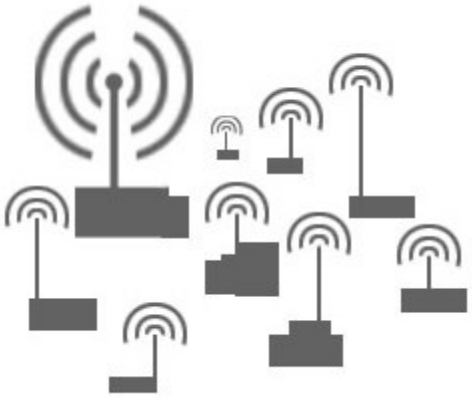
Tallinna Tehnikaülikool
Automaatikainstituut

Taivo Lints
990849LASM

Multihop / Mobiilsed ad hoc võrgud

Referaat aines "Arvutivõrgud" LAP5733
Õppejõud: Rein Paluoja



Tallinn 2004

Sisukord

Autori kontaktandmed
taivo@vkg.werro.ee
http://www.dcc.ttu.ee/taivo/

1. Sissejuhatus

Infotehnoloogia areng on jõudnud etappi, kus omavahel traadita side abil suhelda soovivate digitaalseadmete arv järsult kasvab. Mobiiltelefonide laialdane kasutuselevõtt ning süle- ja pihuarvutitega reisijad on selle arengu silmapaistvam osa, kuid ilmselt jäävad need siiski vaid "jäämäe tipuks". Nimelt on oodata ka selliste seadmete arvu väga suurt kasvu, mille suhtlemine võrgu kaudu on oluliselt autonoomsem ega eelda inimese kohalolekut: alates "intelligentsetest" kodumasinatest kuni "targa tolmuni" ehk tillukeste sensoriteni, mis kommunikatsiooniks kasutavad optilist ja raadiosidet ning mida võidakse vaadeldavasse piirkonda puistata tohututes kogustes (näiteks kümnetes või sadades tuhandetes).

Võrgustatud seadmete arvu plahvatuslik kasv toob kaasa arvutivõrkude kvalitatiivse arengu, sest senikasutatud põhimõtted ei taga paljudel juhtudel enam rahuldavat tulemust. Käesolev referaat vaatlebki üht olulist arvutivõrkude arengusuunda: *multihop* ja / või mobiilseid *ad hoc* võrke.

Märkus: Tõlkeküsimuste lahendamisel on prioriteediks valitud arusaadavus, mitte keele-arendus. Kui eestikeelne termin on vähelevinud või puudub, siis on esitatud kas mõlemad keeled või ainult inglise keel.

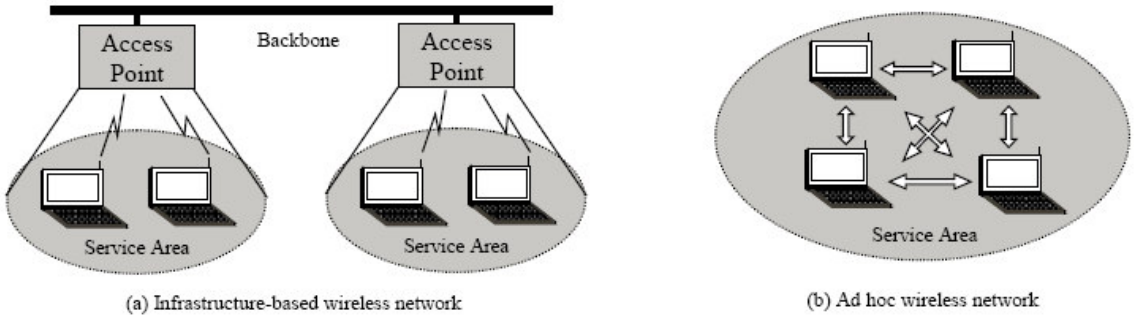
2. Ülevaade valdkonnast

2.1. Mis on *multihop* / mobiilsed *ad hoc* võrgud?

> Mobiilsed *ad hoc* võrgud (MANET'd) on keerulised hajussüsteemid, mis koosnevad mobiilsetest traadita sidet kasutavatest võrgusõlmedest, mis võivad dünaamiliselt organiseeruda, moodustades suvalisi ajutisi *"ad hoc"* võrgutopoloogiaid, võimaldades inimestel ja seadmetel probleemideta suhelda piirkondades, kus puudub eelnevalt rajatud side infrastruktuur. [1]
>
> *Single-hop ad hoc* võrk ühendab ainult seadmeid, mis on kaetud sama saate / vastuvõtupiirkonnaga. Seda piirangut on võimalik ületada, kasutades *multihop ad hoc* (MANET) tehnoloogiat. Funktsionaalsust, mida tavaliselt võimaldab olemasolev võrgu infrastruktuur (nt. marsruuterid, kommutaatorid *(switch)*, serverid), pakuvad MANET korral mobiilsed seadmed koostööd tehes. Otsest ühendust mitteomavad seadmed saavad omavahel suhelda parajasti nende vahel asuvate seadmete vahendusel. [2]

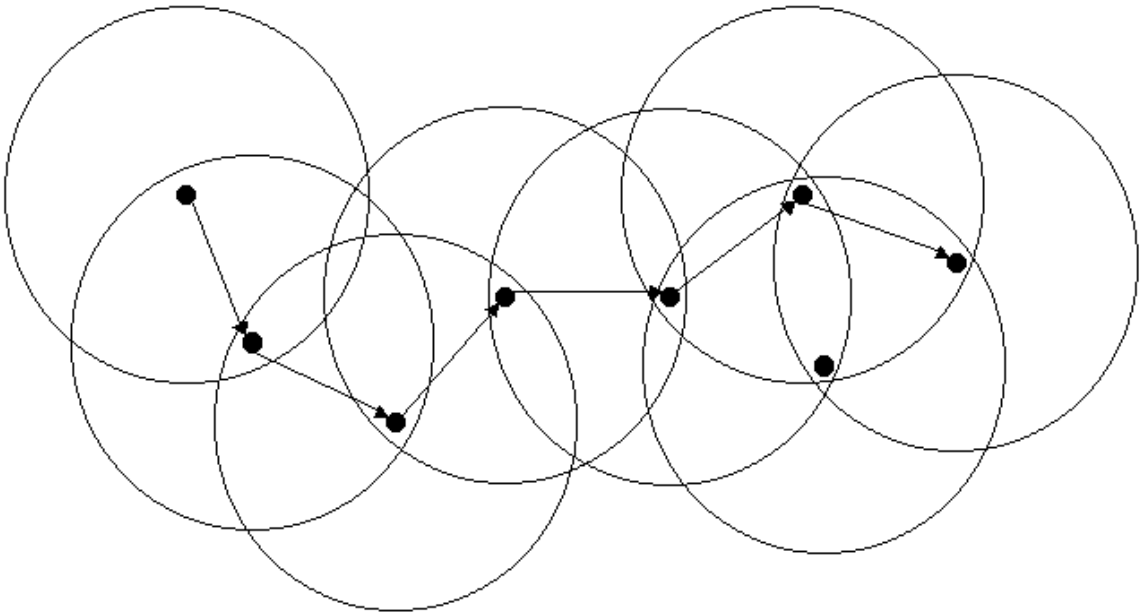
Toodud definitsioonidest võib näha, et "M" lühendis MANET võib sõltuvalt artikli autorist tähistada nii mobiilsust kui *multihop* põhimõttel sidet. Need ei ole üksteist välistavad ega ka täielikult kattuvad mõisted. Käesolevas referaadis vaadeldakse üldjuhul kõige keerulisemat varianti – mobiilseid *multihop ad hoc* võrke – mis hõlmab mõlemad nimetatud võimalused (ka staatilist võrku võib vaadelda mobiilse võrgu erijuhuna, kus võrgusõlmed on parajasti seisma jäänud ning suhtlemine sellevõrra lihtsam).

Termin "*ad hoc* võrk" tähendab, et võrgu struktuur ei ole eelnevalt kindlaks määratud, vaid moodustub kohapeal sõltuvalt olukorrast ning võib seejuures olla dünaamiline, pidevalt muutuv. Eesti keeles võib sellist võrku nimetada näiteks spontaanvõrguks. Et mõista paremini *ad hoc* võrgu erinevust laialt levinud infrastruktuuripõhisest traadita võrgust, vaata järgnevat joonist:



Joonis 1. Traadita võrk eelnevalt rajatud infrastruktuuriga (a) ja spontaanvõrguna (b). [3]

Terminiga *"multihop*" tähistatakse olukorda, kus infopakett peab adressaadini jõudmiseks läbima mitu võrgusõlme ehk tegema mitu "hüpet" (joonis 2).



Joonis 2. *Multihop* põhimõtte näide. Mustad ringid on võrgusõlmed. Ringjooned tähistavad võrgusõlmede saateraadiuseid. Selleks, et kõige vasakpoolsema seadme saadetud pakett jõuaks kõige parempoolsemani, peab see liikuma läbi vahepealsete seadmete, sooritades antud juhul 6 hüpet. [4]

2.2. MANET ajalugu

Dünaamiliste traadita võrkude kasutamine ei ole uus idee. Selle praeguse populaarsuse ja leviku järsu tõusu taga seisab tehnoloogia areng, mis on MANET'de loomiseks sobivad seadmed muutnud piisavalt kättesaadavaks, aga militaarorganisatsioonides on vastava uurimistööga tegeldud juba aastakümneid. Järgnevas on artiklit [1] kasutades toodud lühiülevaade MANET arengust.

Üheks esimeseks *ad hoc* võrgu rakenduseks võib pidada DARPA *Packet Radio Network* (PRNet) projekti aastast 1972 (DARPA – *Defence Advanced Research Projects Agency* – on USA Kaitseministeeriumi alluvuses olev asutus, mille eesmärgiks on luua sõjaväele uusi tehnoloogilisi vahendeid). PRNet oli minimaalse keskse juhtimisega raadiojaamade võrk, mis kasutas *multihop store-and-forward* marsruutimist, võimaldades katta väga suuri geograafilisi alasid.

PRNet oli aga siiski üsna algeline. Tõsisteks probleemideks olid vähene skaleeruvus, turvalisus, võrgusõlmede arvutusvõimsus ja energiasäästlikkus. Nende küsimustega hakkas aastal 1983 tegelema projekt *Survivable Radio Networks* (SURAN), mille põhieesmärgiks oli võimaldada turvalise kümneid tuhandeid seadmeid sisaldava võrgu loomist ning seejuures kasutada väikseid odavaid madala energiatarbega raadioid, mis suudaks toetada keerukaid pakettside protokolle. Projekti tulemusena valmis aastaks 1987 *Low-cost Packet Radio* (LPR) tehnoloogia, mis põhines digitaalselt juhitaval *Direct Sequence Spread Spectrum* (s.t. hajutatud spektriga, kuid mitte ühelt sageduselt teisele hüppaval) raadiol koos Intel 8086 protsessoril põhineva paketikommutaatoriga. Võrgu skaleeruvuse tagas dünaamilisel rühmitumisel baseeruv hierarhiline topoloogia.

1980-te aastate lõpus ja 90-te alguses toimunud Interneti infrastruktuuri areng ja arvutite laiem levik õigustasid paketipõhise raadio ideed ning aastal 1994 sai alguse *DARPA*

Global Mobile (GloMo) *Information Systems* programm, mille eesmärgiks oli võimaldada traadita seadmete ühilduvust *Ethernet* tüüpi võrkudega "igal ajal ja igal pool".

Senini ilmselt suurim realiseeritud traadita *multihop* pakettraadiovõrk on 1997. aastal USA sõjaväes kasutusele võetud *Tactical Internet* (TI). Mastaapne oli ka 1999. aastal sooritatud *Extending the Littoral Battlespace Advanced Concept Technology Demonstration* (ELB ACTD), kus horisondi taha jäävate laevade ühendamiseks MANET võrku kasutati mitmesuguseid mehitamata ning mehitatud õhusõidukeid.

Alates 1990-te keskpaigast on järjest suuremat huvi pakkunud MANET põhimõtete kasutamine ka tsiviilelus. Esialgu toimus uurimistöö peamiselt akadeemilises keskkonnas, kuid pärast selle tehnoloogia tohutu ärilise potentsiaali märkamist on tõsiselt huvi tundma hakanud ka mitmesugused ettevõtted. Esimesed tooted on ka juba turule jõudnud, näiteks firmadelt MeshNetworks (http://www.meshnetworks.com/) ja SPANworks (http://www.spanworks.com/). Ka *Bluetooth* tehnoloogia põhineb *ad hoc* võrkude ideel.

2.3. Raskused ja probleemid MANET'de valmistamisel

Mobiilsete *ad hoc* võrkude üldpõhimõte on lihtne – kui ise ei suuda teadet otse adressaadini kiirata, siis tuleb kasutada teiste parajasti läheduses olevate võrgusõlmede abi. Aga reaalse võrgu kavandamisel ja realiseerimisel kerkib esile suur hulk probleeme. Järgnev allikatel [3], [5] ja [6] põhinev nimekiri ei ole kindlasti täielik, kuid annab ettekujutuse võimalikest raskustest. Mõnedest siin lühidalt esitatud probleemidest tuleb põhjalikumalt juttu hilisemates peatükkides.

Signaalilevi (füüsikalised) probleemid: peegeldused, difraktsioon, hajumine, tõkked saatjate vahel, muutuv keskkond, müra, saatjate omavaheline üksteise segamine.

Juhuslik ja muutuv võrgu topoloogia: seadmed liiguvad üksteise ja keskkonna suhtes (mõnikord väga kiiresti, kui seade on autos või lennuvahendis), keskkond ise muutub (levitõkked saatjate vahel võivad tekkida ja kaduda), seadmed võivad sisse ja välja lülituda.

Adresseerimine: fiksvõrkudes kasutatav IP aadress lähtub eelkõige seadme asukohast. Ka "mobiilse IP" kontseptsioon põhineb sellel, et seadmel on kusagil stabiilses võrgus oma "kodu" ning ainult mõnikord liigutakse mujale. Sel juhul saadab vastav agent koduaadressile saabunud paketid edasi mobiilse seadme ajutisse asukohta (fiksvõrgu mõni teine punkt) ning mobiilne seade võib seejärel soovitada vestluskaaslasel pakette otse uude punkti saata. Aga MANET korral on tavaliselt aadress seotud otseselt seadmega, mitte topoloogilise asukohaga.

Marsruutimine ja ühenduse loomine: tavaliselt ei ole MANET's eraldi marsruutereid, vaid iga võrgusõlm peab vajadusel sellega tegelema. Mobiilses *ad hoc* võrgus on tihti raske või isegi võimatu luua kahesuunalist ühendust. Seega sõnumi kättesaamise kinnitus võib tagasi tulla hoopis mõnda muud teed pidi või üldse tulemata jääda.

"Koonduvus": Interneti marsruutimisprotokolle on alati loodud eeldusega, et võrk liigub ühest stabiilsest ("koondunud") olekust teise läbi aeg-ajalt toimuvate muutuste (ühenduste ja seadmete lisandumine või kadumine) ning neid muutusi vaadeldakse häireolukorrana, kus tuleb kiiresti muuta marsruuterite seadistust. MANET korral toimub aga pidev topoloogia muutumine ning hoopis stabiilne olek on erijuht. Tuleb esitada küsimus, kas tugevat koonduvust on üldse mõtet eesmärgiks seada, sest selle saavutamine on ressursimahukas tegevus.

Kõrgema taseme protokollide töö: näiteks suurema infoterviku transportimine ühest (liikuvast) punktist teise (liikuvasse) punkti ilma kadudeta; teenuste kvaliteedi tagamine.

Skaleeruvus: et võrk töötaks ka väga suure võrgusõlmede arvu korral.

Turvalisus ja usaldusväärsus: võrku võivad ohustada pealtkuulamine, pahatahtlike võrgusõlmede lisandumine, mobiilsuse ja kehva signaalilevi tagajärjel tekkivad vead andmetes.

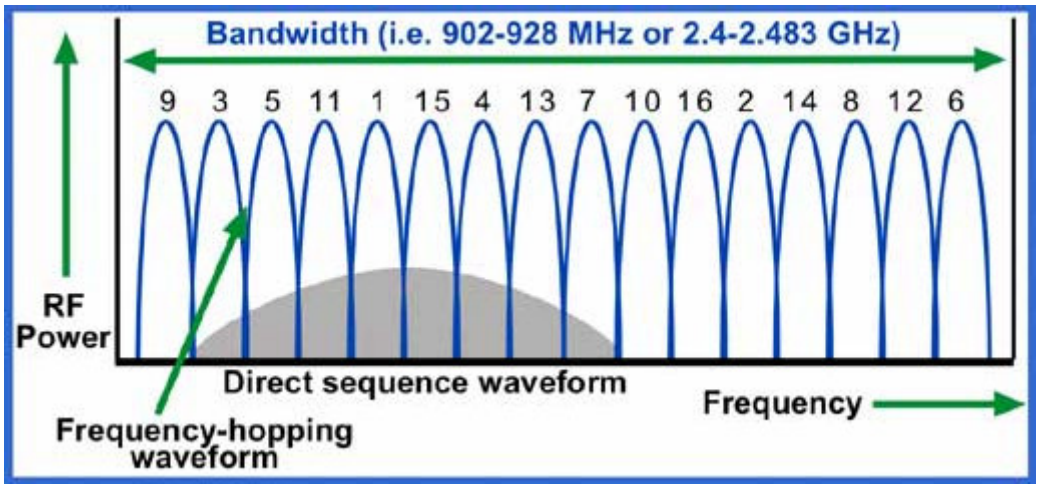
Võrgusõlme piirangud: enamasti on MANET võrgusõlmed väikesed mobiilsed seadmed piiratud arvutusvõimsuse ja mälumahuga ning vähese energiatagavaraga. Samas võrgus võivad olla väga erinevate piirangutega sõlmed.

Loomulikult ei ole lahenduste leidmiseks vaja kõike nullist alustada – mitmete probleemidega (näiteks raadiosignaali levimisega) on teistes valdkondades juba põhjalikult tegeldud. Paljud küsimused on aga siiski MANET-spetsiifilised ning vajavad põhjalikumat uurimistööd.

3. MANET arengut soodustavad standardid ja tehnoloogiad

Kuigi mobiilsete *ad hoc* võrkude idee ei ole uus ja leidis sõjanduses rakendust juba 1970-tel aastatel, seisis selle jõudmine tsiviilellu pikka aega tehnoloogia arengu taga. Alates 1990-te aastate keskpaigast hakkasid aga valmima ja populaarsust võitma mitmesugused traadita andmeside standardid, milledega ühilduvaid tooteid järjest enam ja odavamalt pakutakse. Selliste seadmete suur levik ongi loonud soodsa pinnase huvi järsuks tõusuks MANET vastu. Käesolev peatükk kirjeldab lühidalt neid arengut soodustavaid standardeid, põhinedes peamiselt allikatel [1] ja [7].

Kuna enamikul juhtudest on raadioeetri kasutamisel tegu kas *Direct Sequence Spread Spectrum* või *Frequency Hopping Spread Spectrum* põhimõttega, siis parema arusaadavuse huvides siinkohal lühike seletus.



Joonis 3. DSSS ja FHSS. [8]

Direct Sequence Spread Spectrum (otsejadaga hajaspekter) – infosignaal hajutatakse laiali üle fikseeritud sagedusvahemiku, korrutades teda läbi nii saatjale kui vastuvõtjale teada-oleva pseudojuhusliku signaaliga, millel on infosignaalist palju kõrgem sagedus [9], [10].

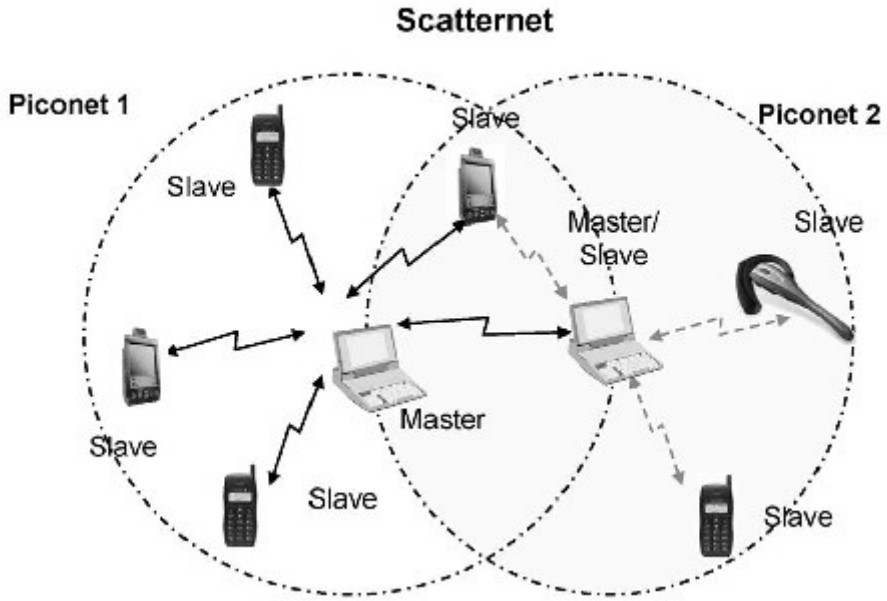
Frequency Hopping Spread Spectrum (sagedushüplemisega hajaspekter) – infosignaali kandesagedust muudetakse kiiresti nii saatjale kui vastuvõtjale teada oleva pseudo-juhusliku jada alusel: kandesagedus hüpleb etteantud sageduspiirkonnas ühelt kanalilt teisele [9], [11].

3.1. Bluetooth

Bluetooth spetsifikatsiooni loomine toimus suure hulga infotehnoloogiafirmade koostöös ning hetkel on see *de facto* standard üksteise lähinaabruses (kuni 10 meetrit) asuvate seadmete vahele raadioühenduse loomiseks. Eelkõige on *Bluetooth* kasutusel mitmesugustes väikestes mobiilsetes seadmetes nagu mobiiltelefonid ning pihu- ja sülearvutid.

Bluetooth töötab 2,4 GHz sagedusalas *Frequency Hopping Spread Spectrum* põhimõttel, saatevõimsus on alla 1 mW, andmeside kiirus kuni 1 Mbps (see sisaldab ka teenindusinfot, nii et kasuliku info liikumiskiirus on mõnevõrra väiksem).

Seadmete rollid *Bluetooth* võrgus ei ole eelnevalt ette kirjutatud, vaid määratakse kohapeal, nii et tegu on *ad hoc* võrguga. Tõsi küll, koheselt moodustatakse tähtvõrk nimega "*piconet*", mille keskel asub *master*, kes saab suhelda kuni seitsme aktiivse *slave*'ga (aadressiväli on kolmebitine). *Slave* võib pakette saata vaid siis, kui *master*'ilt saatekutse *(polling message)* saab. Vajadusel võivad rollid muutuda ning *master*'iks hakkab mõni teine seade. *Piconet* on *single hop* võrk, kuid olemas on ka võimalus moodustada suuremaid *multihop* võrke nimega "*scatternet"*, kus mõned seadmed kuuluvad korraga mitmesse *piconet*'i ja on seega vahendaja rollis (joonis 4). Kuigi *Bluetooth* spetsifikatsioon lubab *scatternet*'i moodustamist, ei ole selle saavutamise mehhanismid kindlaks määratud ja sobivate protokollide väljatöötamine on jätkuvalt aktiivne uurimisala. Väljapakutud protokollide hulka kuuluvad näiteks *BlueStars, BlueNet* ja *BlueMesh*.



Joonis 4. Kahest *piconet'ist* moodustunud *scatternet*. [7]

Bluetooth'i esimesel versioonil 1.0 oli probleeme nii turvalisuse kui erinevate tootjate seadmete ühilduvusega, seetõttu valmis täiustatud versioon 1.1. Enamus hetkel kasutatavaid *Bluetooth* seadmeid toetabki juba versiooni 1.1 ning ka eelnevates lõikudes toodud info käib just selle versiooni kohta. Sellel spetsifikatsioonil põhinevate seadmete laialdane edu julgustas *Bluetooth*'i huvigruppi samas suunas edasi liikuma ning valmimas on juba järgmine versioon – *Bluetooth 2.0* – mis peaks pakkuma andmeside kiirust kuni 20Mbps ja saatekaugust kuni 50 meetrit (või kuuldavasti esialgu siiski veidi vähem). Uuele spetsifikatsioonile vastavad seadmed võivad turule jõuda juba 2005. aastal.

3.2. IEEE 802.11 võrgud

IEEE *(Institute of Electrical and Electronics Engineers)* alustas traadita kohtvõrkude loomiseks sobiva 2,4 GHz sagedusalas töötava standardi 802.11 arendamist aastal 1990 ning esimene versioon võeti vastu aastal 1997. Hiljem on loodud mitmeid töögruppe (tähistega "a", "b", "c" jne.) esialgse standardi laiendamiseks ja täiustamiseks. Paralleelselt IEEE'ga, kes standardeid välja töötab, moodustasid 802.11'le vastavate seadmete tootjad organisatsiooni *Wireless Ethernet Compatibility Alliance* (WECA), mis tegeleb toodete standardile vastavuse kontrolliga ning väljastab sertifikaate. Hiljem nimetati see organisatsioon ümber *Wi-Fi Alliance*'iks, kus *Wi-Fi = Wireless Fidelity*.

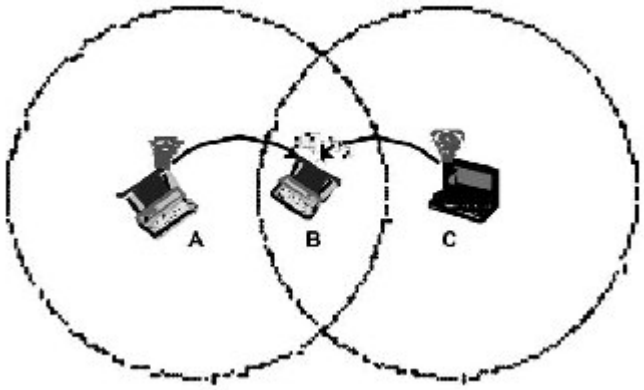
ISO *(International Standards Organization)* OSI *(Open Systems Interconnection)* mudeli füüsilisele tasemele pakub IEEE 802.11 kolme erinevat võimalust: *Direct Sequence Spread Spectrum*, *Frequency Hopping Spread Spectrum* ning infrapunaühenduse kasutamine. Tõsi küll, viimatinimetatu – infrapunasel valgusel põhinev ühendus – ei ole laiemasse kasutusse jõudnud. Lühikokkuvõte levinumate standardi 802.11 variantide füüsilise kihi parameetrite kohta on toodud järgnevas tabelis:

Physical layer	Data rate (Mbps)	Bits/ symbol	Code	Modulation	Symbol rate (Msps)
802.11	1	1	Barker Sequence	BPSK	1
802.11	2	2	Barker Sequence	QPSK	1
802.11b	5.5	4	CCK	QPSK	1.375
802.11b	11	8	CCK	QPSK	1.375

Tabel 1. 802.11 levinumate variantide füüsiliste kihtide parameetreid. [7]
BPSK = Binary Phase Shift Keying; QPSK = Quadrature Phase Shift Keying;
CCK = Complementary Code Keying.

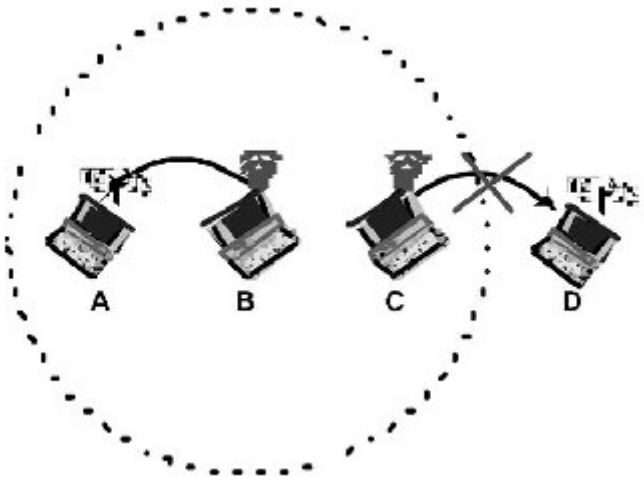
Mitmed 802.11b edasiarendused on juba valminud või lähiajal valmimas, kuid ei ole veel saavutanud ülemaailmset levikut. Näiteks 802.11a kasutab 5 GHz piirkonda, kus segajaid on vähem, ning pakub kiirust kuni 54 Mbps. Teine laiendus – 802.11g – võimaldab, vähemalt teoreetiliselt, samuti kiirust kuni 54 Mbps, kuid kasutab 2,4 GHz sagedusvahemikku ning on ühilduv ka juba olemasolevate 802.11b standardil põhinevate seadmetega, langetades selleks andmeside kiiruse sobivale tasemele.

Kuna üldjuhul on mobiilsetel traadita seadmetel ainult üks antenn, siis ei ole neil võimalik ise infot saates kanalis toimuvat kuulata ja seega tavalisi CSMA/CD *(Carrier Sense Multiple Access with Collision Detection)* põhimõtet järgivaid kandjapöördusprotokolle kasutada ei saa. Neid asendab CSMA/CA *(Carrier Sense Multiple Access with Collision Avoidance)*, mis aga ebasobiva realisatsiooni korral võib oluliselt vähendada kanali läbilaskvust, kuna ka "kokkupõrke" korral edastavad saatjad oma info lõpuni. Kanali kuulamisel *(carrier sense)* põhinevad kandjapöördusprotokollid tekitavad raadioeetrit kasutavates võrkudes teisigi tõsiseid raskusi ning seda eriti *ad hoc* võrkudes, kus keskne kontroll puudub või on minimaalne (ka IEEE 802.11 defineerib lisaks infrastruktuuri-põhisele võrgule (vt. joonis 1) võimaluse töötada *ad hoc* režiimis). Kurikuulsamad probleemid on *hidden terminal (node, station) problem* (peidetud jaama probleem) ning *exposed terminal problem*.



Joonis 5. Peidetud jaama probleem. [1]

Peidetud jaama probleem võib tekkida, kui kaks (või enam) jaama, nt. A ja C (joonis 5) on üksteise saateulatusest väljas ning seega ei suuda tuvastada, kas teine parajasti midagi saadab, kuid osaliselt nende saatepiirkonnad siiski kattuvad. Sel juhul võib tekkida kokkupõrge, kui nii A kui C hakkavad infot saatma jaamale B, kes asub mõlema saateulatuses. 802.11 standard pakub probleemi lahendamiseks mehhanismi, kus saatja kõigepealt teatab oma huvist infot edastada, saates *Request To Send* sõnumi, ning alustab info edastamist alles teate *Clear To Send* saamisel.



Joonis 6. *Exposed terminal* probleem. [1]

Joonisel 6 on toodud tüüpiline juhtum, kus võib tekkida *exposed terminal* probleem. Oletame, et jaamad A ja C kuulevad jaama B, kuid A ei kuule jaama C. Oletame veel, et B parajasti saadab jaamale A ning C soovib saata jaamale D. Põhimõtteliselt võiks C rahulikult saatmist alustada, sest jaama A jaoks see kokkupõrget ei põhjustaks – ta on C mõjupiirkonnast väljaspool. Aga kuna C kuuleb, et raadioeeter on hõivatud, siis vastavalt CSMA mehhanismile jääb ta ootama, põhjustades võrgu efektiivsuse languse.

Mõlema probleemi korral tuleb tähele panna ka seda, et tegelikult on ka sama jaama korral tegu mitme erineva piirkonnaga: saatepiirkond, milles olev (konkreetse vastuvõtutundlikkusega!) teine jaam info edukalt kätte saab; hõivatud raadioeetri tunnetamise piirkond, milles teine jaam märkab, et kanal on hõivatud; segamispiirkond, mille ulatuses käesolev jaam saatmise ajal teisi segab.

3.3. Eelnimetatute ning teiste sarnaste standardite võrdlus

Tabelis 2 on kokkuvõtlikult esitatud nii eelnimetatud kui ka mitmete teiste traadita personaal- ja kohtvõrkude standardite põhiparameetrid.

Tabel 2. •
Traadita PAN ja LAN tehnoloogiate võrdlus. [7]

	Bluetooth 2	802.15.3	DECT	802.11	802.11b	802.11a	802.11g	HiperLAN2
Frequency band	2.4 GHz	2.4 GHz	1.8–1.9 GHz	2.4 GHz	2.4 GHz	5 GHz	2.4 GHz	5 GHz
Technology	FHSS	OFDM	GFSK	DSSS	DSSS	OFDM	DSSS/OFDM	OFDM
Max range	10 cm–10 m	10 m	80 m	150 m	150 m	50 m	100 m	80 m
Power	very low	medium	medium	medium	medium	high/medium	medium/high	medium
Complexity	1 ×	1.5 ×	1.2 ×	1.2 ×	1.2 ×	4 ×	~ 3.5 ×	2.5 ×
QoS	yes	yes	yes	Inherited only in 802.11e. Backwards compatibility is questionable.				yes
Thoughput								
Physical	≤ 10 Mbps	11–55 Mbps	≤ 2 Mbps	2 Mbps	11 Mbps	54 Mbps	54 Mbps	54 Mbps
Effective	≤ 6 Mbps	≤ 30 Mbps	≤ 1 Mbps	≤ 1 Mbps	≤ 7 Mbps	≤ 31 Mbps	≤ 22 Mbps	≤ 31 Mbps
Reg. support	worldwide					US/Asia	worldwide	Europe/Japan
Promoters	2000 +	~ 50	3000 +	100 +	100 +	~ 100	~ 100	< 50

Standardi IEEE 802.15.3 põhieesmärk on *ad hoc* võrkude loomise toetamine.

DECT *(Digital Enhanced Cordless Telecommunications)* valmis juba 1990-te alguses ja on kasutusel peamiselt juhtmeta lauatelefonides.

HiperLAN/2 *(HIgh Performance Radio Local Area Network)* on ETSI *(European Telecommunication Standard Institute)* poolt arendatav kiire traadita kohtvõrgu standard.

OFDM = *Orthogonal Frequency-Division Multiplexing*.

4. Marsruutimine MANET'des

Interneti marsruutimisprotokollid on loodud võrkudele, mille topoloogia muutub väga harva ning kus marsruutimisega tegelevad spetsiaalsed võrgusõlmed, millel ressursse – energia, mälumaht, arvutusvõimsus – on küllaldaselt. Mobiilsete *ad hoc* võrkude korral aga pole need eeldused täidetud ja seetõttu on vaja uusi sobivamaid protokolle. Nende väljatöötamine ongi viimasel ajal üks aktiivsemaid uurimissuundi MANET' de valdkonnas. Käesolev peatükk annab artiklitele [1] ja [12] põhinedes ülevaate tuntumatest väljapakutud marsruutimisprotokollidest.

MANET' de jaoks loodud marsruutimisprotokollid saab jagada kolme kategooriasse: proaktiivsed / globaalsed, reaktiivsed / "vastavalt vajadusele" ja hübriidsed. Proaktiivsete protokollide korral otsitakse kohe võrgu tekkides marsruudid iga võrgusõlmeni (või võrgu osani) ning võrgu muutudes seda infot pidevalt uuendatakse. Reaktiivsed protokollid alustavad paketile tee otsimist alles siis, kui seda vaja on. Hübriidsed marsruutimisprotokollid kombineerivad pro- ja reaktiivsete protokollide meetodeid.

4.1. Proaktiivsed marsruutimisprotokollid

Proaktiivsete protokollide korral omab iga võrgusõlm informatsiooni, millist teed mööda saata paketti iga teise võrku (või võrgu teatud piirkonda) kuuluva seadmeni. Marsruutimisinfot säilitatakse tavaliselt mitmesugustes tabelites, mida perioodiliselt ja / või võrgu topoloogia muutumisel uuendatakse. Need protokollid erinevad üksteisest marsruutimisinfo uuendamise ja võrgu muutuste avastamise meetodite ning säilitatava info poolest.

Destination-Sequenced Distance Vector (DSDV) – iga võrgusõlm omab tabelit, kuhu on salvestatud iga sihtpunkti jaoks hüpete arvu järgi lühim tee selleni. Teenindusliikluse vähendamiseks kasutatakse kahte värskenduspaketti: *"full dump"*, mis sisaldab kogu teadaolevat marsruutimisinfot ja mida saadetakse üksteisele suhteliselt harva, ning *"incremental"*, mis sisaldab ainult muutusi alates eelnevast *"full dump"* paketist. DSDV tagab ka silmuste puudumise info liikumisteedes. DSDV ei sobi suurtele võrkudele, kuna sel juhul kasutaks teenindusinfo ära enamuse võrgu läbilaskevõimest.

Wireless Routing Protocol (WRP) – iga võrgusõlm omab nelja marsruutimistabelit (sihtpunktide kauguste, ühenduste "maksumuste", marsruutide, ja sõnumite korduvsaatmiste *(retransmission)* kohta), mis tähendab suuremat mäluvajadust. WRP puuduseks on ka *hello* sõnumi saatmine naabersõlmede vahel, kui hiljuti ei ole muid pakette liikunud. Lisaks võrgu läbilaskevõime vähendamisele kulutab see ka olulisel määral energiat, sest seadmed peavad pidevalt aktiivsed olema ega saa näiteks mitteaktiivsesse "magamisreziimi" lülituda. WRP tagab samuti silmuste puudumise info liikumisteedes.

Global State Routing (GSR) – iga võrgusõlm omab kogu võrgu ühenduste olekute tabelit, kuid uuendusinfot vahetavad ainult naabrid omavahel. See vähendab oluliselt teenindussõnumite arvu võrgus, kuid vahetatavad sõnumid on suhteliselt suured.

Fisheye State Routing (FSR) – võrgusõlm saadab infot ühenduste oleku kohta lähedalolevatele (hüpete arvu järgi) seadmetele sagedamini kui kaugelolevatele. Seetõttu mida kaugemal paketi adressaat asub, seda ebatäpsem on info kohalejõudmise tee kohta, kuid mida lähemale pakett sihtkohale jõuab, seda täpsemaks ka marsruutimisinfo muutub. FSR skaleerub paremini kui eelpool kirjeldatud protokollid, kuid seda täpsuse hinnaga: mida suurem on seadmete mobiilsus, seda ebatäpsemaks muutuvad teadaolevad teed kaugete

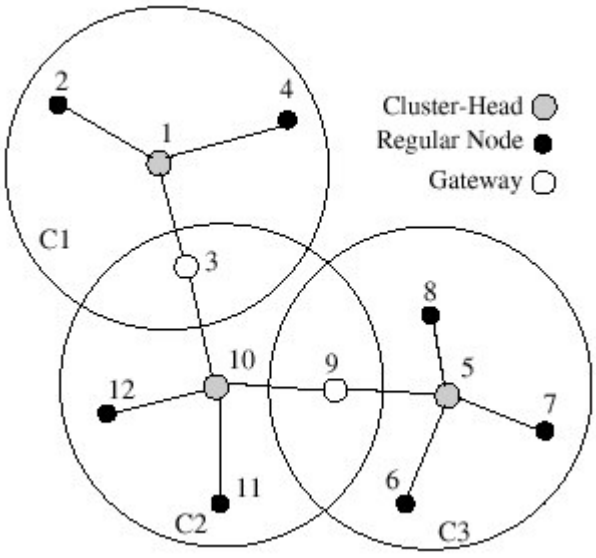
seadmeteni. Nimetatud probleemi saab leevendada, kui teha uue marsruutimisinfo saatmise sagedus lisaks kaugusele sõltuvaks ka seadmete liikuvusest.

Source-Tree Adaptive Routing (STAR) – iga võrgusõlm omab *source tree*'d, mis sisaldab eelistatud teid sellest sõlmest sihtkohtadeni. Marsruutimisinfot vahetatakse ainult naabrite vahel ning seda tehakse mitte perioodiliselt, vaid ainult teatud sündmuste korral. STAR skaleerub tänu vähesele teenindusliiklusele üsna hästi, kuid võib vajada palju mälu ning arvutusvõimsust.

Distance Routing Effect Algorithm for Mobility (DREAM) – erinevalt eeltoodud protokollidest peavad DREAM'i kasutava võrgu seadmed teadma oma geograafilisi koordinaate (nt. GPS'i kasutades). Võrgusõlmed teatavad üksteisele perioodiliselt oma asukoha ja salvestavad teiste asukohad endale tabelisse. Eeliseks on teenindusliikluse vähenemine: koordinaate kandev pakett on väike võrreldes ühenduste olekuid sisaldava paketiga. Lisaks saadetakse infot uue asukoha kohta sõltuvalt selle muutumise kiirusest, mis veelgi vähendab teenindusliiklust, tehes DREAM'i küllaltki hästi skaleeruvaks.

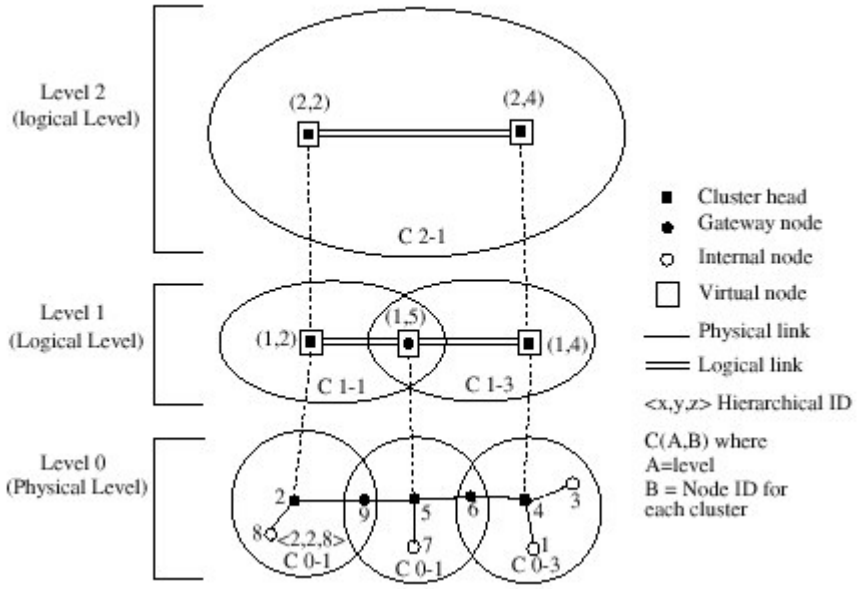
Multimedia Support in Mobile Wireless Networks (MMWN) – võrgu haldamiseks kasutatakse hierarhilist klasterdamist. Igas klastris on kahte tüüpi võrgusõlmi – kommutaatorid ja lõpp-punktid – ning lisaks üks asukohtade määramisega tegelev sõlm. Infot võrgu kohta salvestatakse dünaamilises hajutatud andmebaasis. MMWN'i on keeruline realiseerida.

Cluster-head Gateway Switch Routing (CGSR) – samuti hierarhiline protokoll, kus võrgusõlmed on grupeeritud klastriteks, aga lihtsamal viisil kui MMWN'is. Iga klastrit haldab kohapeal valitud klastripea (*cluster-head*, vt. joonis 7), mis juhib infoedastusmeediumi kasutamist ning teostab klastritevahelist suhtlemist. CGSR'i eeliseks on enamiku seadmete vajadus teada ainult info saatmise teed klastripeani, mitte kogu võrgu struktuuri. Puuduseks on klasterdatud struktuuri hoidmiseks vajaliku teenindusinfo suur hulk väga mobiilsete seadmete korral.



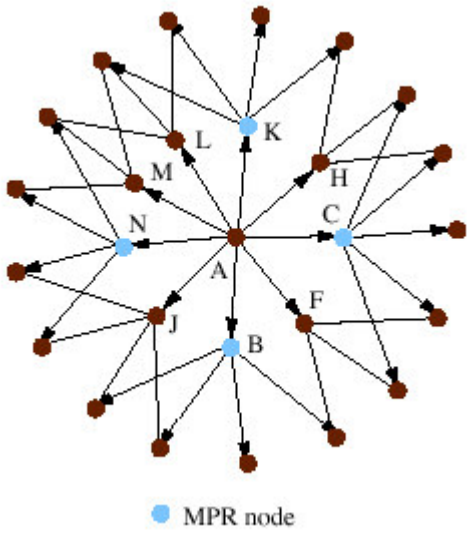
Joonis 7. Tüüpiline klastripõhine võrk. [12]

Hierarchical State Routing (HSR) – kasutatakse hierarhilist adresseerimist: igal seadmel on hierahiline identifikaator:



Joonis 8. Näide HSR topoloogiast. [12]

Optimised Link State Routing (OLSR) – iga võrgusõlm teab marsruute kõigi teiste võrgusõlmedeni, kuid tänu *multipoint relaying* (MPR) meetodile saavutatakse see väiksema teenindusliiklusega kui tavaliselt. Selleks valib iga seade oma ühe-hüppe-naabrusest sõlmed, kelle ühendused kokku katavad kõik kahe-hüppe naabrid (vt. joonis 9). Nüüd ei pea seade enam ise saatma eraldi teeninduspakette kõigile võrgusõlmedele, vaid saadab ainult MPR naabritele, kes need mitmes suunas edasi saadavad.



Joonis 9. *Multipoint relays*.
Seade A on valinud oma MPR sõlmedeks seadmed B, C, K ja N. [12]

Topology Broadcast Reverse Path Forwarding (TBRPF) – iga võrgusõlm saadab naabritele mitte kogu oma marsruuditabeli (puu), vaid ainult osa sellest, ning sõnumid sisaldavad ainult muutusi selles puu osas võrreldes eelmise saadetud marsruutimisinfoga.

Kokkuvõttena võib öelda, et enamus mittehierarhilisi globaalseid marsruutimisprotokolle ei skaleeru hästi, kuna teenindusinfo tarbib suure osa võrgu läbilaskevõimest. Hierarhilised globaalsed protokollid skaleeruvad paremini, kuna väljapoole klastrit saadavad teenindusinfot ainult klastripead. Puuduseks aga on raskused hierarhilise struktuuri säilitamisega juhul, kui võrgusõlmed on väga mobiilsed.

4.2. Reaktiivsed marsruutimisprotokollid

Reaktiivsete protokollide idee on otsida teed sihtpunkti alles siis, kui seda reaalselt vaja on, vältides sel viisil tihedat teenindusliiklust, mida proaktiivsed protokollid vajavad võrgu oleku pidevaks jälgimiseks. Marsruudi leidmine toimub enamasti võrgu "üleujutamise" *(flooding)* teel oma sihtmärgi leidmise sooviga. Kui soov jõuab mõne seadmeni, kes teab teed sihtkohta, või adressaadi endani, siis saadetakse algatajale vastav info tagasi.

Reaktiivsed protokollid saab jagada kaheks. Üks grupp protokolle, *source routed*, leiavad kõigepealt tee sihtkohani ning seejärel lisavad selle tee täpse kirjelduse igasse saadetava paketi päisesse. Seega ei pea teele jäävad paketti edastavad võrgusõlmed ise aktiivselt konkreetse marsruudi jälgimisega tegelema, vaid saadavad paketi edasi vastavalt päises olevale infole. Probleemiks on vähene skaleeruvus: suures võrgus on tee pikk, mis tähendab mahukat marsruutimisinfot iga paketi päises ja suuremat tõenäosust tee katkemiseks enne paketi kohalejõudmist. Teises, *hop-by-hop routing* protokolligrupis kannab andmepaketi päis ainult sihtkoha aadressi ning iga seade peab ise oskama seda paketti õiges suunas edasi saata. Eeliseks on parem kohanemine muutuva topoloogiaga, kuna tee leidmiseks kasutatakse alati värskeimat informatsiooni, kuid puuduseks on nõue teele jäävatele võrgusõlmedele aktiivselt jälgida võimalikke marsruute / suunda vajalikku sihtkohta.

Dynamic Source Routing (DSR) – silmusevaba protokoll, kus iga võrgusõlm jätab varem leitud marsruudid meelde ning alustab uue tee otsimist alles juhul, kui sobivat mälus ei ole. Infopaketile tuleb aga päisesse lisada täpne marsruut sihtmärgini, mistõttu DSR sobib eelkõige väiksematele võrkudele.

Ad hoc On-demand Distance Vector (AODV) – erinevalt DSR' ist teostavad AODV võrgusõlmed perioodilist ümbruse uurimist, samuti kannab paketi päis ainult sihtmärgi aadressi, mitte kogu marsruuti. Tänu sellele saab AODV paremini hakkama väga dünaamiliste võrkudega, kuigi üldiselt töötab väiksema jõudlusega kui DSR. Probleeme on skaleeruvusega.

Routing On-demand Acyclic Multi-path (ROAM) – silmusevaba protokoll, kus võrgusõlmed peavad meeles ainult neid marsruute, kus nad lähiajal aktiivselt osalenud on. Juhul, kui seadme asukoht teda läbiva marsruudi suhtes oluliselt muutub, teavitab ta sellest oma naabreid, mis võimaldab ühenduste paremat säilimist, kuid võib häirida lähiümbruses asuvaid energia säästmise eesmärgil magada soovivaid seadmeid. ROAM suudab ka vältida võrgu liigset üleujutamist teeotsimisteadetega sihtpunktini, mis on võrgust lahkunud.

Light-weight Mobile Routing (LMR) – võrgusõlm peab meeles, millisele oma naabritest paketti edasi saata, et see konkreetsesse sihtkohta jõuaks. Iga sihtkoha jaoks võidakse meeles pidada rohkem kui ühte naabrit juhuks, kui parim variant parajasti kättesaadav ei ole. LMR saab hakkama suhteliselt vähese teenindusinfo liiklusega, kuid võib sagedamini tekitada ebaõigeid marsruute ja seetõttu info saatmisele rohkem aega kulutada.

Temporally Ordered Routing Algorithm (TORA) – põhineb LMR'il, olles sellest veidi efektiivsem, kuid eeldab sünkroniseeritud kellade olemasolu võrgusõlmedes (mida mõnedes rakendustes saab realiseerida GPS'i (*Global Positioning System)* abil).

Associativity-Based Routing (ABR) – võrgusõlm määrab perioodiliselt ühenduse olemasolu enda ja oma naabrite vahel ning vastavalt akumuleerunud informatsioonile valitakse marsruutimisel suurema usaldusväärsusega ühendused. Tänu sellele jõuab info kindlamalt kohale, sest kuigi valitud tee ei pruugi olla lühim, on tema katkemine vähemtõenäoline. Negatiivseks asjaoluks on seadmete suurem energiakulu, sest perioodilise kontrolli tõttu peavad nad pidevalt aktiivsed olema.

Signal Stability based Adaptive routing (SSA) – sarnaneb ABR'ile, kuid ühenduse kvaliteeti hinnatakse mitte lihtsalt tema eelneva olemasolu sageduse järgi, vaid signaalitugevuse ning sõlmede mobiilsuse järgi (paigalseisev sõlm on marsruutimise seisukohalt kindlam kui kiiresti ringiliikuv). Üks SSA puudusi on luhtunud marsruudiotsingu taasalustamine allika juurest, mitte ebaõnnestumise piirkonnast. See võib põhjustada pikemaid viivitusi, kuna kõigepealt tuleb allikat ebaõnnestumisest teavitada.

Relative Distance Micro-discovery Ad hoc Routing (RDMAR) – kui kaks seadet on omavahel juba varem suhelnud, siis järgmine kord oletatakse, et nad vahepeal väga palju liikunud ei ole, ning piiratakse vastavalt marsruudiotsingu pakettide maksimaalset lubatud liikumiskaugust (hüpete arvu järgi). See vähendab kogu võrgu koormamist teenindus-pakettidega.

Location-Aided Routing (LAR) – eeldatakse, et iga võrgusõlm teab (GPS'i abil) oma koordinaate. Marsruudiotsingu pakettide liikumisele seatakse geograafilised piirangud, et vältida kogu võrgu koormamist. Algoritmi ühes variandis määratakse liikumiseks lubatud tsoon, teises variandis lubatakse liikuda ainult suundades, kus kaugus paketi ja sihtkoha vahel väheneb. Suure mobiilsusega võrgu puhul on aga adressaadi asukohta raske ette teada ning tuleb ikkagi kogu võrk otsingupakettidega "üle ujutada".

Ant-colony-based Routing Algorithm (ARA) – Sipelgad jätavad toiduotsingul endast maha aeglaselt lenduva feromooniraja, mida teised sipelgad tajuvad ja järgivad. Mida tihedamalt rada kasutatakse, seda tugevam jälg moodustub. ARA kasutab sarnast põhimõtet: nii teenindus- kui infopaketid suurendavad oma teele jäävates võrgusõlmedes konkreetse marsruudi "feromoonitugevust", mis muidu aeglaselt väheneb. Esmase marsruudi leidmiseks on siiski vaja levitada suurel hulgal otsingupakette, "sipelgaid", mis võib tähendada selle algoritmi piiratud skaleeruvust.

Flow Oriented Routing Protocol (FORP) – jälgib võrgusõlmede liikumist (GPS) ning selle alusel püüab juba ette ennustada, kuna marsruut katkeb, ning üritab õigel ajal ümber-suunamisi teha, vähendades katkestusi andmevoos.

Cluster-Based Routing Protocol (CBRP) – hierarhiline reaktiivne protokoll koos sellest tulenevate tüüpiliste eeliste ja puudustega: oluliselt vähem üle võrgu liikuvat teenindus-liiklust (sellega tegelevad ainult klastripead), kuid lisakulu klastrite moodustamiseks ja haldamiseks. CBRP'd kasutades võivad marsruutides tekkida ka ajutised silmused.

Üldiselt võib öelda, et halvimal juhul – kui saatja ja vastuvõtja pole varem suhelnud – on kulud marsruudi leidmiseks enamikus reaktiivsetes protokollides sarnaselt suured. Töö käigus õpivad võrgusõlmed oma ümbruse kohta järjest enam ning siis sõltub juba

protokollist ja selle sobivusest konkreetse rakendusega, kui edukalt neid teadmisi ära kasutatakse.

4.3. Hübriidsed marsruutimisprotokollid

Hübriidsed protokollid proovivad ühendada pro- ja reaktiivsete protokollide häid omadusi. Enamasti saavutatakse see kasutades võrgusõlme lähipiirkonnas proaktiivseid meetodeid ning kaugete seadmeteni otsitakse teed ainult vajaduse korral.

Zone Routing Protocol (ZRP) – igal võrgusõlmel on kindla raadiusega (hüpete arvu järgi) piirkond, nn. "tsoon", mille sees olevate sõlmedeni teab ta marsruute koheselt tänu proaktiivsetele algoritmidele, aga väljapoole tsooni jäävate sõlmedeni jõudmiseks kasutab mõnda reaktiivset protokolli.

Zone-based Hierarchical Link State (ZHLS) – piirkond on enne töö algust jaotatud mittekattuvateks geograafilisteks tsoonideks, millele on määratud identifikaatorid. Ühes tsoonis asuvad sõlmed moodustavad klastri, kuid puudub eraldi klastripea. Seega jääb ära oht liikluse "pudelikaela" tekkeks või liigseks sõltuvuseks ühestainsast sõlmest. Adressaadi leidmise palve suunatakse tsoonidele, mitte igale võrgusõlmele eraldi: tulemuseks on vähem teenindusliiklust. Seejärel, kuni adressaat püsib ühe tsooni piires, ei ole temaga kontakteerumiseks vaja uut otsingut korraldada: pakett saadetaksega konkreetse tsoonini ja seal on kohalikud asukohad pidevalt teada. ZHLS võib skaleeruda päris hästi.

Scalable Location Update Routing Protocol (SLURP) – sarnane ZHLS' ile, kuid globaalse otsingu vajadus on täielikult kaotatud. Nimelt on igale seadmele määratud kindel kodutsoon, millega ta alati seotud on. Kui seade asub parajasti kusagil mujal, siis hoiab ta sellegipoolest kodutsooni seadmeid oma asukohaga kursis, nii et need oskavad küsijatele teed juhatada. Probleeme võib tekkida väga dünaamilistes võrkudes.

Distributed Spanning Trees based routing protocol (DST) – võrk jaguneb puudeks, millest igaühte haldab puu juureks olev võrgusõlm *(root node)*. Puuduseks on suur sõltuvus üksikutest juurteks olevatest sõlmedest.

Distributed Dynamic Routing (DDR) – samuti puupõhine protokoll, kuid puu haldamine ei sõltu ühestainsast juursõlmest.

Hübriidsetel marsruutimisprotokollidel on potentsiaali suuremaks skaleeruvuseks kui puhtalt pro- või reaktiivsetel protokollidel.

4.4. Kolme kategooria võrdlus

Routing class	Proactive	Reactive	Hybrid
Routing structure	Both flat and hierarchical structures are available	Mostly flat, execpt CBRP	Mostly hierarchical
Availability of route	Always available[a]	Determined when needed	Depends on the location of the destination
Control traffic volume	Usually high, attempt at reduction is made. E.g., OLSR, TBRPF	Lower than Global routing and further improved using GPS. E.g., LAR	Mostly, lower than proactive and reactive
Periodic updates	Yes, However some may use conditional. E.g., STAR	Not required. However some nodes may require periodic beacons. E.g., ABR	Usually used inside each zone, or between gateways
Handling effects of mobility	Usually updates occur at fixed intervals. DREAM alters periodic updates based on mobility	ABR introduced LBQ. ROAM employs threshold updates. AODV uses local route discovery	Usually more than one path may be available. Single point of failures are reduced by working as a group
Storage requirements	High	Depends on the number of routes kept or required. Usually lower than proactive protocols	Usually depends on the size of each cluster or zone may become as large as proactive protocols if clusters are big
Delay level	Small routes are predetermined	Higher than proactive	For local[b] destinations small. Interzone may be as large as reactive protocols
Scalability level[c]	Usually up to 100 nodes. OLSR and TBRPF may scale higher	Source routing protocols up to few hundred nodes. Point-to-point may scale higher. Also depends on the level of traffic and the levels of multihopping	Designed for up to 1000 or more nodes

[a] If the nodes are reachable.
[b] Local destinations represents the nodes that are in the same zone or cluster as the source. For remote, they are in different clusters.
[c] The ability to perform efficient routing for up to an approximate number of nodes.

Tabel 3. Kolme marsruutimisprotokollide klassi – proaktiivsed, reaktiivsed, hübriidsed – võrdlus. [12]

5. Turvalisus *ad hoc* võrkudes

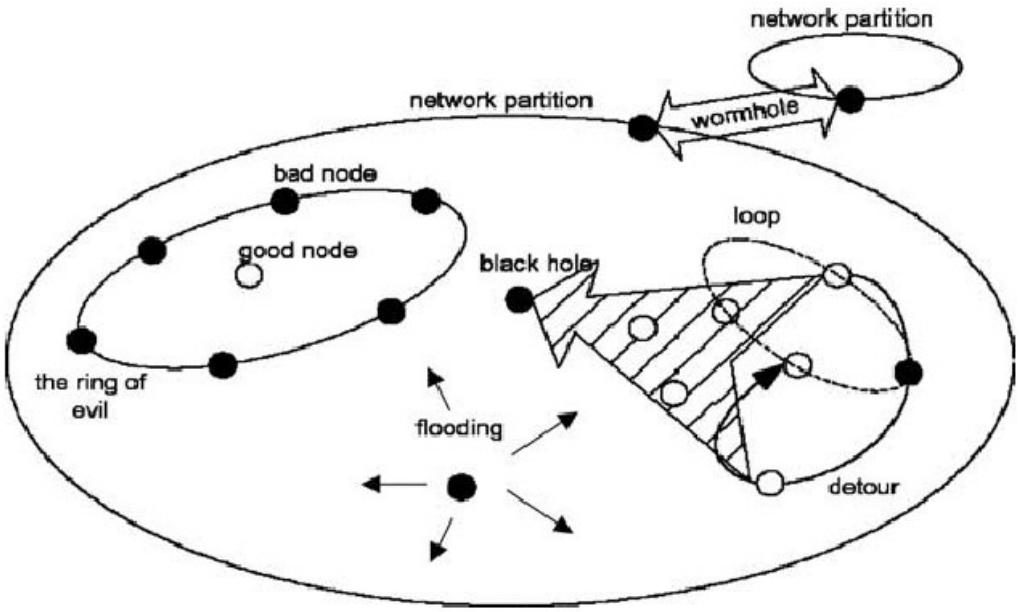
Turvalisus fikseeritud, läbi juhtmete suhtlevates võrkudes nagu tavalised kohtvõrgud ja enamus Internetist on pidevalt aktuaalne teema hoolimata mahukatest uuringutest ning vahenditest turvalisuse tõstmiseks. Raadioeetri kasutamine juhtmete asemel suurendab turvariske märgatavalt, kuna infosignaal levib oluliselt suuremas ruumipiirkonnas, mille kaitsmine on sõltuvalt olukorrast kas väga raske või üldse võimatu. Võrkude *ad hoc* olemus ja mobiilsus lisavad veelgi probleeme võrreldes paigalseisvatest seadmetest koosnevate fikseeritud topoloogiaga võrkudega. Käesolev peatükk annab artiklitele [1], [13] ja [14] põhinedes lühiülevaate olulisematest turvaprobleemidest MANET' des ning mõningatest võimalikest suundadest lahenduste otsimisel.

5.1. Turvaprobleemid

Traadita *ad hoc* võrke saab rünnata erinevatel tasemetel ja viisidel ning eesmärgiks võib olla võrgu töö häirimine, võrgus liikuva info pealtkuulamine ja / või info ebaõigeks muutmine. Rünnak võib olla passiivne pealtkuulamine, mille avastamine traadita võrgus on äärmiselt keeruline, või aktiivne tegevus, mille näiteid on toodud järgnevas loetelus.

Ründed füüsilisel tasemel: raadioeetri täitmine müraga; pidev pakettide kokkupõrgete tekitamine; seadmete lõhkumine või nende füüsiline omastamine, turvainfo väljalugemine ja (salaja) modifitseerimine – näiteks kui tegu on järelevalveta piirkonda puistatud sensorite võrguga.

Ründed marsruutimistasemel. Kui pahatahtlik seade on suutnud märkamatult võrguga liituda, saab ta marsruutimispakettidega "mängides" oluliselt häirida võrgu tööd. Sissetungija võib temani jõudnud marsruutimispaketi lihtsalt ära kustutada, modifitseeritult edasi saata või valevastuse tagasi saata. Lisaks võib ta ise uusi valeandmetega teeninduspakette tekitada. Mida sissetungija üksikute pakettidega teeb, sõltub tema üldisemast eesmärgist, milleks võib olla näiteks:



Joonis 10. Näiteid marsruutimistaseme rünnakutest. [14]

- Musta augu tekitamine – kogu lähiümbruse liikluse suunamine endasse ning kõigi (info)pakettide kustutamine.
- Võrgu üleujutamine marsruutimispakettidega võrguliikluse häirimiseks või seadmete energiavarude ammendamiseks.
- Silmuste *(loops)* tekitamine, nii et paketid liiguvad ringiratast samas piirkonnas.
- Liikluse ümbersuunamine ebaefektiivsele teele, ummikute tekitamine.
- *Wormhole* – kanal kahe sissetungija vahel, läbi mille liikuvad paketid jõuavad kusagile ootamatusse kohta, kas sama võrgu mõnda kaugesse piirkonda või hoopis teise võrku.
- Võrgu teatud piirkonna või üksiku sõlme isoleerimine teistest, moodustades selle ümber ringi pahatahtlikest seadmetest.

Ründed kõrgematel tasemetel: võrgus liikuva kasuliku (s.t. mitte teenindus-) info modifitseerimine, valeinfo tekitamine.

Eelpoolnimetatutele analoogseid probleeme võib tekkida ka ilma pahatahtlike isikute / seadmeteta: raskusi võivad tekitada osaliselt riknenud "heatahtlikud" võrgusõlmed. Tõsi küll, sel juhul räägitakse tavaliselt võrgu usaldusväärsusest, mitte turvalisusest, kuid need kaks on omavahel üsna tihedalt seotud.

5.2. Võimalikke lahendusi

Üldjoontes võib turvamehhanismid jagada kaheks: preventiivsed ja probleeme avastavad.

Preventiivsus põhineb enamasti krüpteerimisel ja seetõttu on oluliseks küsimuseks dekodeerimisvõtmete jaotamine: millal ja kuidas. Traditsioonilistes Internetile mõeldud lahendustes lähtutakse tihti kesksest turvalisest serverist ja teadaolevast võrgu infrastruktuurist, kuid MANET' des sellised võimalused puuduvad ning seetõttu tuleb kasutada näiteks hajutatud võtmehaldussüsteemi, kus kõik "heatahtlikud" seadmed vastutavad turvalisuse eest ühiselt.

Probleeme avastavad turvamehhanismid püüavad näiteks aru saada, kui toimub marsruutide kahtlane ümbersuunamine või võrgu üleujutamine ebaoluliste pakettidega, ning vastavalt avastatud probleemile see kõrvaldada, isoleerida vms.

6. Raadioside efektiivsem kasutamine

Kuigi infovahetus *ad hoc* võrkudes võib toimuda mistahes signaalikandja – näiteks valguse või heli – abil, on levinuimaks siiski raadioside kasutamine. Sellega seonduvad aga kaks olulist probleemi. Esiteks on raadiosaatja kasutamine üsna energiamahukas tegevus ning MANET' des on energia väga piiratud ressurss (eriti näiteks sensorvõrkudes, mis koosnevad väga väikestest seadmetest, kuid peavad töötama ilma inimese sekkumiseta isegi aastaid). Teiseks on raadiospekter väga paljude kasutajate vahel rangelt ära jagatud ning vabakasutuseks on jäänud vaid üksikud kitsad lõigud. Käesolev peatükk annab lühiülevaate neist probleemidest ning võimalikest lahendustest. Lisaks allpool eraldi väljatoodud allikatele on jaotuse 6.1 koostamisel kasutatud artiklit [1].

6.1. Energia säästmine raadioseadmes

Mobiilsetes võrkudes kulub seadmete omavahelisele suhtlemisele märkimisväärne osa energiast. Sülearvutite korral võib see olla kusagil 10% ringis kogu energiatarbest, pihuseadmetes kuni 50% ja *ad hoc* võrguna keskkonda paisatud sensorites lausa põhiosa kogu tarbimisest. Seetõttu ongi võrgusõlme eluea pikendamiseks tehtaval energia kasutamise optimeerimisel oluline pöörata põhitähelepanu justnimelt raadioseadme ja selle kaudu toimuva suhtlemise efektiivsemaks muutmisele. Selleks kasutatavad strateegiad saab jagada kahte klassi: lokaalsed ja globaalsed.

Lokaalsed säästustrateegiad toimivad ühe võrgusõlme piires ja peamine viis kokkuhoiuks on raadioaparatuuri haldmine magamisrežiimis võimalikult suure osa ajast. Probleem on nimelt selles, et ka lihtsalt raadioeetrit kuulav seade, mis parajasti ei teosta pakettide vastuvõttu ega saatmist, kasutab üsna palju elektrit. Tarbitava energia suheteks olekutes tegevuseta : vastuvõtt : saatmine on enamkasutatavatel raadioseadmetel mõõdetud näiteks 1 : 1,05 : 1,4 ; 1 : 1,2 : 1,7 ja 1 : 2 : 2,5 [15], magamisolekus aga on kulu suurusjärgu võrra väiksem. Raadio võib magama panna näiteks ajaks, kui keegi läheduses juba saatmisega tegeleb: sellel ajal peavad teised võrgusõlmed niikuinii vaiksed olema. Samuti võib paremaid aegu ootama jääda juhul, kui kanalis on parajasti suur müra või tihe liiklus (mille korral on suur kokkupõrgete tekke tõenäosus).

Raadioaparatuur ei ole jagamatu tervik, vaid koosneb moodulitest: analoogvastuvõtt, analoog-digitaalmuundur, dekodeerimine, jne. Põhimõtteliselt on võimalik ka neid eraldi magama panna, nii et iga moodul käivitub vaid siis, kui tema sisendile uus info saabub [16].

Lisakokkuhoidu võib anda muudetava saatekauguse kasutamine: kiirata ainult nii tugevalt, et lähim naaber info kätte saab ja selle ise edasi saadab. Kuna raadiosignaal nõrgeneb saatjast eemaldudes rohkem kui lineaarselt, võib sel viisil saavutada ka globaalset kokkuhoidu – kuigi paketi edasisaatmisega peab tegelema rohkem võrgusõlmi, on kulu nendele lühikestele "hüpetele" kokkuvõttes väiksem [15]. Lisaks võib väheneda ka pakettide kokkupõrgete arv ja kasvada võrgu läbilaskvus, kuna ühe saatja "segamispiirkond" on väiksem. Kas eelistada väiksemat arvu kaug- või suuremat arvu lähiülekandeid, sõltub siiski konkreetsest olukorrast.

Globaalsete säästustrateegiate eesmärgiks on maksimiseerida võrgu kui terviku eluiga, säilitades seejuures võrgu töövõime. Kui iga seade ärkaks ainult selleks ajaks, kui tal endal midagi saata vaja on, siis ei oleks enamasti piisavalt teisi ärkvelolevaid võrgusõlmi, kelle kaudu infot edasi saata. Seetõttu on mõttekas organiseerida magamisgraafikud näiteks

selliselt, et kogu piirkond oleks pidevalt vähese arvu aktiivsete seadmete poolt leviga kaetud ja aeg-ajalt toimuvad vahetused: infoedastajate rolli võtavad üle järgmised seadmed. Teine variant on kõigi seadmete üheaegne magamine ja eelnevalt määratud ajavahemike järel korraga aktiivseks muutumine.

Veel ideid energiakulu vähendamiseks [16]:

- Jätta ära raadioühenduse loomise kahepoolne protsess ning lihtsalt proovida oma infot naabritele edastada. Sobiva ajastuse, saatesageduse, faasi ja teiste parameetrite arvutamiseks ära kasutada kogu kättesaadav info (näiteks seadme(te) asukoht, kiirus ja kiirendus, nendest tulenevad signaalide saabumisajad, Doppleri efekt jms.) – arvutusintensiivne marsruutimine vastandina liiklusintensiivsele marsruutimisele.
- Ligipääs raadiokanalile reguleerida sünkroniseerimise abil, mitte MAC *(Media Access Control)* sõnumitega.
- Jätta ära loogilise ühenduse loomine adressaadiga, vaid lihtsalt sõnum teele saata.
- Viia miinimumini pakettides sisalduv teenindusinfo.
- Integreerida protokollikihid, nii et ka kõrgemad tasemed on teadlikud füüsilise kihi (energia)probleemidest ning osalevad aktiivselt nende lahendamisel.
- Saadetav info kokku koguda ning ühekorraga kiiresti ära saata.

Nende ideede kasutatavus sõltub konkreetsest rakendusest.

6.2. Raadiospektri efektiivsem kasutamine

Raadiospekter on jagatud kitsasteks sagedusvahemikeks ja huvigrupid-organisatsioonid võivad kasutada ainult neile litsentseeritud sageduspiirkondi. Järgmisel lehel on näitena toodud USA raadiospektri jaotus (A4 formaadis ei ole väljatrükk küll eriti hästi loetav, aga huvi korral saab seda tabelit *National Telecommunications and Information Administration*' i kodulehelt PDF formaadis alla laadida [17]). Raadio teel suhtlevate seadmete arv aga üha kasvab ja seda eriti just mõnedes sageduspiirkondades, näiteks suhteliselt kitsastes vabakasutuses olevates (s.t. litsentsi mittenõudvates) vahemikes. Probleemiks on ka spektrijaotuse erinevused riigiti, mis raskendab mobiilsete seadmete globaalset kasutamist. Õnneks on aktiivselt asutud lahendusi otsima ning kahte võimalust – ultralairibatehnoloogia ja *Cognitive Radio* – ongi järgnevas lühidalt tutvustatud.

Ultralairiba *(Ultra Wideband, UWB)* on tegelikult tuntud juba 1960-test aastates alates, kuigi siis kasutati teistsugust terminoloogiat: *"carrier-free"*, *"baseband"* või *"impulse"* tehnoloogia [18]. UWB põhimõte on ülilühikeste raadioimpulsside kasutamine, mille kestus on tüüpiliselt mõõdetav piko- või nanosekunditega ja impulsi "pikkus" on üks kuni paar kandevsageduse lainepikkust. Tekkiv signaal on nii suure ribalaiusega, et tihti on tegelikku kandevsagedust raske määratleda. Kuna energia ja info on väga suurde sagedus-piirkonda laiali jaotatud, siis on energiatihedused (vattides ühe sagedusriba hertsi kohta) väga väikesed ning seetõttu UWB kitsaribalisi tugevaid signaale eriti ei häiri. Samuti ei sega need kitsaribalised signaalid eriti UWB signaali, sest viimases on info niivõrd "laiali määritud", et peaaegu alati leidub piisavalt laiu sagedusvahemikke, kus signaal segamatult adressaadini jõuab.

Selle lehe asemele tuleb eraldi värviprinteriga trükitud raadiosageduste jaotustabel http://www.ntia.doc.gov/osmhome/allochrt.pdf. Tühi leht lihtsalt selleks, et leheküljenumbrid pärast õigesti läheks.

Tänu UWB tehnoloogiale on FCC (*Federal Communications Commission*, USA) paaril viimasel aastal hakanud mõningaid konkreetsetele kasutajatele litsentseeritud sagedusalasid avama ka litsentseerimata isikutele. Seda mõistagi tingimusel, et kasutatavad UWB signaalid oleks nii väikse võimsustihedusega, et sageduste põhikasutajaid ei häiriks.

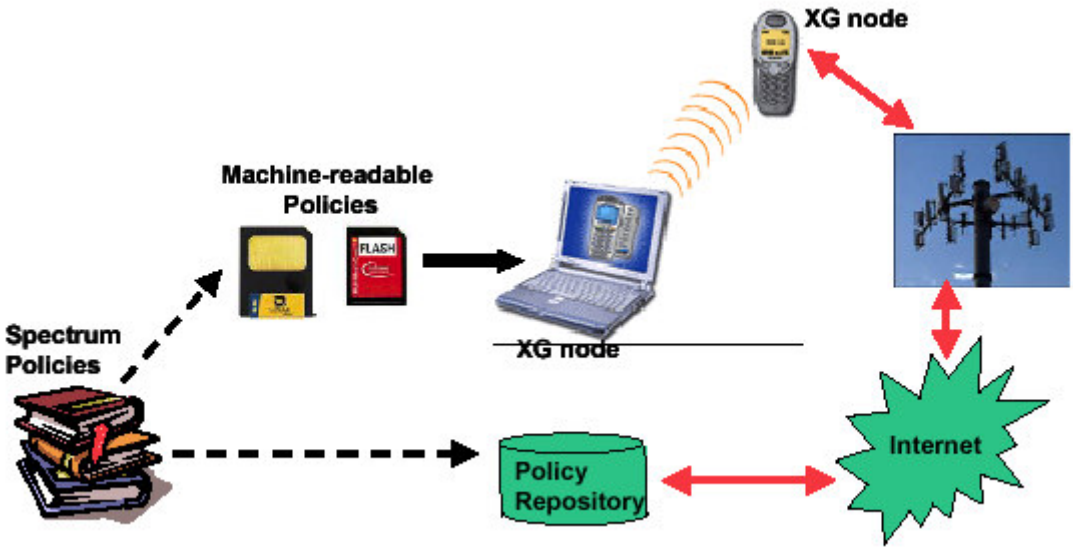
Cognitive Radio (CR) on raadioseade, mis suudab jälgida ("*cognitive*" on otsetõlkes "tunnetuslik") ümbritsevat keskkonda, eelkõige raadiospektri kasutust teiste poolt, ja oma asukohta ning vastavalt olukorrale muuta oma võimsust, sagedust, modulatsiooni ning teisi parameetreid [19]. Nimelt on raadiospekter kui ressursiruum mitmemõõtmeline [20]:

- Signaali kandesagedus.
- Aeg, mille jooksul signaali edastatakse.
- Ruumiosa, kus signaal on vastuvõetav või häiringuid põhjustab.
- Signaali formaat – mil viisil on info raadiosignaali kodeeritud.

Seniajani on ainus vaadeldav parameeter olnud sagedus, mille lubatud vahemikud on igale kasutajale rangelt kindlaks määratud (üksikutes rakendustes, näiteks traadita kohtvõrkudes, on küll kasutatud sageduste valikut vastavalt olukorrale, kuid see on siiski toimunud väga kitsastes piirides) ja üldiselt on jäänud mulje, et spektriressurss võib vaikselt ammenduma hakata. Kui aga vaadelda ka ülejäänud parameetreid, on kasutamata ressursiruumi tohutult. Näiteks on vahemikust 0 kuni 100 GHz igal ajahetkel kasutuses vaid 5..10 protsenti ja seega on põhimõtteliselt 90 GHz ulatuses vaba raadiospektrit [19]. *Cognitive Radio* peab suutma ära kasutada neid hetki, kus sagedusvahemiku litsentsi omanik parajasti saatmisega ei tegele, ning põhiomaniku tagasi eetrisse tulekul koheselt "eest ära hüppama".

Mõistagi on vaja mõned sagedused ka eranditult põhikasutaja valdusse jätta, näiteks päästeteenistuste omad. Samuti võib olla vajalik piirangute veel täpsem seadmine, keelates CR' del mõne sagedusala kasutamise mingis geograafilises piirkonnas ja teatud kellaaegadel. Kõigi piirangute jäik seadmesse sissekirjutamine raadio valmistamise ajal oleks keeruline – algul peaks riistvara tootmine ootama regulatsioonide valmimise taga ning hiljem, kui piirangud ja seadmed valmis, oleks keeruline või võimatu vajadusel piiranguid muuta. Seetõttu peaks nii tehnoloogia kui sageduste kasutuslubade jagajad lähtuma dünaamilisest piirangute seadmisest – infot keelatud tegevuste kohta hoitakse vastavas serveris ning igaüks võib sealt alla laadida temale vajaliku osa piirangutest, näiteks konkreetse geograafilise piirkonna kohta (joonis 11).

Cognitive Radio ei ole ainult üksikute uurimisasutuste huviala, vaid selle ideega on kaasa läinud ka organisatsioonid, kelle toetus CR' i reaalseks rakendamiseks on väga oluline: FCC ning IEEE. Näiteks on algatatud standardi IEEE P802.22 loomine, mille täispikk ametlik nimi on *"Standard for Wireless Regional Area Networks (WRAN) – Specific requirements – Part 22: Cognitive Wireless RAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Policies and procedures for operation in the TV Bands."* ja mille eesmärgiks on välja töötada spetsifikatsioon televisiooni VHF/UHF sagedusalade (54..862 MHz) kasutamiseks CR toetusega traadita piirkondlike võrkude poolt [21].



Joonis 11. Dünaamiline piirangute seadmine. XG on DARPA projekt uue põlvkonna *(neXt Generation)* spektrikasutustehnoloogiate väljatöötamiseks. [22]

7. MANET rakendused

Mobiilsete *ad hoc* võrkude kasutusvõimalusi on väga palju ning sellest tulenebki kiirelt kasvav huvi nende arendamise vastu. Selle huvi põhjuste paremaks mõistmiseks on käesolevas peatükis toodud mitmesuguseid näiteid MANET' de võimalikest kasutusvaldkondadest. Loetelu koostamisel on kasutatud allikaid [1], [3], [23] ja [24].

Päästeteenistused: kommunikatsioon päästeoperatsioonidel; loodusõnnetustes hävinud sideinfrastruktuuri ajutine asendamine; liiklusõnnetuse korral juhiste edastamine lähiümbruse sõidukijuhtidele (eeldusel, et enamikus liiklusvahendites on võrguseadmed); päästja ja muude oluliste objektide asukoha näitamine kaardil või majaplaanil (näiteks tuletõrjujale tema kiivris oleva HUD' (*Head Up Display)* abil).

Kommertskasutus: mitmesugused e-äri rakendused, näiteks elektrooniliste maksete sooritamine taksodest jms.; mobiilne kontor; koosolekutel, seminaridel, konverentsidel osalejate mobiilsetest seadmetest loodavad / tekkivad koostööd ja suhtlemist soodustavad võrgud; mobiilsest seadmest printimine suvalises punktis firma territooriumil; esitlustehnika seadistamine otse oma mobiilsest seadmest, mitte spetsiaalsete pultide abil; personaalvõrk kantavatest ja paari meetri raadiuses olevatest seadmetest; asukohast sõltuvate uudiste, teeolude, ilmateate, muusika, reklaamide edastamine sõidukitele; asukohast sõltuv otsing – kus on lähim vaatamisväärsus, printer, pangaautomaat, bensiinijaam, kino; transpordivahendite omavaheline suhtlemine, logistika.

Haridus ja meelelahutus: loengu kuulajate sülearvutite ühendamine koostööd ja arutelu soodustavasse võrku; virtuaalsed klassiruumid; võrgumängud *(multi-user games).*

Kodukasutus: traadita koduvõrk; Interneti leviala laiendamine majas, õues, naabruskonnas; võrku ühendatud kodurobotid.

Taktikalised võrgud: militaarkommunikatsioon; lahinguvälja automatiseerimine.

Oluline MANET' de liik on sensorvõrgud – suur hulk vaadeldavasse keskkonda paisatud või installeeritud traadita side abil suhtlevaid sensoreid – mis on rakendatavad kõigis eeltoodud valdkondades. Lahinguvälja jälgimine, (piiri-, liikumiskeelu-) lepingutest kinnipidamise kontroll; virtuaalne klaviatuur (kiirendusanduritega sensorid sõrmeküüntel); kaupade liikumise jälgimine; seadmete monitooring ja rikete ennetamine tehastes, näiteks vibratsiooniandurite abil; inimeste jälgimine: info lapse, vanainimese, patsiendi liikumisest, tervislikust seisundist; epideemiate varajane avastamine, kasvõi aevastuste sageduse järgi rahvarikastes kohtades; teadusele vajalike andmete kogumine looduse kohta; parkla oleku jälgimine – millised kohad parajasti vabad on; põllumajanduslikud rakendused: kariloomade ja põldude oluliste parameetrite pidev jälgmine.

Sensorvõrkude loogiline edasiarendus on sensor- ja täiturvõrgud (*Wireless Sensor and Actor Networks*, WSANs), kus sensorid ja täiturid moodustavad üheskoos funktsioneeriva MANET [25]. Näiteks kui tulekahjuandurid avastavad tulekolde, siis saadavad selle info võrku laiali. Teade jõuab ka samas võrgus asuvate kustutusseadmeteni, kes vastavalt tulekahju asukohale ja suurusele lepivad omavahel kokku sobiva kustutamisstrateegia.

8. Kokkuvõte

Mobiilsed *ad hoc* võrgud omavad suurt potentsiaali – nende kasutuselevõtt edendaks väga paljusid erinevaid eluvaldkondi. Esimesed projektid said küll alguse juba 1970-tel aastatel, kuid alles praeguseks on tehnoloogia areng jõudnud piisavalt kaugele, et tekitada laiemas üldsuses piisavalt huvi MANET' de kasutamise vastu. Kuigi mitmed olulised küsimused nagu marsruutimine ja energia säästmine mobiilsetes *ad hoc* võrkudes vajavad veel põhjalikku uurimis- ja arendustööd, on esimesed tooted juba turule jõudnud ning lähiajal võib oodata MANET' de laialdast kasutuselevõttu.

9. Kasutatud materjalid

Internetis asuvaid materjale on kasutatud sellistena, nagu nad olid ajavahemikus november kuni detsember aastal 2004.

Mitmed viited on aadressile http://www.sciencedirect.com, mis tähendab, et on kasutatud kirjastuse Elsevier teadusajakirjade täistekste sisaldavat *online*-andmebaasi ScienceDirect, millele on ligipääs TTÜ arvutivõrgust. Märge "Corrected proof" tähendab järgnevat:

> **Corrected proofs:** these are articles containing the authors' corrections. The content of the article will usually remain unchanged, and possible further corrections are fairly minor. Typically the only difference with the finally published article is that specific issue and page numbers have not yet been assigned. [ScienceDirect]

1. Mobile ad hoc networking: imperatives and challenges.
Imrich Chlamtac, Marco Conti, Jennifer J.-N. Liu.
Ad Hoc Networks. Volume 1, Issue 1, July 2003, Pages 13-64.
http://www.sciencedirect.com/

2. Ad hoc networking for pervasive systems. Editorial. Marco Conti, Enrico Gregori.
Ad Hoc Networks. Article in Press, Corrected Proof.
http://www.sciencedirect.com/

3. Mobile ad hoc networking: an essential technology for pervasive computing.
Jun-Zhao Sun.
Proc. International Conferences on Info-tech & Info-net, Beijing, China, C:316 - 321.
http://www.mediateam.oulu.fi/publications/pdf/92.pdf

4. picoNet II Mobile Router. Alex Song.
Undergraduate Honours Thesis Project.
http://piconet.sourceforge.net/thesis/main.html

5. Quality of service provisioning in ad hoc wireless networks: a survey of issues and solutions. T. Bheemarjuna Reddy, I. Karthigeyan, B.S. Manoj, C. Siva Ram Murthy.
Ad Hoc Networks. Article in Press, Corrected Proof.
http://www.sciencedirect.com/

6. An outsider's view of MANET. F. Baker.
Network Working Group, Internet-Draft. March 17, 2002.
http://w3.antd.nist.gov/wctg/manet/draft-baker-manet-review-01.txt

7. Evolution of the Wireless PAN and LAN standards. Th. Zahariadis.
Computer Standards & Interfaces. Volume 26, Issue 3, May 2004, Pages 175-185.
http://www.sciencedirect.com/

8. Spread Spectrum Diagram: Typical Frequency Hopping Pattern.
http://www.data-linc.com/articles/spsptech.htm

9. Direct Sequence vs. Frequency Hopping.
http://www.wavewireless.com/classroom/whitepapers/FHSSvDSSS.pdf

10. Direct-sequence spread spectrum.
Wikipedia.
http://en.wikipedia.org/wiki/DSSS

11. Frequency-hopping spread spectrum.
Wikipedia.
http://en.wikipedia.org/wiki/Frequency-hopping_spread_spectrum

12. A review of routing protocols for mobile ad hoc networks.
Mehran Abolhasan, Tadeusz Wysocki, Eryk Dutkiewicz.
Ad Hoc Networks. Volume 2, Issue 1, January 2004, Pages 1-22.
http://www.sciencedirect.com/

13. How to misuse AODV: a case study of insider attacks against mobile ad-hoc routing protocols. Peng Ning, Kun Sun.
Ad Hoc Networks, Article in Press, Corrected Proof.
http://www.sciencedirect.com/

14. Security considerations in ad hoc sensor networks. Fei Hu, Neeraj K. Sharma.
Ad Hoc Networks. Volume 3, Issue 1, January 2005, Pages 69-89.
http://www.sciencedirect.com/

15. Radio range adjustment for energy efficient wireless sensor networks.
Q. Gao, K.J. Blow, D.J. Holding, I.W. Marshall, X.H. Peng.
Ad Hoc Networks. Article In Press, Corrected Proof.
http://www.sciencedirect.com/

16. Advanced Technology Office Connectionless Networking Program Industry Day Briefing, 4 March 2003. Preston Marshall.
http://www.darpa.mil/ato/solicit/CN/cn_brief.pdf

17. United States Frequency Allocations, The Radio Spectrum (October 2003)**.**
http://www.ntia.doc.gov/osmhome/allochrt.pdf

18. Ultra Wideband (UWB) Frequently Asked Questions (FAQ).
http://www.multispectral.com/UWBFAQ.html

19. Sharing spectrum the smarter way. Patrick Mannion.
CommsDesign, Apr 05, 2004.
http://www.commsdesign.com/showArticle.jhtml?articleID=18700443

20. Wireless Networking Systems Research. Joseph B. Evans.
NSF Workshop on Wireless Communications, Honolulu, Hawaii, 15 October 2003.
http://www.ittc.ku.edu/~evans/programmablewireless/wireless_nets_research.pdf

21. IEEE Starts Standard To Tap Open Regions In The TV Spectrum For Wireless Broadband Services.
IEEE Press Release, 12 Oct. 2004.
http://standards.ieee.org/announcements/pr_80222.html

22. The XG Vision, Request For Comments, Version 2.0.
http://www.darpa.mil/ato/programs/XG/rfc_vision.pdf

23. Improving Life and Industry with Wireless Sensors.
http://www.intel.com/research/exploratory/wireless_sensors.htm

24. Smart Dust. Autonomous sensing and communication in a cubic millimeter.
http://robotics.eecs.berkeley.edu/~pister/SmartDust/

25. Wireless sensor and actor networks: research challenges.
Ian F. Akyildiz, Ismail H. Kasimoglu.
Ad Hoc Networks. Volume 2, Issue 4, October 2004, Pages 351-367.
http://www.sciencedirect.com/