menetelmä, eikä aseta vaatimuksia solmujen tai sinkin sijainnille. Se myös käyttää kahta parametria pääsolmun muodostamisessa taatakseen pääsolmujen mahdollisimman hyvän hajonnan verkon alueelle. HEED-protokolla ei määrittele menetelmää solmujen sijoittamiselle. Klusterointi tapahtuu vakiomäärällä

iterointikierroksia riippumatta verkon tiheydestä, laajuudesta tai topologiasta. Klustereitten väliselle ja muulle verkon sisäiselle viestinnälle protokolla ei aseta rajoituksia. Sovelluksesta riippuen pääsolmut kommunikoivat suoraan PAN-koordinaattorin kanssa tai viestivät keskenään käyttäen multihop-menetelmää, datan kokoamista sekä muita luvussa 4 esiteltyjä menetelmiä.

5.1 Protokollan sopivuus sensoriverkolle

HEED-protokollaa voidaan ajaa tehokkaasti tyypillisissä langattomissa sensoriverkkosovelluksissa. Protokolla tukee juuri niitä langattoman sensoriverkon ominaisuuksia, joita tarvitaan tasapainottamaan pääsolmujen kuormaa ja mahdollistamaan verkon pitkä elinkaari. Verkon solmujen, ainakin niiden, jotka ilmoittautuvat pääsolmuehdokkaiksi, tulee pysyä lähes paikallaan. Solmut, jotka liikkuvat nopeasti verkossa, voivat huonontaa klusteroinnin laatua, koska klusterin sisäinen solmujen sijoittelu muuttuu. Solmujen staattisuus onkin tyypillistä sensoriverkkosovelluksille. Solmujen keskinäinen energiankulutus on yleensä epätasaista, ja sitä tasataan protokollassa pääsolmuvastuun kierrätyksellä. HEED-protokollaa hyödyntävässä sensoriverkossa solmujen sijaintitietoa ei käytetä, joten paikannusmenetelmiä ei tarvita. Protokolla ei aseta mitään oletuksia solmujen sijainnin tasaisuudelle verkon alueella, verkon tiheydelle tai halkaisijalle, virrankulutuksen jakaantumiselle solmujen välillä tai tiedonkeruupisteiden läheisyydelle. Se soveltuu hyvin sovelluksiin, joiden verkkorakenne on suhteellisen staattinen, solmujen sijaintia ei tarvitse paikantaa ja verkon solmut ovat tiedonkäsittelykapasiteetiltaan samantasoisia ja tasa-arvoisia, eikä niitä valvota sijoittamisen jälkeen. HEED-protokolla soveltuu hyvin myös sovelluksiin, jotka vaativat tehokasta datan kokoamista, esimerkiksi ympäristön tarkkailu. Erityisesti näissä sovelluksissa, joissa solmuja ei sijoittamisen jälkeen valvota, verkon elinkaaren pidentäminen on tärkeää. Vaikka HEED-protokolla on suunniteltu pääsääntöisesti staattisiin ympäristöihin, artikkelissa [26] on todettu sen sietävän hyvin myös solmujen liikkumista. [12]

5.2 Klusteroinnin tavoitteet

Klusterointia suunniteltaessa täytyy huomioida klusterointikertojen tiheys. Klusterointikertojen välin tulee olla pidempi kuin yhden klusterointikierroksen keston, jotta klusteroinnin kuormitus ei kasva liian suureksi. Klusterointikertojen tiheyden ratkaisee sovelluksen ominaisuudet. Klusterointi voi olla kannattavaa tehdä usein, jopa sekuntien tai minuuttien välein, jos klusterointiin kuluva energiankulutus suhteessa verkon normaalitoimintaan on pieni. Harvakseltaan tietoa keräävässä verkossa klusteroinnin vaatima energiakulutus suhteessa verkon normaalitoimintaan voi olla suuri, joten klusterointikierrosten välit kannattaa pitää myös suurina. HEED-protokolla lupaa seuraavat ominaisuudet klusteroinnille [12]:

1. Klusterointi on täysin hajautettua, jokainen solmu päättää itsenäisesti omasta klusteristaan paikallisen informaation perusteella.

2. Riippumatta verkon solmujen lukumäärästä tai tiheydestä, yhden klusteroinnin iterointikierrosten määrä on vakio. Kierroksia on vähintään kaksi ja enintään N kappaletta, missä N on kaikkien verkon solmujen määrä.

3. Klusteroinnin päättyessä jokainen solmu on joko pääsolmu tai tavallinen solmu, joka kuuluu täsmälleen yhteen klusteriin.

4. Tehokas klusterointi vaatii vain vähän solmujen välistä viestien vaihtoa tai datan prosessointia.

5. Pääsolmut valitaan siten, että ne kattavat hyvin koko verkon alueen, ja että klusterin muut solmut ovat yhden hypyn päässä pääsolmusta.

5.3 Klusterointiparametrit

Klusterin pääsolmun valinta perustuu ensisijaisesti solmun energiatasoon. Varsinaista energiatason mittausta ei kuitenkaan tarvita, jos havainnoinnin, prosessoinnin ja viestinnän vaatima energiankulutus/bitti pystytään arvioimaan. Toissijaisen klusterointiparametrin kannattaa perustua klusterin sisäiseen kustannukseen, esimerkiksi naapurisolmujen

läheisyyteen tai klusterin kokoon. Ensisijaista parametria käytetään erityisesti pääsolmujen valinnassa, toissijaisen parametrin merkitys on ratkaista tilanteet, joissa solmu on kahden pääsolmun kuuluvuusalueella tai kaksi pääsolmuehdokasta on samalla kuuluvuusalueella. Kuuluvuusalueeseen vaikuttaa solmun käyttämä lähetysteho, mitä suurempi lähetysteho sitä suurempi kantama eli kuuluvuusalue. Klusterin lähetysteholla tarkoitetaan klusterin sisäiseen viestintään ja klusterointiin tarvittavaa lähetystehoa. Suositeltavaa on valita klusterin lähetystehoksi alhaisempi lähetysteho, jotta korkeammat lähetystehot voidaan varata klustereitten väliseen viestintään. Näiden korkeampien lähetystehojen kantama täytyy olla vähintään kahden klusterin halkaisijan suuruinen, jotta verkon yhtenäisyys säilyy. Klusterin lähetysteho sanelee myös tarvittavien klustereitten määrän. Käytännössä klustereitten määrän optimointi on hankalaa, koska sensoriverkon topologia voi muuttua solmujen poistumisen ja uusien solmujen liittymisen myötä. [12]

Mikäli pääsolmuehdokkaita on samaan klusteriin useampia, toissijaisena valintakriteerinä voi olla jokin klusterille toivottu ominaisuus. Se voi olla klusterin koko tai lähetystehon säästäminen niissä tapauksissa, joissa solmut voivat itse säädellä lähetystehoaan. Mikäli solmut eivät voi säätää lähetystehoaan, valintaparametrina voidaan käyttää joko solmun pienimmän asteen kustannusta (minimum degree cost) tai solmun suurimman asteen kustannusta (maximum degree cost). Käytettäessä solmun pienimmän asteen kustannusta, solmut liittyvät siihen pääsolmuun, jolla on pienin aste eli vähiten naapureita ja siten hajautetaan pääsolmujen kuormaa. Kun halutaan muodostaa tiheitä klustereita, käytetään solmun suurimman asteen kustannusta. Tällöin solmut liittyvät siihen pääsolmuun, jonka aste on suurin. Siinä tapauksessa, että solmuille sallitaan lähetystehon vaihtelut klusterin sisäisessä viestinnässä, voidaan kustannuksia arvioida pienimmän tarvittavan lähetystehon keskiarvon, AMRP:n (Average Minimum Reachability Power), avulla. AMRP:llä tarkoitetaan keskiarvoa klusterin solmujen pienimmistä lähetystehoista, mitä niiden pitää käyttää saavuttaakseen pääsolmu. Kun solmu valitaan pääsolmuksi, mittaa solmun AMRP koko klusterin sisäisen viestinnän kustannusta. Käyttämällä AMRP:tä kustannusparametrina, pystytään edullisin pääsolmu erottamaan selkeästi niissä tilanteissa, joissa useammat pääsolmuehdokkaat kilpailevat samalla kuuluvuusalueella. Taulukossa 6 on yhteenveto eri vaihtoehdoista klusterien muodostamiseen. [12]

Tavoite	Lähetysteho sama kaikilla	Lähetysteho voi vaihdella
Pääsolmun kuorman vähentäminen	solmun aste	AMRP
		solmun aste
Tiheät klusterit	1/ solmun aste	AMRP
		lähin solmu

Taulukko 6. Yhteenveto klusterien muodostamisen eri vaihtoehdoista [12].

5.4 Klusterointioperaatiot

Uudet pääsolmut valitaan väliajoin (T_{kp} + T_{vt}), missä T_{kp} on klusterointiin kuluva aika ja T_{vt} klusterointien välinen verkon toiminnan aika eli T_{kp}:n päättymisen ja uuden T_{kp}:n alkamisen välinen aika. Jokainen klusterointi muodostuu tietystä määrästä iterointikierroksia (N_{iter}). Jokainen iterointikierros kestää ajan T_c, minkä aikana solmu ehtii vastaanottamaan naapurisolmuiltaan lähetetyn viestin. Pääsolmujen alustava määrä, C_{tod}, alustetaan tietyksi prosenttiosuudeksi kaikkien solmujen määrästä, esimerkiksi 5%:iin. Tämän alustavan pääsolmujen määrän asettamisen tarkoitus on rajoittaa pääsolmuehdokkaitten määrää, eikä se vaikuta suoraan lopulliseen klusterimäärään. [12]

5.4.1 Pääsolmuehdokkaaksi asettuminen

HEED-algoritmin aluksi, solmu asettaa todennäköisyytensä tulla valituksi pääsolmuksi, $CH_{tod,}$ seuraavan kaavan avulla

$$CH_{tod} = C_{tod} \quad x \quad \frac{E_{res}}{E_{max}} ,$$

missä E_{res} on solmun pariston jäljellä oleva virta ja E_{max} solmun pariston virtamäärä täyteen ladattuna. Yleensä solmuilla on sama E_{max}, mutta HEED pystyy käsittelemään myös laitteita, joilla on erilaiset paristot. CH_{tod}-arvolle asetetaan minimiarvo (P_{min}), jonka alle se

ei saa laskea. Tätä rajoitusta tarvitaan, jotta algoritmi päättyy vakioajassa. P_{min}-arvolla pystytään myös vaikuttamaan iterointikierrosten määrään. Minimiarvo on käänteisesti verrannollinen E_{max}-arvoon. [12]

5.4.2 Pääsolmun valinta

Jokaisella iterointikierroksella i, $i \leq N_{iter}$, solmuista, jotka eivät vielä ole saaneet viestiä pääsolmuehdokkaalta, eli eivät ole peitettyjä, arvotaan pääsolmuehdokkaat todennäköisyydellä CH_{tod}. Jokaisen iterointikierroksen jälkeen pääsolmuehdokkaitten joukkoon, S_{ch}, lisätään uudet pääsolmuehdokkaat. Solmu valitsee omaksi pääsolmuehdokkaakseen kustannukseltaan edullisimman pääsolmuehdokkaitten joukosta. Se voi valita myös itsensä, mikäli se kuuluu pääsolmuehdokkaitten joukkoon ja sen kustannus on edullisin. Iterointikierroksen lopuksi jokainen solmu kaksinkertaistaa CH_{tod}-arvonsa ennen seuraavaa iterointikierrosta. Iterointi päättyy sitä seuraavalla kierroksella, kun CH_{tod} saavuttaa arvon yksi. [12]

HEED-algoritmin voi esittää pseudokoodina seuraavasti [12]:

I Vaihe, alustus:

```
1. S_nbr <- {v: v sijaitsee kuuluusalueellani}
2. Laske ja lähetä kustannus solmulle, joka ∈ S_nbr
3. CH_tod <- max (C_tod x (E_res/E_max), P_min)
4. is_final_CH <- FALSE
```

II vaihe, iterointi

```
Do {
5. If ((S_ch <- {v: v on pääsolmu}) ≠ ∅)
6.  my_cluster_head <- least_cost(S_ch)
7.  If my_cluster_head = NodeID
8.    If (CH_tod = 1)
9.      Cluster_head_msg(NodeID, final_CH, cost)
10.     is_final_CH <- TRUE
11.   Else
12.     Cluster_head_msg(NodeID, tentative_CH, cost)
13.ElseIf (CH_tod = 1)
14.   Cluster_head_msg(NodeID, final_CH, cost)
15.   is_final_CH <- TRUE
16.ElseIf Random (0,1) ≤ CH_tod
17.   Cluster_head_msg(NodeID, tentative_CH, cost)
18.CH_prev <- CH_tod
19.CH_tod <- min(CH_tod x 2, 1)
} While(CH_prev < 1)
```

III Vaihe, viimeistely:

```
20.If(is_final_CH = FALSE)
21.   If ((S_ch <- {v: v on final cluster head}) ≠ ∅)
22.     my_cluster_head <- least_cost(S_ch)
23.     join_cluster(cluster_head_ID, NodeID)
24.   Else Cluster_head_msg(NodeID, final_CH, cost)
25.Else Cluster_head_msg(NodeID, final_CH, cost)
```

Riveillä 1–4 solmu etsii naapurisolmut, laskee ja lähettää kustannuksensa, esimerkiksi solmun asteen, muille klusterin solmuille sekä laskee oman todennäköisyytensä (CH_{tod}) pääsolmuksi. CH_{tod}-arvo on vähintään ennalta määrätty minimiarvo P_{min}. Mikäli solmuille

on sallittu lähetystehon vaihtelu klusterin sisäisessä viestinnässä, hakee solmu ne naapurisolmut, joiden lähetysteho on pienempi tai yhtä suuri kuin klusterin lähetysteho. Tällöin oletetaan, että mikäli solmu *u* kuulee solmun *v* tietyllä lähetysteholla, myös solmu *v* kuulee solmun *u* samalla lähetysteholla. Naapureiden etsiminen ei ole välttämätöntä jokaisella uudella klusterointikierroksella, mikäli sensoriverkon luonne on staattinen. Naapurusto pysyy suhteellisen samana ja solmut päivittävät automaattisesti naapuruston rakennetta lähettämällä ja vastaanottamalla säännöllisesti beacon-viestejä. Aloitusvaiheessa myös ”nollataan” pääsolmutilanne, eli poistetaan pääsolmuilta tila *final_CH*. Sama solmu voi valikoitua pääsolmuksi peräkkäisillä klusterointikierroksilla, mikäli sen energiataso on korkea ja kustannukset matalat. [12]

Rivien 5–19 silmukassa solmu päättää asettumisestaan pääsolmuehdokkaaksi. Pääsolmuehdokkaitten joukko (S_{ch}) muodostuu solmuista, joiden tila on *tentative_CH* tai *final_CH*, jos solmun todennäköisyys (CH_{tod}) on jo saavuttanut arvon yksi. Pääsolmuehdokkaat lähettävät muille solmuille viestejä solmutunnuksestaan, valintatilastaan ja kustannuksestaan. Solmu pitää itseään ”peitettynä”, mikäli se kuulee viestin joko *tentative_CH* tai *final_CH* -tilan solmulta. Tällöin se ei itse ala pääsolmuehdokkaaksi iterointivaiheessa. Solmu voi kuitenkin algoritmin viimeistelyvaiheessa tulla pääsolmuksi, mikäli se lopettaa iteroinnin ennen muita pääsolmuehdokkaita eli sen CH_{tod}-arvo on korkein. Silmukan lopuksi solmujen CH_{tod}-arvo tallennetaan CH_{prev}-muuttujaan ja CH_{tod}-arvo kaksinkertaistuu. Iterointi päättyy, kun solmun CH_{prev} saavuttaa arvon yksi ja algoritmi siirtyy viimeistelyvaiheeseen riville 20, missä solmut liittyvät pääsolmuihin. Iterointikierroksia käydään vähintään kaksi, koska minkään solmun CH_{tod}-arvo ei voi ensimmäisellä kierroksella olla yksi, mikäli C_{tod}-arvo on määritelty alle 100 %. Painavimmat solmut, joilla on suuri CH_{tod} -arvo, käyvät vähiten iterointikierroksia ja ovat siten ensimmäisinä viimeistelyvaiheessa joko pääsolmuina tai liittymässä niihin. [12]

Pääsolmuehdokkaitten joukon ollessa tyhjä (rivi 5) ja solmun CH_{tod}-arvon ollessa alle yksi (rivi 13), arvotaan satunnaisluku väliltä 0–1 (rivi 16). Mikäli satunnaisluku on pienempi kuin solmun CH_{tod}-arvo, vaihtuu solmun tilaksi *tentative_CH* (rivit 16-17) ja se liittyy pääsolmuehdokkaitten joukkoon S_{ch}. Satunnaisluvun ollessa suurempi kuin solmun CH_{tod},

tila ei muutu ja solmu jatkaa seuraavalle kierrokselle. Mikäli rivillä 13 todetaan, että solmun CH_{tod} on jo saavuttanut arvon yksi, solmu ilmoittaa tilakseen *final_CH* liittyen pääsolmuehdokkaitten joukkoon ja iterointikierroksen lopussa algoritmi siirtyy riville 20. Tässä tapauksessa kuuluvuusalueella on todennäköisesti ainoastaan yksi tai enintään muutama solmu. [12]

Mikäli pääsolmuehdokkaitten joukossa (S_{ch}) on jo solmuja, etsii solmu pääsolmuehdokkaitten joukosta sen, jonka kustannus on edullisin (rivi 6) ja jatkaa iterointia silmukan loppuun asti. Solmu voi valita myös itsensä pääsolmuehdokkaakseen edellyttäen, että se kuuluu pääsolmuehdokkaitten joukkoon ja että sen oma kustannus on edullisin (rivi 7). Solmun CH_{tod}-arvon ollessa yksi tai suurempi, tilaksi vaihtuu *final_CH*, solmu ilmoittaa muille tilansa ja algoritmi siirtyy iterointikierroksen lopuksi päätösvaiheeseen riville 20. CH_{tod} -arvon ollessa alle yksi, solmu ilmoittaa olevansa edelleen tilassa *tentative_CH* ja jatkaa iterointia, kunnes sen CH_{tod} saavuttaa arvon yksi. Algoritmin mukaan pääsolmuehdokas, jonka tila on *tentative_CH*, voi muuttua tavalliseksi solmuksi myöhemmällä iterointikierroksella löytäessään pääsolmuehdokkaan, jolla on alempi kustannus tai tila *final_CH* eli se ei enää lähetä viestejä muille tilastaan ja kustannuksestaan. Kun ensimmäinen solmu saavuttaa *final_CH* -tilan, muut solmut hylkäävät aikaisemman pääsolmuehdokkaansa ja valitsevat *final_CH*-tilassa olevan solmun pääsolmukseen. [12]

Algoritmin viimeistelyvaiheessa (rivit 20–25) pääsolmut lähettävät viestiä tilastaan (*final_CH*) sekä kustannuksestaan. Muut solmut liittyvät pääsolmuun, jolla on pienin kustannus sitä mukaa, kun päättävät oman iterointinsa. Mikäli solmu päättää iteroinnin ennen kuin sen valitsema pääsolmu, eli solmun oma CH_{tod}-arvo on suurempi kuin sen pääsolmuehdokkaan, julistautuu se itse pääsolmuehdokkaaksi tilassa *final_CH*. Siten se solmu, jolla on suurin CH_{tod}, valitaan ensisijaisesti pääsolmuksi ja kustannus on vasta toissijainen parametri. [12]

5.4.3 HEED-algoritmin vaikutus yksittäiseen solmuun

Algoritmi voi päättyä solmun osalta seuraavilla tavoilla [12]:

1. Solmu liittyy pääsolmuehdokkaitten joukkoon satunnaislukuarvonnan jälkeen ja valitsee itsensä pääsolmuehdokkaakseen, mikäli sen oma kustannus on matalin. Solmu jatkaa iterointia, kunnes CH_{tod} saavuttaa arvon yksi. Solmusta tulee pääsolmu, mikäli se lopettaa ensimmäisenä iteroinnin.

2. Solmu liittyy pääsolmuehdokkaitten joukkoon satunnaislukuarvonnan jälkeen ja valitsee pääsolmuehdokkaakseen sen, jolla on matalin kustannus. Mikäli se ei ole valinnut itseään, se ei enää ilmoittele pääsolmuehdokkuudestaan, eli sen tila on vaihtunut tavalliseksi solmuksi. Solmu jatkaa iterointia, kunnes CH_{tod} saavuttaa arvon yksi. Viimeistelyvaiheessa se liittyy pääsolmuun, jonka tila on *final_CH*. Mikäli oma tai mikään muu pääsolmuehdokas ei ole vielä tilassa *final_CH*, solmu asettuu itse pääsolmuksi. Useampien pääsolmujen kilpailutilanteessa solmut valitsevat pääsolmukseen sen, jolla on alhaisin kustannus.

3. Solmu ei saa satunnaislukuarvonnassa CH_{tod}-arvoaan pienempää lukua, joten siitä ei tule pääsolmuehdokasta. Solmu valitsee oman pääsolmuehdokkaansa ja jatkaa iterointia, kunnes CH_{tod} saavuttaa arvon yksi. Viimeistelyvaiheessa se liittyy pääsolmuun. Mikäli oma tai mikään muu pääsolmuehdokas ei ole vielä tilassa *final_CH*, solmu asettuu itse pääsolmuksi. Useampien pääsolmujen kilpailutilanteessa solmut valitsevat pääsolmukseen sen, jolla on alhaisin kustannus.

4. Solmu ei saa satunnaislukuarvonnassa CH_{tod}-arvoaan pienempää lukua, joten siitä ei tule pääsolmuehdokasta. Pääsolmuehdokkaitten joukko pysyy tyhjänä, joten kyseessä on eristyksissä oleva solmu/solmut. Iterointi jatkuu kunnes solmun CH_{tod} saavuttaa arvon yksi. Mikäli se on ensimmäinen solmu, jonka tilaksi tulee *final_CH*, siitä tulee pääsolmu.

5. Solmu tahdistuu klusteroinnin jo alettua, joten se aloittaa HEED-algoritmin suorittamisen myöhemmin, kuin muut kuuluvuusalueen solmut. Siitä ei voi tulla

pääsolmuehdokasta, mikäli pääsolmuehdokkaitten joukko on ei-tyhjä, joten se valitsee oman pääsolmuehdokkaansa muista ehdokassolmuista. Solmu jatkaa iterointia, kunnes CH_{tod} saavuttaa arvon yksi. Viimeistelyvaiheessa se liittyy pääsolmuun. Mikäli oma tai mikään muu pääsolmuehdokas ei ole vielä tilassa *final_CH*, solmu asettuu itse pääsolmuksi. Useampien pääsolmujen kilpailutilanteessa solmut valitsevat pääsolmukseen sen, jolla on alhaisin kustannus.

Kohdassa neljä huomataan, että on olemassa pieni todennäköisyys sille, että kaksi eristyksissä olevaa naapurisolmua päättää iteroinnin yhtä aikaa, eikä kumpikaan ole ilmoittautunut pääsolmuehdokkaaksi ennen viimeistelyvaihetta. Molemmista voi tulla pääsolmu, koska niiden kustannus on sama. Artikkelin [12] mukaan todennäköisyys tähän on kuitenkin häviävän pieni. Asiaa on käsitelty seuraavassa luvussa Lemmassa 5. Verkon elinkaaren aikana todennäköisyys vielä pienenee, koska solmujen CH_{tod}-arvot ovat sitä epätodennäköisemmin samat mitä kauemmin verkko on toiminut.

Mikäli solmu tahdistuu myöhemmin jo alkaneeseen klusterointiin, on mahdollista, että se ei tule valituksi pääsolmuksi, vaikka sillä olisi hyvät ominaisuudet siihen (korkea energiataso ja matala kustannus). Artikkelissa [12] on kuitenkin simuloimalla todettu, että HEED toimii verrattain hyvin myös silloin, kun osa solmuista tahdistuu klusteroinnin jo alettua. Siten tahdistus ei ole kriittinen HEED-algoritmin toiminnalle.

5.5 Klusteroinnin oikeellisuus ja kompleksisuus

HEED-protokollan tavoite on olla täysin hajautettu. Se toteutuu tässä algoritmissa, koska solmu voi päättää tulla pääsolmuksi CH_{tod}-arvonsa perusteella tai se voi päättää liittyä johonkin pääsolmuun kuuntelemalla viestejä klusterinsa kuuluvuusalueella. Siten solmu tekee päätöksensä täysin paikallisen informaation perusteella. [12]

Lemma 1. HEED-algoritmi pysähtyy vakioajassa, $N_{iter} = O(1)$.

Todistus: Pahin tapaus ilmenee, kun solmulla on erittäin matala E_{res} CH_{tod}-arvon asettuessa minimiin P_{min}. CHt_{od}-arvo kuitenkin kaksinkertaistuu jokaisella askeleella ja algoritmi päättyy sen askeleen jälkeen, kun CH_{tod} saavuttaa arvon yksi. Niinpä

$$2^{Niter-1} \text{ x } P_{min} \geq 1$$

ja siten

$$N_{iter} \leq [\log_2 \frac{1}{P_{min}}] + 1 \quad ,$$

joten $N_{iter} \sim O(1)$. Alustamalla minimiarvo, $P_{min,}$ sopivasti, voidaan iteraatioiden määrää rajoittaa järkevään määrään. Kun E_{res}-arvo on lähellä E_{max}-arvoa, eli solmun energiataso on korkea, tarvittavien iterointikierrosten määrä on pieni ja riippuu C_{tod}-arvosta. Koska algoritmi päättyy aiemmin korkean energiatason solmuilla, se mahdollistaa myös matalan energiatason solmujen liittymiseen niiden klustereihin. [12]

Lemma 2. Algoritmin päättyessä kaikki solmut kuuluvat johonkin klusteriin tai ovat pääsolmuja.

Todistus: Algoritmin II-vaihe voi päättyä siten, että solmu ei ole pääsolmuehdokas eikä sen oma pääsolmuehdokas ole vielä tilassa *final_CH*. Mikäli muita pääsolmuja (tilassa *final_CH*) ei vielä ole, eli se päättää iteroinnin ensimmäisenä, tulee solmusta itsestään pääsolmu. [12]

Lemma 3. Algoritmin aikavaativuus on O(N)/solmu, missä N on verkon solmujen lukumäärä.

Todistus: Algoritmin alustusvaiheessa solmujen kustannusten laskemiseen käytettävä aika on vakio ≤ N, missä N on solmujen lukumäärä verkossa, mikäli kustannuksen perusteena käytetään AMRP:tä. Samoin viimeistelyvaiheessa pääsolmujen sovitteluun ehdokkaitten kesken käytetään aikaa enintään N. Iterointivaiheessa pääsolmuiksi sovittelu tapahtuu myös vakioajassa, koska se vie enintään ajan, jonka pääsolmuehdokkaat käyvät iterointikierroksia, N_{iter} x N. Lemman 1 mukaan algoritmi pysähtyy vakioajassa, joten algoritmin aikavaativuus on siten O(N). [12]

Lemma 4. Lähetettävien viestien määrä on O(1)/solmu eli O(N)/verkko.

Todistus: Algoritmin aikana pääsolmuehdokas tilassa *tentative_CH* generoi pääsolmuviestejä enintään iterointikierrosten verran. Tavallinen solmu lähettää vasta viimeistelyvaiheessa yhden liittymisviestin pääsolmulle. Näitä liittymisviestejä on vähemmän kuin verkon solmumäärä, koska ainakin yksi solmu on pääsolmu. Siten viestien kokonaismäärä on enintään N_{iter} x N ja vaativuus siten O(N). [12]

Lemma 5. Todennäköisyys sille, että samalla kuuluvuusalueelle on kaksi pääsolmua, on pieni, eli pääsolmut ovat hyvin hajautettuna verkon alueelle.

Todistus: Haastavimmassa tapauksessa verkossa on kaksi eristyksissä olevaa solmua, jotka ovat keskenään naapureita. Oletetaan että solmut ovat keskenään täysin tahdistetut ja kumpikaan ei valikoidu pääsolmuksi ennen kuin niiden CH_{tod} saavuttaa arvon yksi. Silloin on kaksi mahdollista skenaariota:

Case 1. Molempien arvot ovat sen verran keskenään erilaisia, että ne käyvät eri määrän iterointikierroksia algoritmin vaiheessa kaksi. Siten toisesta tulee pääsolmu ensin ja toinen rekisteröityy sitten sen jäseneksi. Vaikka solmut eivät olisi keskenään tahdistettuja, on todennäköistä, että ne käsittelevät ja päättävät algoritmin eri aikoina, siksi tahdistus ei ole kriittinen HEED algoritmin toiminnalle.

Case 2. Molemmat solmut, *u* ja *v*, käyvät iterointikierroksia yhtä paljon vaiheessa kaksi. Tässä tapauksessa kumpikaan solmuista, *u* tai *v*, ei ala pääsolmuehdokkaaksi todennäköisyydellä $p_i = (1 - CH_{todu})\ (1 - CH_{todv})$. Merkitään tod_u:lla CH_{todu}:n alkuarvoa ja tod_v:llä CH_{todv}:n alkuarvoa. Iterointikierroksella i, kun $0 \leq i \leq N_{iter} - 2$, kulloinenkin $CH_{todu} = tod_u \times 2^i$ ja $CH_{todv} = tod_v \times 2^i$. Lasketaan todennäköisyys, P_{nbr}, sille, että kumpikaan solmuista *u* tai *v* ei tule valituksi pääsolmuksi millään iterointikierroksella i, eli viimeistelyvaiheen jälkeen molemmat ovat pääsolmuja:

$$P_{nbr} = \prod_{i=0}^{Niter-2} (1 - tod_u \times 2^i)(1 - tod_v \times 2^i).$$

Kun $tod_u = tod_v = p$, saadaan

$$P_{nbr} = \prod_{i=0}^{(\log 1/p - 1)} (1 - p \times 2^i)^2.$$

CH_{tod}-arvon tyypillisillä alkuarvoilla todennäköisyys P_{nbr} on hyvin pieni. Esimerkiksi kun p = 3 %, P_{nbr}= 0,00016 tai p = 5 % niin P_{nbr}= 0,006. [12]

5.6 HEED-protokollan hyötyminen IEEE 802.15.4 -standardista

IEEE 802.15.4. -standardin suunnittelun lähtökohta on tarjota sensoriverkolle lyhyen kantaman palveluita ilman tukiasemia. Standardi on suunniteltu tukemaan myös maantieteellisesti laajoja verkkoja, joissa voi olla paljon laitteita. HEED-protokolla toimii samalla periaatteella riippumatta laitteiden määrästä tai maantieteellisestä laajuudesta, solmu päättää klusteriin liittymisestään täysin paikallisen informaation perusteella. Keskeinen periaate molemmille protokollille on pidentää verkon elinikää toimimalla mahdollisimman energiatehokkaasti säästäen ja tasaten laitteiden virrankulutusta.

5.6.1 Topologia

IEEE 802.15.4. -standardi ei aseta vaatimuksia sensoriverkon topologialle. Se hyväksyy niin tähtitopologian, kuin mesh-, klusteri- ja klusteripuutopologiankin. HEED-klusteri on rakenteeltaan tähtitopologian mukainen, eli jokainen klusterin solmu on liittynyt suoraan pääsolmuun. Siten erityisesti tähtitopologialle suunniteltuja toimintoja voidaan soveltaa HEED-protokollassa klusterin sisäiseen toimintaan muulloin, kuin klusteroinnin aikana. HEED-protokolla ei ota kantaa klustereitten väliseen viestintään, eikä siihen, miten yhteys PAN-koordinaattoriin hoidetaan. HEED:iä voidaan siten ajaa myös klusteripuuverkoissa, joissa klustereitten keskinäinen hierarkkinen järjestäminen hoidetaan jonkin toisen protokollan avulla. Kumpikaan protokolla ei ota kantaa PAN-koordinaattorin valintaan, se voidaan hoitaa sovellukselle järkevimmällä tavalla, joita on kerrottu luvussa 3.2.1.

5.6.2 Verkon laitteet

IEEE 802.15.4. -standardi määrittelee sensoriverkkoon kahdenlaisia laitteita, FFD- ja RFD-laitteita. FFD-laitteet ovat älykkäämpiä ja pystyvät hoitamaan esimerkiksi pääsolmun tehtäviä. RFD-laitteet ovat yksinkertaisia, jotka pystyvät viestimään ainoastaan FFD-laitteen kanssa. HEED-algoritmia voidaan käyttää ainoastaan FFD-laitteille. Toki HEED-algoritmia hyödyntävässä verkossa voi olla myös RFD-laitteita, jotka liittyvät valittuun pääsolmuun, mutta eivät osallistu varsinaisen HEED-algoritmin toimintaan.

5.6.3 Viestintä ja tiedonsiirtomenetelmät

Klusterointi voi alkaa standardin määrittelemällä disassosiaatiolla, missä yhteydet pääsolmuun puretaan ennen HEED-algoritmin suorittamista. Klusteroinnin aikana on tarpeen jonkinlainen kanavanvarausmenetelmä, jotta yhteentörmäyksiltä vältytään pääsolmuehdokkaitten mainostaessa tilaansa. Standardin tarjoaman CSMA-CA-kilpavarausmenetelmän avulla laite lähettää tietonsa vasta, kun se havaitsee radiotien oleva vapaa. Klusteriin liittyminen voidaan aloittaa MAC-komentokehyksen ja kuittauskehysten avulla. Valituksi tullut pääsolmu lähettää muille laitteille standardin mukaisen MAC-komentokehyksen ja ohjaa muita liittymään siihen. Klusterin muut laitteet kuittaavat saaneensa viestin kuittauskehyksen avulla. Pääsolmuun liittymisessä voidaan hyödyntää myös assosiaatiota, missä solmut lähettävät valitsemalleen pääsolmulle assosiaatiopyynnön.

Klusterin sisäisessä viestinnässä ei käytetä multihop-viestintää, vaan jokainen klusterin solmu viestii vain pääsolmun kanssa. Klusteri hyötyy erityisesti superframe-rakenteesta, jonka avulla klusterin sisäinen viestintä voidaan organisoida ja tarvittaessa pääsolmu voi varata lähetysaikaa tietylle klusterin laitteelle. Standardi määrittelee MAC-kerroksellaan myös ACL-tunnistuspalvelun, jossa MAC ylläpitää tietoja laitteista, joiden kanssa se saa viestiä. Sen avulla laitteelle voidaan sallia viestiminen ainoastaan pääsolmun kanssa.

5.6.4 Tahdistaminen

Standardi tukee laitteiden matalaa virrankulutusta sallimalla lähettimien ja vastaanottimien olevan suurimman osan toiminta-ajastaan virransäästötilassa. Tämä aiheuttaa niissä

klusterointimenetelmissä hankaluuksia, joissa laitteiden tulee olla tahdistettuja klusteroinnin alkaessa. HEED-algoritmi toimii kuitenkin myös silloin, kun osa laitteista tahdistuu vasta klusteroinnin alettua. Niinpä myös tätä standardin ominaisuutta voidaan hyödyntää HEED-algoritmia käyttävässä verkossa. Standardi tarjoaa tuen myös laitteiden tahdistamiseen, sitä käsiteltiin luvussa 3.6.4.

5.6.5 Kanavaskannaus

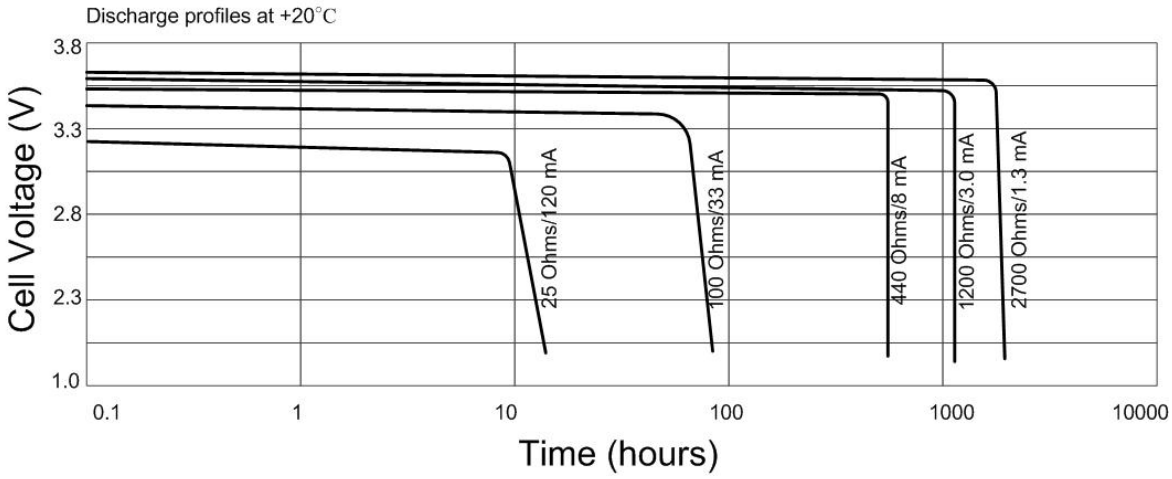
HEED-algoritmissa käytetään pääsolmun valinnassa kahta parametria, joista ensisijainen on solmun jäljellä oleva energia. Toissijainen parametri on vapaasti valittavissa ja esimerkiksi sellaisissa sovelluksissa, joissa laitteet voivat itse säädellä lähetystehoaan, voidaan toinen parametri sitoa pienimpään tarvittavaan lähetystehoon. Klusterin sisäistä viestinnän kustannusta voidaan siten arvioida näiden keskiarvon, AMRP:n, avulla. Standardi tarjoaa lähetystehon mittaamiseen kanavan energiamittauksen, ED-skannauksen. Energiamittauksessa haluttuja kanavia kuunnellaan ja jokaiselta mitataan suurin signaaliteho. Tätä voidaan HEED:ssä hyödyntää mittaamalla suurimman sijaan pienin signaaliteho. HEED hyötyy myös muista standardin kanavaskannausmenetelmistä. Orphan-kanavaskannauksen avulla laite voidaan liittää takaisin klusteriin, mikäli yhteys on vahingossa katkennut. Passiivisen ja aktiivisen kanavaskannauksen avulla voidaan ylläpitää tietoa naapurustosta, joten klusteroinnin alussa ei tarvita erikseen naapurikartoitusta.

5.7 Haasteita HEED-protokollan käytettävyyteen

HEED-protokollaa analysoidessa heräsi muutamia kysymyksiä, joihin algoritmi itsessään ei ota kantaa, kuten langattoman tiedonsiirron epävarmuus, paristojen virranpurkautuminen tai linkin vahvuus pääsolmua valitessa. Algoritmia havainnollistettiin Opnet-simulaattorilla Alvesin *ym.* [2] kehittelemän IEEE 802.15.4. -standardin mukaisen mallin päällä. Kokeilu toteutettiin 200 x 150 metrin kokoisessa verkossa sadalla solmulla joiden kuuluvuusalue oli 50 metriä. C_{tod}-arvoksi valittiin 5 % ja toissijaiseksi parametriksi solmun aste eli haluttiin hajauttaa pääsolmujen kuormaa. Varsinainen simulointi ja sen tulokset ovat tämän

tutkimuksen ulkopuolella ja ovat hyvänä pohjana jatkotutkimuksille. Muutamia ajatuksia ja huomioita tämä esiselvitys kuitenkin herätti.

Virrankulutus sensorilaitteiden paristoissa ei välttämättä ole lineaarinen. Yleensä energiataso pysyy pitkään muuttumattomana ja pariston eliniän loppuvaiheessa romahtaa hyvin nopeasti, kuten kuvan 16 [9] Elfa-pariston virtatason purkautumisprofiili näyttää. Siten solmu, joka näyttää korkeaa napajännitettä ja saa siten korkean CH_{tod}-arvon HEED-algoritmissa, voi todellisuudessa olla elinkaarensa loppupäässä. Tällöin voin käydä niin, että solmu valitaan pääsolmuksi, mutta se lopettaa toimimisensa heti klusteroinnin päätyttyä ja verkon yhtenäisyys on vaarassa.

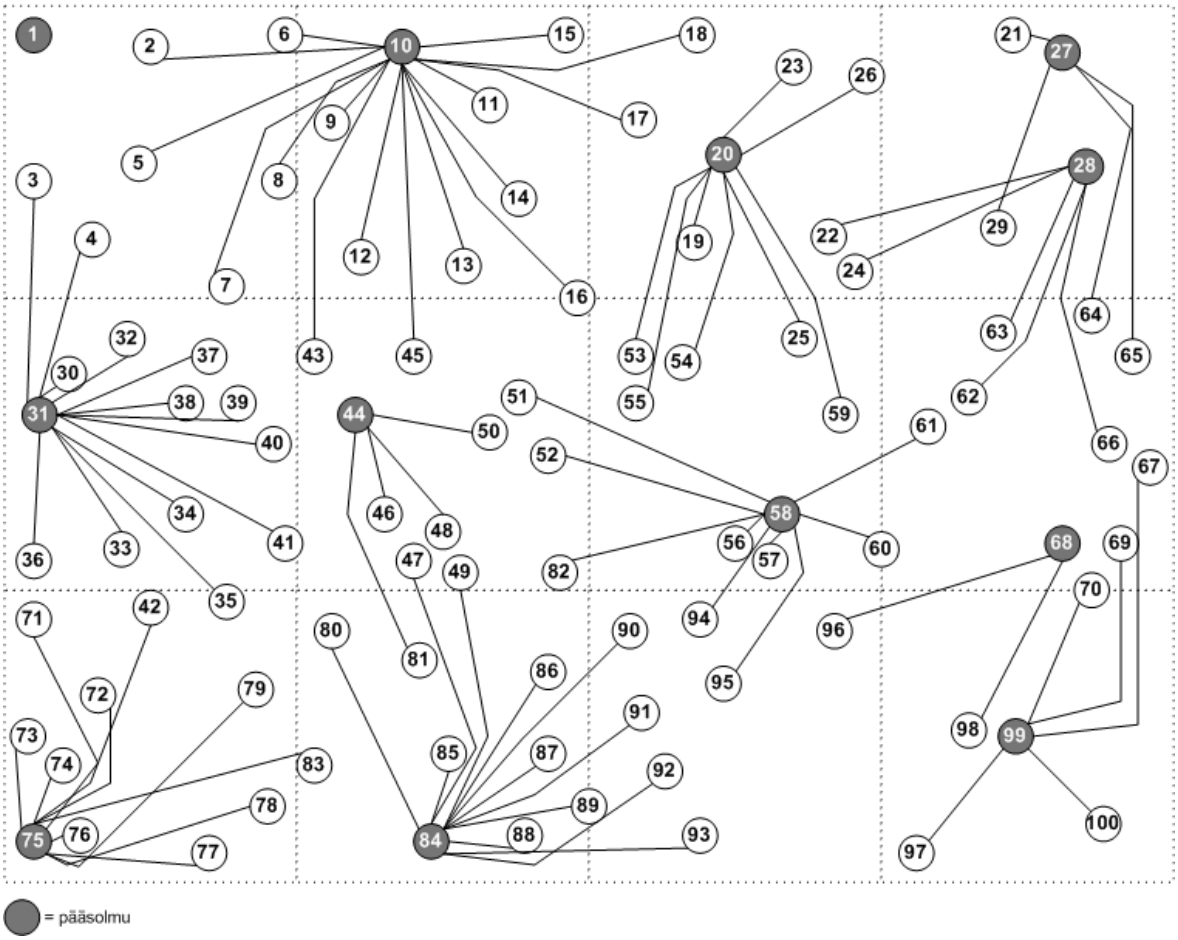


Kuva 16. Elfa-pariston virranpurkautumisprofiili [9].

Algoritmin toteutuksessa täytyy huomioida langattoman tiedonsiirron epävarmuus. Esimerkiksi algoritmin aloitusvaiheessa naapurustotietojen ja päätösvaiheessa pääsolmutietojen täytyy ehtiä päivittyä solmuihin. Voikin olla tarpeellista lisätä uusintalähetyksiä sekä algoritmin aloitus- että lopetusvaiheessa, jotta kaikkien sanomien perillepääsy varmistuu. Alustavissa kokeiluissa orpojen solmujen määrä väheni, kun uusintalähetyksiä ja satunnaisuutta lähetyksiin lisättiin. Verkon tahdistamiseen täytyy myös kiinnittää huomiota. Verkon solmuille täytyy saada tieto, että klusterointi on alkamassa, jotta ne voivat siihen osallistua.

Kokeilut selkeyttivät myös sitä, miksi että iterointikierroksia täytyy jokaisen solmun kohdalla jatkaa, kunnes sen CH_{tod} saavuttaa arvon yksi huolimatta siitä, että se on jo kuullut *final_CH* viestin joltain pääsolmulta. Siten solmuilla on valinnanvaraa, mihin pääsolmuun liittyä, mikäli niiden kuuluvuusalueella on useampia pääsolmuja. Painavimmat solmut liittyvät pääsolmuihin ensin ja toissijaisesta parametrista saadaan suurin hyöty irti. Muussa tapauksessa klustereitten koot ja kuormitus tulevat epätasaisiksi.

HEED-algoritmi ei huomioi linkin vahvuutta, jos solmut käyttävät vakiolähetystehoa, ellei sitä ole määritelty toissijaiseksi parametriksi. Naapuriklusterin ollessa kustannukseltaan edullisempi, solmu liittyy siihen, vaikka olisi järkevämpää liittyä lähempänä olevaan pääsolmuun. Esimerkiksi kuvassa 17 solmut 69 ja 70 ovat liittyneet pääsolmuun 99 solmun 68 sijaan. Tästä seuraa myös se, että klustereitten alueet eivät ole selvärajaisia vaan menevät osaksi päällekkäin.



Kuva 17. HEED-algoritmin simulaatiotulos.

Kokeilut osoittivat, että HEED-protokolla on toimiva ratkaisu langattoman sensoriverkon klusterointiin, mikäli toteutuksessa huomioidaan myös langattoman tiedonsiirron epävarmuustekijät. Tämä esiselvitys luo hyvän pohjan jatkotutkimuksille.

6 Yhteenveto

Lyhyen kantaman langattomat sensoriverkot ovat teollisuuteen tai muuhun ympäristöön tarkoitettuja tiedonkeruujärjestelmiä. Ne tarjoavat muita langattomia teknologioita matalaenergiaisemman ja halvemman vaihtoehdon langattomaan tiedonsiirtoon erityisesti sellaisille sovellusalueille, joissa tiedonsiirtokapasiteetista voidaan tinkiä. Siinä missä WLAN ja Bluetooth -standardit luotiin tarkasti määritellyille sovellusalueille, sensoriverkkojen sovellusalueet vaihtelevat suuresti.

Langattomien sensoriverkkojen käytön odotetaan nousevan tulevaisuudessa räjähdysmäisesti niiden edullisuuden ja sovelluskohteitten suuren määrän ansiosta. Sovellusalueita löytyy niin kotitalouksien, teollisuuden ja kaupan sektoreilta, kuin myös lääketieteen, sotatieteen ja ympäristötieteiden aloilta. Niiden avulla pystytään valvomaan kohteita, joissa kulku on vaarallista tai mahdotonta, sekä esimerkiksi antamaan täsmällistä, reaaliaikaista tietoa tietyn alueen olosuhteista, esimerkiksi maataloudessa ja teollisuudessa. Nykyautoissa käytetään runsaasti erilaisia sensoreita lisäämään ajomukavuutta ja tarjoamaan kulkuneuvon hallintaan lisäominaisuuksia. Kodin elektroniikka, taloautomaatio ja turvallisuus sekä lelut ja pelit ovat myös potentiaalisia sensoriverkkoteknologian kohteita.

Suurimmat haasteet langattomien sensoriverkkojen toteuttamisessa koskevat laitesuunnittelua, topologian hallintaa ja tiedonsiirtoprotokollia. Sensoriverkossa voi olla satoja, jopa tuhansia laitteita tiheästi sijoitettuna. Yhden laitteen valmistuskustannukset eivät niin ollen saa nousta korkeaksi. Keskeistä laitesuunnittelussa on paristonkesto, koska usein laitteet sijoitetaan kohteeseen, jossa niiden huoltaminen, korjaaminen tai paristonvaihto on hankalaa, jopa mahdotonta. Paristonkesto voi olla siten käytännössä laitteen elinikä. Lisäsensoreitten sijoittaminen täytyy olla mahdollista koko verkon elinkaaren ajan korvaamaan toimimattomia sensoreita ja suorittamaan lisätehtäviä. Laitteita myös poistuu verkosta virran loppumisen tai ympäristöolosuhteitten muutoksen johdosta. Verkon topologian suunnittelu ja hallinta on erityisen tärkeää, koska muutoksiin täytyy pystyä sopeutumaan ilman, että verkon yleinen toiminta häiriintyy. Sensoriverkkojen täytyy olla myös itseorganisoituvia, koska suuren solmumäärän

käsinkonfigurointi on mahdotonta. Tiheissä verkoissa siirrettävän datan ruuhkautumisen ja kehysten törmäämisen vaara on suuri. Niinpä kehysten samanaikaista lähettämistä on rajattava toistensa kuuluvuusalueella olevissa laitteissa topologian hallinnan ja tiedonsiirtoprotokollien avulla.

IEEE julkaisi vuonna 2003 802.15.4-standardin langattomille sensoriverkoille. Standardista julkaistiin päivitetty versio vuonna 2006 ja sen keskeinen ominaisuus on lyhyen kantaman palvelut ilman tukiasemia ja kyky tukea myös hyvin laajoja verkkoja. Standardi määrittelee ainoastaan protokollapinon alimmat kerrokset, fyysisen ja MAC-kerroksen. Fyysinen kerros on vastuussa laitteen radiolähettimen ja -vastaanottimen ohjauksesta, käytetyn kanavan energian ja yhteyden laadun mittaamisesta, vapaan kanavan valinnasta ja kanavanvarauksesta. Se myös lähettää sanomat radiotielle ja vastaanottaa ja välittää ne MAC-kerrokselle. MAC-kerroksen tärkeimmät tehtävät ovat verkon infrastruktuurin luominen sekä yhteysresurssien tehokas ja oikeudenmukainen jakaminen laitteiden välillä. Standardi ei määrittele verkonmuodostuksen yksityiskohtia, ainoastaan MAC-kerroksen tuen sille, kuten esimerkiksi verkkoon liittymisen ohjaaminen, tahdistaminen ja beacon-sanomien generointi.

Standardin lisäksi verkonmuodostukseen tarvitaan erikoistuneita menetelmiä pitämään verkon topologia hallittuna, verkon energiankulutus mahdollisimman alhaisena ja kuormitus tasaisena. Verkonhallintaprotokollat on yleensä tehty järeämmille laitteille, kuin sensoriverkossa käytetään, joten niihin suunnitellut tekniikat ja protokollat eivät sovellu langattomiin sensoriverkkoihin sellaisenaan. Sensoriverkon tiheä rakenne korostaa joitakin sille tyypillisiä ongelmia, kuten tiedonkulun häiriöitä ja reitityksen monimutkaisuutta. Topologian hallinnan avulla rajoitetaan tarkoituksella aktiivisten solmujen ja linkkien toimintaa tavoitteena solmujen virrankulutuksen vähentäminen ja verkon tiedonsiirtokapasiteetin nostaminen. Useissa sensoriverkkosovelluksissa riittää, että tukiasemalle siirretään vain tarpeellinen tieto, ei kaikkea kerättyä tietoa. Klusterointi onkin todettu tehokkaaksi tavaksi organisoida verkko. Ryhmän pääsolmu kerää tiedot ryhmän muilta solmuilta, käsittelee sen ja lähettää edelleen PAN-koordinaattorille. Koska pääsolmut kuluttavat energiaa enemmän kuin ryhmän muut solmut, kannattaa sensoriverkko klusteroida uudelleen säännöllisesti.

HEED-protokolla on energiatehokas klusterointiprotokolla sensoriverkoille. Se pidentää verkon elinikää tasaamalla energiankulutusta pääsolmuvastuuta kierrättämällä. Klusterointi on täysin hajautettua ja päättyy vakioajassa vaatien vain vähän solmujen välistä tiedonvaihtoa ja datan prosessointia. HEED-algoritmin tuloksena pääsolmut kattavat hyvin koko verkon alueen ja klusterin muut solmut ovat yhden hypyn päässä pääsolmusta. HEED käyttää kahta parametria klusteroinnissa. Ensisijaisena parametrina on solmun jäljellä oleva energia ja toissijaisena jokin klusterille toivottu ominaisuus, esimerkiksi koko. HEED-protokollan etuna on sen soveltuvuus monentyyppisiin sensoriverkkosovelluksiin. Se ei aseta vaatimuksia solmujen sijainnille, määrälle tai verkon maantieteelliselle koolle. HEED on myös täysin paikallinen menetelmä, joten solmujen sijaintitietoa ei tarvita.

IEEE 802.15.4 -standardi ja HEED-protokolla sopivat hyvin samoihin sovelluksiin. Standardissa määritellään useita niitä menetelmiä, jotka ovat tarpeellisia HEED-protokollassa, kuten kanavaskannaus- ja kanavanvaraus-menetelmät. HEED-klusteri on tähtitopologian mukainen, se hyötyy siten myös standardin tähtitopologioille määrittelemistä toiminnoista, kuten superframe-rakenne klusterin sisäisessä tiedonsiirrossa. Sekä IEEE 802.15.4 -standardin että HEED-protokollan tavoitteet sensoriverkon ominaisuuksille ovat samat. Molemmissa on huomioitu sensoriverkon matala ja tasainen energiankulutus eikä verkon koko määrällisesti tai maantieteellisesti rajoita niiden soveltamista.

HEED-algoritmi ei sinänsä ota kantaa muutamiin langattoman sensoriverkon keskeisiin ominaisuuksiin. Näitä ovat esimerkiksi paristojen virranpurkautumisprofiilin vaikutus pääsolmun valinnassa, linkin vahvuus tai langattoman tiedonsiirron epävarmuus. Alustavat HEED-protokollan kokeilut IEEE 802.15.4. -standardin mukaisen mallin päällä herättävätkin mielenkiintoisen aiheen seuraaville tutkimuksille.

Lähteet

[1] Akyildiz I., Cayirci E., Sankarasubramaniam Y. ja Su W., *A Survey on Sensor Networks*, IEEE Communications Magazine, vol. 40, No. 8 (2002), s. 102–114.

[2] Alves M., Hanzálek Z., Jurčík P., Koubâa A. ja Tovar E., *A Simulation Model for the IEEE 802.15.4 Protocol: Delay/Throughput Evaluation of the GTS Mechanism*, kirjassa "15th IEEE International Symposium on Modeling, Analysis and Simulation", IEEE Computer Society, 2007, to appear.

[3] Balakrishnan H., Chandrakasan A. ja Heinzelman W., *An Application-Specific Protocol Architecture for Wireless Microsensor Networks*, IEEE Transactions on Wireless Communications, vol. 1, No. 4 (2002), s. 660–670.

[4] Barrett R. Jr, Callaway E. Jr. ja Gutiérrez J., "Low-Rate Wireless Personal Area Networks, Enabling Wireless Sensors with IEEE 802.15.4", The Institute of Electrical and Electronics Engineers, Inc., New York, 2003.

[5] Berry V., Lamb S., Lapinski M., Newman M., Sexton D. ja Werb J., *Improved Quality of Service in IEEE 802.15.4 Mesh Networks*, kirjassa "International Workshop on Wireless and Industrial Automation (WIA'05)", 11th IEEE Real-Time and Embedded Technology and Applications Symposium, 2005.

[6] Bhardwaj M., Chandrakasan A., *Bounding the lifetime of sensor networks via optimal role assignments*, kirjassa "Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2002)", IEEE Computer Society, s. 1587–1596, 2002.

[7] Chong C. ja Kumar S., *Sensor Networks: Evolution, Opportunities, and Challenges*, Proceedings of the IEEE, vol. 91, No. 8 (2003), s. 1247–1256.

[8] Cipollone E., Cuomo F., Della Lunaa S., Suihko T. ja Todorova P., *Topology formation in IEEE 802.15.4: cluster-tree characterization*, kirjassa "Proceedings of the 6th Annual IEEE International Conference on Pervasive Computing and Communications (IEEE PERCOM 2008)", IEEE Computer Society Press, s. 276-281, 2008, to appear.

[9] Elfa Oy, "Produktinformation, ELFA artikelnr 69-285-01 Batteri Li 3,6V LS17500, 69-285-27 Batteri Li 3,6V LS17500 CNR", saatavilla WWW-muodossa <URL: https://www1.elfa.se/data1/wwwroot/webroot/Z_DATA/0c837e90-7ad1-11dc-9199-0019bbdf5d02.pdf>, 11.6.2002.

[10] Estrin D., Govindan R., Heidemann J., Intanagonwiwat C. ja Silva F., *Directed Diffusion for Wireless Sensor Networking,* IEEE/ACM Transactions on Networking (TON), IEEE Press, vol. 11, No. 1 (2003), s. 2–16.

[11] Estrin D., Krishnamachari B., ja Wicker, S., *The Impact of Data Aggregation in Wireless Sensor Networks*, kirjassa "Proceedings of 22nd International Conference on Distributed Computing Systems Workshops, 2002", IEEE Computer Society, s. 575–578, 2002.

[12] Fahmy S. ja Younis O., *HEED: a hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks,* IEEE Transactions on Mobile Computing, IEEE Press, vol. 3, No. 4 (2004), s. 366–379.

[13] Granlund K., "Tietoliikenne", Docendo Finland Oy, Jyväskylä, 2003.

[14] Ha´c A., "Wireless Sensor Network Designs", John Wiley & Sons, Inc., England, 2003.

[15] Haghighat A., Honary M., Shokrzadeh H. ja Tashtarian F., *A New Energy-Efficient Clustering Algorithm for Wireless Sensor Networks*, kirjassa "15th International Conference on Software, Telecommunications and Computer Networks (SoftCOM 2007)", IEEE Communication Society, s. 1–6, 2007.

[16] Hu H., Luo J. ja Zhang Y., “Wireless Mesh Networking”, Taylor and Francis Group, USA, 2007.

[17] IBM, ”Beacon Institute and IBM Team to Pioneer River Observatory Network”, saatavilla WWW-muodossa <URL: http://www-03.ibm.com/press/us/en/pressrelease/22162.wss>, 16.8.2007.

[18] IEEE Computer Society, ”IEEE Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs)”, the Institute of Electrical and Electronics Engineers, Inc., USA, 2006.

[19] IEEE 802 LAN/MAN Standards Committee, “IEEE 802.15 WPAN™ Task Group 4 (TG4)”, saatavilla WWW-muodossa <URL: http://www.ieee802.org/15/pub/TG4.html>, 11.9.2006.

[20] IETF Secretariat, “IPv6 over Low power WPAN (6lowpan)”, saatavilla WWW-muodossa <URL: http://www.ietf.org/html.charters/6lowpan-charter.html>, 16.4.2007.

[21] Jennic Ltd, “Preliminary Data Sheet – JN5139-xxx-Myy”, saatavilla WWW-muodossa <URL: http://www. jennic.com/files/support_files/JN-DS-JN5139MO-1v2.pdf>, *viitattu 14.10.2007*.

[22] Karl H. ja Willig A., “Protocols and Architectures for Wireless Sensor Networks”, John Wiley & Sons Ltd, England, 2005.

[23] Krishnamachari B., “Networking Wireless Sensors”, Cambridge University Press, U.K., 2005.

[24] Krunz M., Ramasubramaniam S. ja Younis O., *Node Clustering in Wireless Sensor Networks: Recent Developments and Deployment Challenges*, IEEE Network, vol. 20, No. 3 (2006), s. 20–25.

[25] Lehto A. ja Räisänen A., ”Radiotekniikan perusteet”, Oy Yliopistokustannus/Otatieto, Helsinki, 2001.

[26] Levy R., Li J. ja Yu M., *Mobility Resistant Clustering in Multi-Hop Wireless Networks*, Journal of Networks, vol. 1, No. 1 (2006), s.12–19.

[27] MacQueen, J., *Some methods for classification and analysis of multivariate observations*, kirjassa “Proceedings of the Fifth Symposium on Math, Statistics and Propbability”, University of California Press, s. 281–297, 1967.

[28] Madria S. ja Tubaishat M.*, Sensor Networks: An Overview*, IEEE Potentials, vol.22, No.2 (2003), s. 20–23.

[29] Mhatre V. ja Rosenberg C., *Design guidelines for wireless sensor networks: communication, clustering and aggregation*, The Ad Hoc Networks, vol. 2, No. 1 (2004), s. 45–63.

[30] Mhatre V. ja Rosenberg C., *Homogenous vs. heterogenous Clustered Sensor Networks: A Comparative Study*, kirjassa “2004 IEEE International Conference on Communications (ICC 2004)”, IEEE Communications Society, s. 3646–3651, 2004.

[31] Puska M., “Lähiverkkojen tekniikka”, Satku-Kauppakaari, Helsinki, 2000.

[32] Ramanathan R. ja Redi J., *A Brief Overview of Ad Hoc Networks: Challenges and Directions*, IEEE Communications Magazine, vol. 40, No. 5 (2002), s. 20–22.

[33] Royer E. ja Toh C-K., *A Review of Current Routing Protocols for Ad-Hoc Mobile Wireless Networks*, IEEE Personal Communications, vol. 6, No. 2 (1999), s. 46–55.

[34] Santi P., “Topology Control in Wireless Ad Hoc and Sensor Networks”, John Wiley & Sons Ltd, England, 2005.

[35] Schwedick H. ja Wolf A., *PSSS - parallel sequence spread spectrum a physical layer for RF communication*, kirjassa “Proceedings of 2004 IEEE International Symposium on Consumer Electronics”, IEEE Conference proceedings, s. 262–265, 2004.

[36] Tikkakoski M., ”LR-WPAN sensoriverkkotekniikkana”, Tietotekniikan pro gradu-tutkielma, Jyväskylän yliopisto, (2003).

[37] Viestintävirasto, ”Määräys luvasta vapaiden radiolähettimien yhteistaajuuksista ja käytöstä. (Viestintävirasto 15W/2006 M)”, saatavilla WWW-muodossa <URL: http://www.ficora.fi/attachments/suomi_R_Y/1158858976905/Files/CurrentFile/Viestintavirasto15W2006M.pdf>, 3.8.2006.

[38] Zimmermann H., *OSI Reference Model-The ISO Model of Architecture for Open Systems Interconnection*, IEEE Transactions on Communications, vol. 28, No. 4 (1980), s. 425–432.