WiMAX

- teknologi, funksjonelle egenskaper og sikkerhet

Bodil Hvesser Farsund

Forsvarets forskningsinstitutt (FFI)

23. juni 2010

FFI-rapport 2010/01347

1126

P: ISBN 978-82-464-1798-1
E: ISBN 978-82-464-1799-8

Emneord

Trådløs bredbåndsaksess

OFDM

Sikkerhet

Lokasjonsbaserte tjenester

Utbygging

Godkjent av

Kjell Olav Nystuen	Prosjektleder
Vidar Stensrud Andersen	Avdelingssjef

Sammendrag

I dag er det en rivende utvikling innen infrastrukturer for elektronisk kommunikasjon. Trenden er at sivile og militære kommunikasjonsinfrastrukturer smelter sammen, både i forhold til teknologibruk og anvendelse. Sivile kommunikasjonsteknologier vil dermed få større betydning for Forsvaret i tiden fremover. På bakgrunn av dette vil det ved Forsvarets forskningsinstitutt gjøres studier av noen utvalgte relevante sivile systemer og teknologier for elektronisk kommunikasjon. I denne rapporten beskrives WiMAX. WiMAX står for *Worldwide Interoperability for Microwave Access.*

WiMAX er en trådløs aksessteknologi for bredbåndstilknytning. I dag er det to versjoner av denne teknologien som blir bygd ut. De blir vanligvis omtalt som stasjonær og mobil WiMAX. De bygger på henholdsvis IEEE 802.16-2004- og IEEE 802.16e-2005-standardene.

Den kanskje viktigste egenskapene til WiMAX-teknologien er høy spektrumsutnyttelse i mange ulike miljøer. Rapporten beskrivelser fysisk lag, og spesielt *orthogonal frequency division multiplexing* og *multiple input multiple output* antenneteknikker. Disse teknikkene bidrar spesielt til høy spektrumsutnyttelse. Andre tema som rapporten omhandler er *media access control*-laget og WiMAX Forum sin referansemodell for nettverksarkitektur. Sikkerhet og sårbarhet, og lokasjonsbaserte tjenester er av spesiell interesse, og er derfor beskrevet mer detaljert. Avslutningsvis følger status på utbygging.

English summary

Today the infrastructures for electronic communication is developing tremendously. The tendency is that commercial and military infrastructures for electronic communication are converging, in case of both technology utilization and applications. Commercial communications technology will have a greater impact on the Norwegian Defence in times to come. With this background the Norwegian Defence Research Establishment will study some selected relevant commercial systems and technologies for electronic communication. In this report WiMAX is being described. WiMAX stands for Worldwide Interoperability for Microwave Access.

WiMAX is a technology for broadband wireless access. There are two versions of the technology that is being deployed today. They are commonly called fixed and mobile WiMAX, and refer to the IEEE 802.16-2004 and IEEE 802.16e-2005 standards respectively.

The most important property of the WiMAX-technologies is high spectrum utilization in very different environments. This report describes the physical layer, and particularly orthogonal frequency division multiplexing and multiple input multiple output antenna techniques. They are of special importance. Other topics in the report are the media access control layer and the network reference model developed by WiMAX Forum. Security and vulnerability, and location based services are of special relevance, and are therefore being described in more detail. At the end the status of deployment is reported.

Innhold

1 Innledning

Utviklingen innen infrastrukturer for elektronisk kommunikasjon (EKOM) gjennomgår i dag en rivende utvikling. Det er en klar trend at militære og sivile EKOM-infrastrukturer smelter sammen, både i forhold til teknologibruk og anvendelse. Sivile EKOM-teknologier vil dermed i stadig større grad ha betydning for Forsvaret. I den forbindelse vil det som ledd i arbeidet med prosjekt 1126 UNET på FFI gjøres sammenfattende beskrivelser av noen utvalgte relevante sivile EKOM-systemer og -teknologier. I denne rapporten beskrives WiMAX, mens den nært beslektede teknologien *Long Term Evolution* (LTE) vil bli beskrevet i en annen rapport.

1.1 Målsetning med rapporten og avgrensning

Denne rapporten beskriver WiMAX (*Worldwide Interoperability for Microwave Access*) som baserer seg på IEEE 802.16-standardene og er en teknologi for trådløs bredbåndsaksess. IEEE 802.16-standarden inneholder flere utgaver og mange valgmuligheter, men i denne rapporten har fokuset vært de delene av IEEE-standarden som WiMAX Forum [1] har valgt for sin standardisering av WiMAX, se delkapittel 2.3. Denne rapporten tar for seg standardene IEEE 802.16-2004 (også kalt IEE 802.16d) [2] og IEEE 802.16e-2005[3], kjent som henholdsvis *stasjonær WiMAX* og *mobil WiMAX*. Mobil WiMAX er den teknologien som i størst grad blir bygd ut i dag, følgelig er det flere detaljer om denne i rapporten.

I rapporten er det først og fremst lagt vekt på radioforbindelsen mellom basestasjon (BS) og abonnentterminal/*subscriber station* (SS) og de lavere protokollagene. Det er også disse lagene som blir spesifisert i IEEE-standarden. I tillegg er temaet sikkerhet og lokasjonsbaserte tjenester viet en del oppmerksomhet.

1.2 Rapportens oppbygging

I neste kapittel blir WiMAX-teknologien introdusert, samt at de ulike WiMAX-versjonene blir beskrevet i forhold til IEEE 802.16-standarden. I Kapittel 3 blir de sentrale elementene på fysisk lag beskrevet, som for eksempel *orthogonal frequency division multiplexing* (OFDM) og *multiple input multiple output* (MIMO), mens *media access control* (MAC)-laget blir beskrevet i kapittel 4. WiMAX-arkitekturen blir gjennomgått i kapittel 5, og sikkerhetsfunksjonaliteten i WiMAX blir beskrevet i kapittel 6, samt hvilke sårbarheter denne teknologien innehar. Videre gis det en oversikt over WiMAX og lokasjonsbaserte tjenester i kapittel 7, mens status på WiMAX-utbyggingen blir gjengitt i kapittel 8. Tilslutt følger en oppsummering i kapittel 9.

2 WiMAX – en kort oversikt

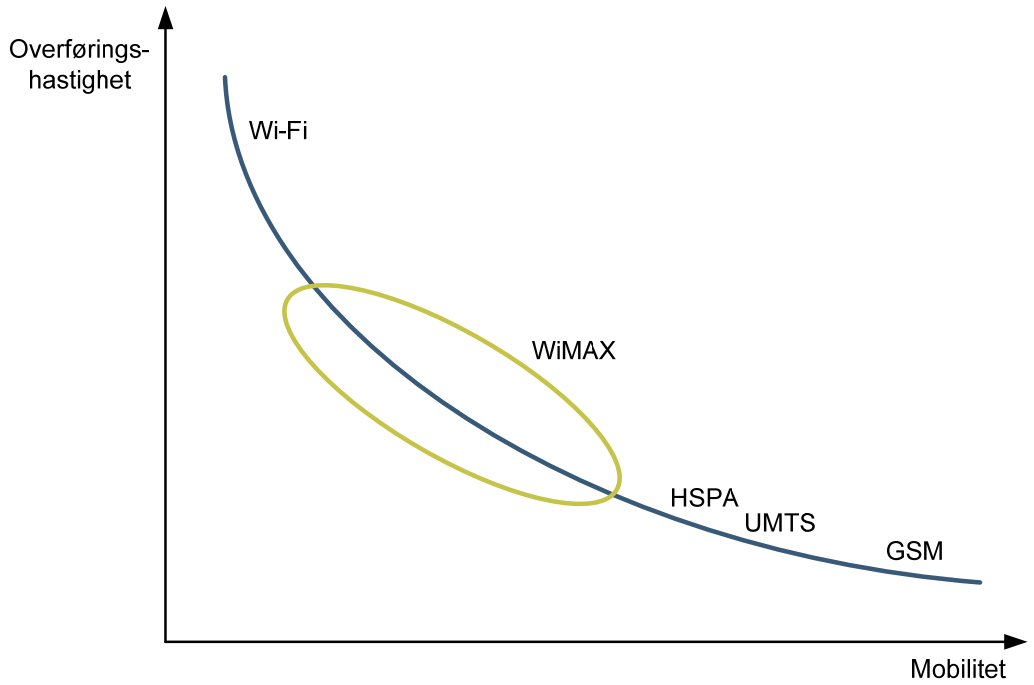
WiMAX baserer seg som tidligere nevnt på IEEE 802.16-standarden og er en trådløs bredbåndsaksessteknologi som tilbyr data- og telekommunikasjonstjenester. WiMAX Forum som ble stiftet i 2001 beskriver WiMAX som *a standards-based technology enabling the delivery of last mile wireless broadband access as an alternative to cable and DSL*. Mulige anvendelser av

WiMAX og utviklingen av standardene blir nærmere beskrevet under. WiMAX Forum, som er sentral når det gjelder sertifisering av utstyr og promotering av disse standardene, er beskrevet til slutt i dette kapitlet.

2.1 WiMAX anvendelse

WiMAX er et alternativ for både ulike typer *digital subscriber line* (xDSL) og mobiltelefonteknologiene *global system for mobile communications* (GSM) og *code division multiple access* (CDMA). WiMAX har allerede rukket å bli bygd ut i 148 land, hvor mer enn 621 millioner mennesker har dekning [4]. En annen anvendelse er som trådløs backhaulteknologi for teknologier som Wi-Fi [5] *hotspots* og GSM. WiMAX ble også tidlig tatt i bruk som midlertidig nett under katastrofer. Den ble blant annet brukt til å kommunisere både i, og ut og inn av Aceh i Indonesia etter tsunamien i desember 2004, og av Intel Corporation for å assistere *Federal Communications Commission* (FCC) og *Federal Emergency Management Agency* (FEMA) med deres kommunikasjonsbehov etter orkanen Katrina.

Teknologien tilbyr opp til 72 Mbit/s symmetrisk bredbåndshastighet. I følge WiMAX Forum kan 40 Mbit/s forventes ved celleradier opp mot 10 km for stasjonær WiMAX. Med mobil WiMAX kan man tilsvarende forvente 15 Mbit/s med celleradier på 3 km. Disse tallene gjelder totalkapasitet som deles mellom brukerne. For sammenligning av WiMAX, Wi-Fi og ulike mobilteknologier når det gjelder mobilitet, det vil si evne til å fungere under bevegelse, og overføringshastighet, se Figur 2.1



Figur 2.1 Sammenligning mellom ulike mobilteknologier, WiMAX og Wi-Fi.

På grunn av potensielt høy overføringshastighet stilles det i WiMAX-utbygginger stort krav til backhaulkapasitet [1] i forhold til dagens mobiltelefonsystem. Tradisjonelle backhaulløsninger med kobberlinjer er derfor ikke tilstrekkelige. Det høye kravet til backhaulkapasitet gjør at det er utfordrende å bygge ut WiMAX i områder hvor det mangler eller er begrenset tilgang til fiberbasert infrastruktur.

2.2 WiMAX-utvikling

Arbeidet med IEEE 802.16-standarden startet på slutten av 90-tallet, og den første standarden kom i desember 2001. Denne definerte radiogrensesnitt for et punkt-til-multipunkt (PMP) trådløst bredbåndssystem i frekvensområdet 10-66 GHz. Det ble utviklet ulike tillegg til standarden før ny versjon, IEEE 802.16-2004, kom i 2004. Denne er også kjent som IEEE 802.16d og som tidligere nevnt kalt *stasjonær WiMAX*. I desember 2005 kom et vedlegg til denne standarden som ga støtte for mobilitet. Denne er kjent som IEEE 802.16(e)-2005 eller *mobil WiMAX*. Denne rapporten vil omhandle disse to versjonene, og de vil heretter bli benevnt som *stasjonær WiMAX* og *mobil WiMAX*. Stasjonær og mobil WiMAX er ikke kompatible, da det meste av utstyret må byttes hvis en operatør ønsker å gå over fra stasjonær til mobil WiMAX.

I Tabell 2.1 under er det oppsummert noen av nøkkelegenskapene til den originale IEEE 802.16-standarden, som er mer å regne som en backhaulløsning på grunn av høy frekvens og behovet for frisikt, samt egenskapene til stasjonær og mobil WiMAX.

	802.16	**802.16-2004**	**802.16E-2005**
Utgitt	Des 2001	Juni 2004	Des 2005
Spektrum	10-66 GHz	< 11 GHz	< 6 GHz
Kanalforhold	Frisikt	Ikke frisikt	Ikke frisikt
Bitrate	32-134 Mbps med 28 MHz kanalbåndbredde	Opp til 75 Mbps med 20 MHz kanalbåndbredde	Opp til 15 Mbps med 5 MHz kanal-båndbredde
Luftgrensesnitt	TDMA med TDD og FDD	OFDM og OFDMA med TDD og FDD	Scalable OFDMA med TDD og FDD
Mobilitet	Fast	Fast, portabel	Nomadisk portabel, Full mobilitet
Kanalbåndbredde	20, 25 og 28 MHz	Skalerbar 1.5 til 20 MHz	Skalerbar 1.5 til 20 MHz
Typisk celleradius	2-5 km	7-10 km	2-5 km

Tabell 2.1 Sentrale egenskaper til ulike versjoner av WiMAX.

Videre blir de to mest brukte standardene, mobil og stasjonær WiMAX beskrevet, samt en ny IEEE 802.16m-standard som er på trappene nå.

[1] Med backhaul menes transport mellom aksesspunkter og mer sentraliserte punkter i nettverket

2.2.1 Stasjonær WiMAX

IEEE 802.16-2004(d) åpner for både PMP og multipunkt-til-multipunkt (MP-MP). Bruksområdet er primært som bredbåndsaksess til boliger og foretak som alternativ til trådbunden aksess. Standarden er ment som et alternativ til trådbunden internettilgang i mer spredt befolkede områder, der det å bygge ut kabelbasert infrastruktur er uforholdsmessig dyrt. Fordi man ikke har bevegelse og ikke trenger å ta hensyn til begrenset batterikapasitet, har denne standarden høyere overføringskapasitet enn mobil WiMAX.

Standarden kan også brukes som backhaul for WiFi hotspots, 2G og 3G, og standarden kan brukes nomadisk. Med nomadisk menes flyttbar, det vil si at man må koble forbindelsen ned og opp igjen når man skal flytte seg fra en basestasjon til en neste.

Det fins sertifiseringsprofiler i 3.5 GHz-båndet hvor kanalbredden er enten 3.5 eller 7 MHz, og i 5.8 GHz båndet for 10 MHz kanalbåndbredde. WiMAX Forum sitt kart [6] over WiMAX-utbygginger i verden viser at de fleste nettverk er bygd i 3.5 GHz-båndet, men at det også er noen utbygde nettverk i 2.3, 2.5, 3.3 og 5.4 GHz-båndene, i tillegg til det sertifiserte 5.8 GHz-båndet. Stasjonær WiMAX er standardisert for både frekvensdelt dupleks (FDD) og tidsdelt dupleks (TDD).

2.2.2 Mobil WiMAX

IEEE 802.16-2005(e) støtter foreløpig kun PMP. Med mobilt menes sømløs handover mellom basestasjoner og sektorer og at systemet takler bevegelser opp til og med kjøretøyhastighet. Mobil WiMAX er ment som et alternativ til mobiltelefonsystemene GSM, *Universal Mobile Telecommunications System* (UMTS) og senere også LTE. Og mens GSM og UMTS egentlig er designet for tale, og prøver å tilpasse seg datatrafikk, er mobil WiMAX og LTE designet for datatrafikk. Dermed må talekommunikasjon baseres på en pakkedataløsning.

I dag er det mobil WiMAX som i størst grad blir bygd ut, og teknologien har allerede gått forbi stasjonær WiMAX når det gjelder antall utbygginger.

Sertifiseringsprofiler finnes bare for TDD, og er definert for kanalbåndbreddene 3.5, 5, 7, 8.75 og 10 MHz og for frekvensbåndene 2.3, 2.5 og 3.5 GHz. Utbyggingskartet til WiMAX Forum viser at det er mange utbygginger i både 2.5 og 3.5 GHz-båndet, men også en del i 2.3 GHz-båndet.

2.2.3 IEEE 802.16m

Standarden IEEE 802.16m som forventes å tilfredsstille kravene til 4G teknologi vil etter planen sluttføres i midten av 2010, mens man planlegger de første sertifiseringene av produkter i siste del av 2011. Man regner at teknologien vil være kommersielt tilgjengelig i løpet av 2011/2012. Kravet til 4G er en overføringskapasitet på 100 Mbit/s mobilt og 1 Gbit/s stasjonært. Denne nye standarden, også kalt *Mobile WiMAX Release 2*, skal være bakoverkompatibel med eksisterende mobil WiMAX, Mobile WiMAX Release 1 og 1.5. Det vil si at operatørene bare trenger å skifte

ut kanalkort og programvare, og at brukere av dagens mobile WiMAX-utstyr skal kunne kommunisere med Release 2-systemer.

Den økte overføringskapasiteten forventes oppnådd ved hjelp av flere endringer, blant annet høyere spektrumseffektivitet gjennom mer avansert bruk av MIMO enn tidligere releaser og mindre overhead på fysisk- og MAC-lag. Det vil også være lavere forsinkelse ved hjelp av raskere MAC-signallering og støtte for høyere mobilitet (opptil 350 km/t). Det er også ventet at denne utgaven skal være mer energieffektiv [7].

2.3 WiMAX Forum

WiMAX Forum er en industriledet, nonprofit-organisasjon etablert for å sertifisere og fremme kompatibilitet og interoperabilitet av trådløse bredbåndsprodukter basert på IEEE 802.16/ETSI HiperMAN standarden. ETSI HyperMAN er den europeiske versjonen av WiMAX som adresserer spektrumaksess under 11 GHz. En av WiMAX Forums målsetninger er å akselerere introduksjonen av disse systemene i markedet. De sertifiserer også produkter, som da skal være garantert interoperable.

WiMAX Forum har 500 medlemmer som består av både operatører og ulike utsyrsleverandører, som for eksempel Cisco Systems, Motorola, Nokia og Telenor.

Det er profiler definert i standarden IEEE 802.16 som ikke WiMAX Forum sertifiserer. Her har vi valgt å konsentrere oss om de WiMAX Forum støtter, fordi disse antakelig vil bli mest utbredt.

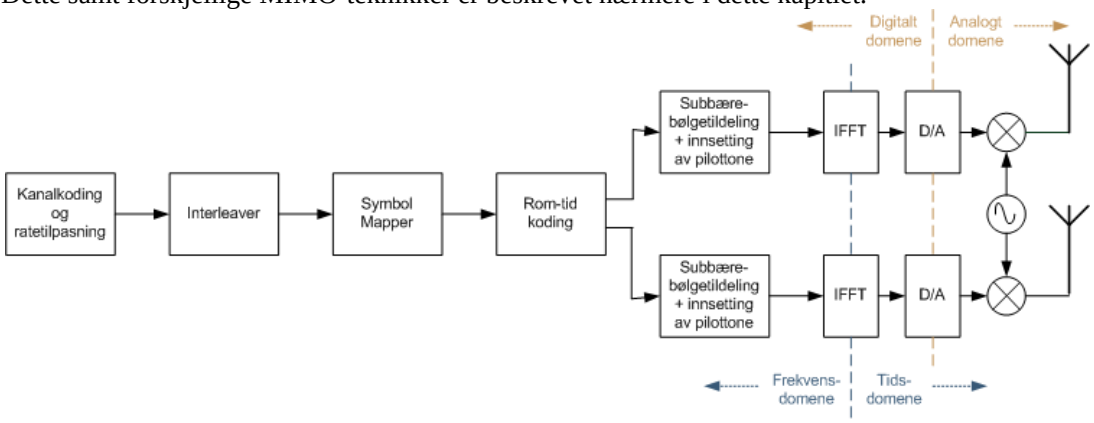
En ulempe med WiMAX og WiMAX Forum er at de ikke er helt åpne med alle valg de har gjort i IEEE 802.16-standardene, om man ikke er medlem. Informasjon om WiMAX må derfor hentes fra ulike kilder, og det kan være vanskelig å finne ut hva som er rett, når ulike kilder ikke stemmer overens. Det kan også være vanskelig å vite hvilken versjon av WiMAX eller IEEE-standarden som blir beskrevet. Dette har vært en utfordring under arbeidet.

3 Fysisk lag

Hensikten med fysisk lag i WiMAX er å få sendt informasjon i form av bits over lufta mellom BS og SS. På fysisk lag blir det brukt svært avanserte teknikker får å oppnå høy spektrumsutnyttelse og dermed høy overføringskapasitet. Det er helt nødvendig å kunne håndtere støy, interferens og varierende kanalforhold på grunn av mobilitet. Utviklingen av fysisk lag i WiMAX er sterkt påvirket av fysisk lag i Wi-Fi, men det er også store forskjeller, siden disse teknologiene er tiltenkt helt forskjellige miljøer. I dette kapitlet er innholdet først og fremst hentet fra [8], [9]og [10], samt at [11] er brukt der det har vært nødvendig for å tilegne seg mer forståelse,

Fysisk lag på WiMAX består i hovedsak av følgende elementer: Kanalkoding, *hybrid automatic repeat request* (HARQ, valgfritt), *interleaving*, symbolmapping, og sist men ikke minst OFDM og de relaterte teknikkene *orthogonal frequency division multiple access* (OFDMA) og *scalable*

OFDMA (SOFDMA). Figur 3.1 viser en oversikt over de funksjonelle trinnene på fysisk lag. Dette samt forskjellige MIMO-teknikker er beskrevet nærmere i dette kapitlet.



Figur 3.1 Funksjonelle trinn på fysisk lag i WiMAX.

3.1 Kanalkoding

Kanalkoding blir utført for hver *forward error correction* (FEC) –blokk, og målet er å oppnå tilstrekkelig robusthet. Økt robusthet vil imidlertid gå på bekostning av lavere informasjonsrate og/eller mer kompleksitet, slik at det her må gjøres en avveining. Kanalkodingen i WiMAX er adaptiv slik at den kan optimaliseres for gjeldende kanalforhold.

Dette kapitlet refererer til hva som er beskrevet i standarden IEEE 802.16e. Der vi har klart å finne ut hva WiMAX har standardisert utover dette, er dette også nevnt. I IEEE 802.16e består kanalkodingen av datarandomisering og feilkorrigerende koding. Dette er nærmere beskrevet under.

3.1.1 Datarandomisering

Datarandomisering foregår både på opp- og nedlink. Det brukes en skiftregistersekvens med maksimal lengde som blir initialisert på begynnelsen av hver FEC-blokk. Skiftregistersekvensen er modulo-2 lagt sammen med datasekvensen for å randomisere dataene. Hensikten med datarandomiseringen er å få til en form for kryptering på lag 1. Når HARQ blir brukt, beholdes samme seed i skiftregisteret, slik at man kan oppnå felles dekoding av den samme FEC-blokken over flere transmisjoner.

3.1.2 Feilkorrigerende koding

Feilkorrigerende koding går ut på å legge inn redundante bit i en datasekvens. Disse bitene kan så bli brukt til å detektere og korrigere feil som har oppstått på grunn av forskjellig type støy. Målet med feilkorrigerende koding er å redusere feilsannsynligheten og/eller nødvendig signal-støyforhold på bekostning av økt båndbredde og kompleksitet.

I mobil WiMAX spesifiseres fire typer feilkorrigerende kode:

- Konvolusjonskode med *tailbiting*
- Konvolusjons-turbokode

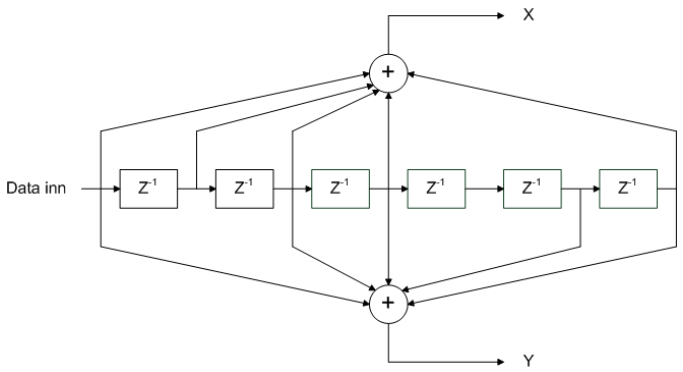
- Blokk-turbokode
- *Low-density parity-check* (LDPC) -kode

Disse er beskrevet nedenfor.

3.1.2.1 Konvolusjonskode med tailbiting

Konvolusjonskodene er en mye anvendt gruppe koder. En viktig egenskap ved denne typen kode er at den har hukommelse. Det er vanlig å angi en konvolusjonskode med *(n,k,K). K* er lengden på skiftregisteret, såkalt *constraint length* og egentlig makslengden på minnet til koden, *k* er antall bit som blir skiftet inn i registeret av gangen, og *n* er antall kodete bit som koden genererer hver gang k bit blir skiftet inn. Koderaten er *k/n*. Med *tailbiting* konvolusjonskode menes at start- og sluttilstanden er den samme, det vil si at bit fra slutten av datablokken blir lagt til begynnelsen for å bli brukt som *flush-bits*. De første paritetsbitene som blir generert av koden er avhengig av bitene forlatt av foregående FEC-blokk, men disse blir slettet. Bruk av tailbiting er båndbreddeeffektivt, men krever mer kompleks dekoding fordi start- og sluttilstand ikke er kjent.

Den obligatoriske kanalkodingen i e-utgaven er en ikke-rekursiv konvolusjonskode med lengde 7 og rate 1/2. I IEEE 802.16e brukes følgende generatormatriser: *g(0) = [1111001]* og *g(1) = [1011011]*. WiMAX støtter følgende koderater: 1/2, 2/3, 3/4 og 5/6. For å oppnå en koderate høyere enn 1/2, benyttes punktering, se delkapittel 3.2.



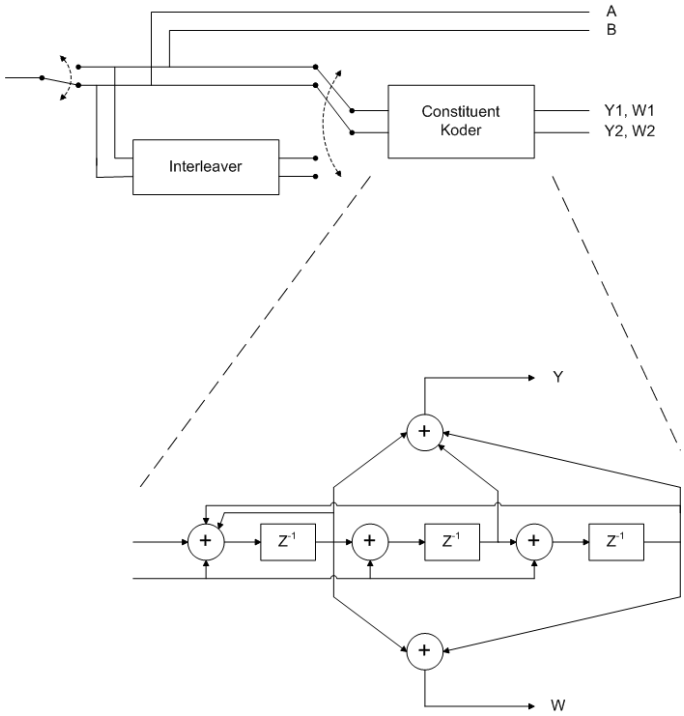
Figur 3.2 Obligatorisk konvolusjonskode for IEEE 802.16e.

I nedlinken på OFDM-mode, blir dataene først kodet med en ytre Reed Solomon kode (se for eksempel [11]), og deretter med en indre binær konvolusjonskode med rate *r = 1/2*.
Før man kjente til turbokode var kombinasjonen Reed-Solomon kode og konvolusjonskode det nærmeste man kom Shannon-grensen. Shannon-grensen sier noe om hvor mye informasjon det er mulig å sende over en kanal med en gitt båndbredde og et gitt signal-støyforhold.

3.1.2.2 Konvolusjons-turbokode

I IEEE 802.16e er det valgfritt å bruke en duobinær turbokode, med en *constituent* rekursiv koder hvor lengden på skiftregisteret er 4. I en duobinær turbokode blir to etterfølgende bit fra den ukodete bit-sekvensen sendt til koderen samtidig, og den genererer to utsekvens-bit, med følgende generatormatriser: *g(0) = [1011]* og *g(1) = [1001]*. Siden to etterfølgende bit er brukt

som simultane innsekvens-bit, har denne koderen fire mulige tilstandsoverganger, sammenlignet med to mulige tilstandsoverganger for en binær kode. Duobinær turbokode er en form for ikke-binære turbokoder, og disse har mange fordeler fremfor konvensjonelle binære turbokoder når det gjelder bedre konvergens, større minimumsavstand mellom kodeord, mindre sensitivitet med hensyn til punkteringsmodell, samt mer robust dekoder. Med punkteringsmodell menes hvilken modell man bruker for å slette kodete bit på en systematisk måte for å øke koderaten. Den duobinære konvolusjons-turbokoden med rate $r = 1/3$, som er benyttet i IEEE 802.16e, er vist i Figur 3.3.



Figur 3.3 Duobinær konvolusjons-turbokode anvendt i IEEE 802.16e.

Utsekvensen blir først separert i seks subblokker: *A, B, Y1, Y2, W1* og *W2*. *A* og *B* inneholder de systematiske bitene, *Y1* og *W1* inneholder paritetsbitene til den kodete sekvensen i naturlig rekkefølge, mens *Y2* og *W2* inneholder paritetsbitene til den *interleavede* sekvensen. De kodete paritetsbitene blir så punktert, for å oppnå ønsket koderate, og med HARQ type II (se avsnitt under) kan punkteringsmodellen endres fra en transmisjon til en neste. Disse subblokkene blir deretter *interleavet*, først internt innen hver blokk. Deretter blir henholdsvis *Y1* og *Y2 interleavet* sammen og det samme gjelder *W1* og *W2*.

3.1.2.3 Blokk-turbokode og LDPC-kode

Disse feilkorrigerende kodene er valgfrie, og det blir ansett som lite sannsynlig at noen av disse blir implementert i hverken stasjonær eller mobil WiMAX. Grunnen er at de fleste utstyrsleverandørene har bestemt seg for heller å implementere konvolusjons-turbokoden, på grunn av dens gode feilkorrigerende egenskaper.

Blokk-turbokoden består av to binære utvidete Hamming-koder som blir anvendt på de respektive urørte og *interleavede* informasjonsbitsekvensene. LDPC-koden er basert på en lineær feilkorrigerende kode, som har gode egenskaper for høye koderater. Den er mindre kompleks enn turbokodene. Siden disse kodene i liten grad vil bli brukt, går vi ikke nærmere inn på disse her.

3.2 Rate matching og HARQ

HARQ er en kombinasjon av en feilkorrigerende- og en feildetekterende kode. Det finnes to typer HARQ, kalt type I og type II, og IEEE 802.16e standarden støtter begge. I type I HARQ blir ikke punkteringen endret fra en transmisjon til den neste. Mottakeren bruker nåværende og alle tidligere mottatte HARQ-transmisjoner av datablokken for å dekode den. Påliteligheten til de kodete bitene øker for hver transmisjon, og dermed reduseres feilsannsynligheten på dekodingen. Prosessen foregår til blokken blir dekodet uten feil, det vil si passerer *cyclic rendundancy check* (CRC) -sjekken, eller at maksimalt antall retransmisjoner er nådd. I sistnevnte tilfelle vil et høyere lag, MAC eller Transport Control Protocol/ Internet Protocol (TCP/IP), retransmittere datablokken, og hele HARQ-prosessen starter på nytt.

I type II HARQ reduseres koderaten for hver retransmittering. Det vil si at flere og flere redundante bit blir sendt for hver gang.

3.3 Interleaving

Etter at dataene har blitt kodet, blir de *interleavet* i en to-trinns-prosess. Det første trinnet sørger for at etterfølgende bit ikke havner på nærliggende subbærebølger. Dette sikrer frekvensdiversitet og øker ytelsen til dekoderen. Det andre trinnet sikrer at nærliggende bit vekselvis blir flyttet til mindre og mer signifikante bit i modulasjonskonstellasjonen. Denne *interleaveren* blir ikke brukt hvis man bruker konvolusjons-turbokoden, på grunn av *interleaveren* som allerede ligger der.

3.4 Symbol Mapping

Her blir sekvenser av binære bit konvertert til sekvenser av komplekse symboler. WiMAX bruker adaptiv modulasjon og koding, som gjør at den kan tilpasse seg ulike omgivelser og avstander. De obligatoriske konstellasjonene er QPSK og 16QAM, mens 64QAM er valgfritt. Selv om denne er valgfri, implementerer de fleste denne, i det minste på nedlinken.

3.5 OFDM

Fysisk lag i stasjonær WiMAX er basert på OFDM som er en form for *multi carrier modulation* (MCM). Andre begrep som brukes på samme teknikk er *coded OFDM* (COFDM) og *discrete multi-tone modulation* (DMT). OFDM har gode egenskaper når man ønsker høy datakapasitet, samtidig som man kan ha relativt dårlige radiokanalforhold. Modulasjonsformen har vært kjent lenge, men det er først etter at *fast fourier transform* (FFT) og *inverse FFT* (IFFT)-kretser som er kraftige nok kunne lages billig nok, at anvendelsen har tatt av. I dag blir OFDM brukt i mange systemer som for eksempel Wi-Fi, digitale TV-systemer (for eksempel DVB-T og DVB-H), radiokringkatingssystemer (for eksempel DAB), kablede systemer (for eksempel ADSL) og LTE.

I dette delkapitlet blir OFDM, og de nært beslektede OFDMA og SOFDMA, som er anvendt i mobil WiMAX, beskrevet.

3.5.1 OFDM teori kort oppsummert

OFDM går ut på at en datastrøm med høy datarate deles opp i flere parallelle datastrømmer med lavere rate. Hver av disse datastrømmene moduleres på separate ortogonale bærebølger. Hvis datastrømmen deles i *m* parallelle datastrømmer vil hver datastrøm få rate *1/m* og symbollengden vil øke med faktoren *m*. Intersymbolinterferensen på grunn av flerveisspredning reduseres når symbollengden blir betydelig lengre enn forsinkelsesspredningen på kanalen. OFDM har derfor gunstige egenskaper når man har flerbaner, og modulasjonsformen gjør det også mulig at flere sendere i et nettverk kan sende samme signal samtidig på samme frekvens, da det er mer sannsynlig at signalene vil kombineres konstruktivt, enn ved *single-carrier* systemer.
I tillegg til den lange symbollengden, er det gunstig med et lite guardintervall (opphold) slik at siste del av et symbol ikke interferer med symbolet etter. Dette fører også til mer robusthet med tanke på tidssynkronisering og blir brukt i WiMAX.

I OFDM blir subbærebølgene valgt slik at de er ortogonale i forhold til hverandre. Dette oppnås ved å velge symbolraten slik at symbollengden T_s er nøyaktig lik $1/\Delta f$, der Δf er avstanden mellom subbærebølgene. Derfor vil den totale båndbredden bli omtrent $N*\Delta f$, der N er antall subbærebølger. Ortogonaliteten fører til at krysstale mellom subbærebølgene blir eliminert, og at guardbånd mellom subbærebølgene ikke kreves. Dette forenkler både sender og mottaker, og det kreves ikke egne filtre for hver subbærebølge som i konvensjonell frekvensdelt multiplekser (FDM). Effekten av frekvensselektive kanalforhold, for eksempel fading forårsaket av flerbaner, kan betraktes som konstant over en subbærebølge, hvis subbærebølgen er tilstrekkelig smal. Det er derfor ikke behov for noen komplisert utjevner i mottakeren.

OFDM er spektraleffektiv med en symbolrate nær Nyquistraten. Dette er på grunn av at ortogonalitetsegenskapene diskutert over medfører at bærebølgene kan ligge tett. Det brukes for eksempel 256 bærebølger og FFT basert OFDM i IEEE 802.16d. Av disse blir 192 brukt til dataoverføring.
WiMAX har tre klasser av subbærebølger:

- Data subbærebølger som blir brukt til å transportere data
- Pilot subbærebølger som blir brukt til å transportere symboler som er kjent a priori, og som kan bli brukt til å estimere kanalparametre og til kanaltilpasning
- Null subbærebølger som blir sendt uten effekt, og inkluderer DC-subbærebølger og guard-subbærebølger mot endene av symbolet (i frekvensplanet). Hensikten med disse er blant annet å redusere interferensen mellom tilliggende kanaler.

3.5.2 Syklisk prefiks

På grunn av egenskapene til den Fouriertransformen som benyttes, vil frekvensselektiv fading forårsake interferens mellom nabosubbærebølgene. Metoden som i praksis blir brukt for å fjerne slik interferens kalles syklisk prefiks, og går ut på at siste del av et symbol legges i guardintervallet før dette symbolet. På denne måten kan man ”jukse” seg til et syklisk signal, og

man kan benytte sirkulær konvolusjon som forenkler kanalestimeringen og dermed utjevneren. Å gå i detalj på dette vil føre for langt i denne rapporten. I IEEE 802.16 standarden kan man legge inn syklisk prefiks om utgjør 1/32, 1/16, 1/8 eller 1/4 av hele symbollengden. Ulempen er at guardintervallet og syklisk prefiks fører til dårligere utnyttelse av signalet. En avveining må derfor gjøres ut fra gjeldende kanalforhold, før en velger lengden på syklisk prefiks.

3.5.3 OFDM svakheter

En svakhet med OFDM er at den krever nøyaktig frekvenssynkronisering mellom sender og mottaker, hvis ikke vil ikke lenger subbærebølgene være ortogonale og man vil få krysstale mellom bærebølgene. Årsaken til dårlig frekvenssynkronisering er som oftest feiltilpassede sender- og mottakeroscillatorer eller dopplerskift på grunn av bevegelse. Dopplerskift alene kan bli kompensert for i mottakeren, men i kombinasjon med flerbaner, hvor de ulike refleksjonene vil ha varierende frekvensavvik, er dette vanskeligere å takle. Dette problemet blir større jo større hastigheten blir, og er en begrensende faktor for OFDM i høyhastighetskjøretøyer. Ulike teknikker for å håndtere krysstale er foreslått, men de øker kompleksiteten til mottakeren.

Forholdet mellom maksimalt og gjennomsnittlig signalnivå, *peak-average-ratio,* er relativt høyt for OFDM. Det kommer av at totalnivået er sammensatt av bidrag fra alle subbærebølgene, slik at for et gitt gjennomsnittlig signalnivå, vil maksimalt signalnivå ligge høyere enn for *single-carrier* systemer med samme gjennomsnittlige signalnivå. Dette gir større krav til linearitet i digital-til-analog konverteren og radioens kraftforsterker, som er en av de dyreste komponentene i en radio. Høyt *peak-to-average-power* ratio fører også til relativt dårlig energieffektivitet. Dette er grunnen til at LTE har valgt en annen multiplekser på opplink.

3.5.4 OFDMA

OFDMA er en multipellaksess metode basert på OFDM, som blir benyttet i mobil WiMAX. I OFDMA blir subbærebølgene delt i grupper av subbærebølger og danner subkanaler. En subkanal er en basisenhet når det gjelder ressursallokering på fysisk lag. Den består av flere data- og pilotsubbærebølger. Subbærebølgene i en subkanal trenger ikke å være tilliggende. Disse subkanalene blir deretter tildelt forskjellige brukere. Flere brukere kan også bli tildelt samme subkanal i tilfelle broadcasting. Antall og distribusjon av subbærebølger som danner en subkanal er avhengig av *subcarrier permutation mode*.

Antall subkanaler allokert for å sende en datablokk er avhengig av flere parametre. Dette er størrelse på datablokk, modulasjonsformat og koderate. Nærliggende subkanaler allokert til en enkelt bruker, eller flere brukere hvis broadcast, er referert til som dataregionen til brukeren og blir alltid sendt med samme *burst profile*. I denne sammenheng vil *burst profile* være kombinasjon av valgt modulasjonsformat, koderate og type FEC.

Det er to forskjellige tilnærminger for å fordele subbærebølgene til subkanalene:

- *Distributed subcarrier allocation*/ *Frequency diverse transmission*
- *Adjacent subcarrier allocation*/ *Frequency selective transmission*

I *distributed subcarrier allocation* vil en subkanal inneha subbærebølger vilkårlig plassert i hele kanalbåndbredden. Denne tilnærmingen maksimerer frekvensdiversiteten, mens den utgjør et gjennomsnitt hva gjelder intercelle-interferens. Denne brukes under høye hastigheter og generelt når kanalforholdene endrer seg raskt. *Distributed subcarrier allocation* kan deles i *full usage of subchannels* (FUSC) and *partial usage of subchannels* (PUSC) mode.

I *adjacent subcarrier allocation* velges tilliggende subbærebølger til en subkanal ved hjelp av *band adaptive modulation and coding* (AMC) mode. Her velger man de subbærebølgene som har det høyeste *signal-to-interference-plus-noise ratio* (SINR). Dette kan gi en kapasitetsøkning på opptil 30%. Ulempen med metoden er at den gir mer overhead, og at den krever relativt stabile kanalforhold. Den egner seg derfor ikke for høye hastigheter.

Det er ikke OFDMA i stasjonær WiMAX, men det er lagt inn en mulighet for subkanalisering på opplink. Det vil si at antall OFDM-kanaler som benyttes fra terminalen reduseres, men at totaleffekten beholdes. På denne måten oppnås større rekkevidde, og man kan også kompensere for dempning. Antall kanaler kan reduseres helt ned til 1/16.

3.5.5 SOFDMA

SOFDMA tilfører skalerbarhet til OFDMA. Den skalerer FFT-størrelsen, antall subbærebølger, til kanalbåndbredden, mens frekvensavstanden mellom subbærebølgene er konstant. Ved å holde denne frekvensavstanden konstant, reduseres systemkompleksiteten til smale kanaler og forbedrer ytelsen til bredere kanaler. SOFDMA er OFDMA-moden brukt i IEEE 802.16e. Den støtter kanalbåndbredder fra 1.25 MHz til 20 MHz. På denne måten kan WiMAX teknologi tilpasses ulike frekvensreguleringer og fleksibelt imøtekomme krav fra ulike operatører og *internet service providers* (ISP). FFT-størrelser på 128, 512, 1024 og 2048 er støttet i IEEE 802.16e. I IEEE 802.16d støttes både 256 og 2048 FFT størrelser, men sistnevnte støttes ikke av WiMAX Forum.

3.6 Dupleksing

Ved FDD brukes det ulike frekvenser på opp- og nedlink, mens ved tidsdelt dupleks (TDD) sendes det med samme frekvens på opp- og nedlink, men ved ulike tidsluker. Både IEEE 802.16d og -e standardene støtter i utgangspunktet TDD og FDD. Imidlertid er det kun støtte for begge i stasjonær WiMAX. I mobil WiMAX har man foreløpig valgt å bare støtte TDD.

3.7 MIMO

Multiple input and multiple output (MIMO) er en teknikk der man bruker flere antenner på senderen og/eller mottakeren for å øke yteevnen til kommunikasjonssystemet. MIMO-teknologi får mye oppmerksomhet innen trådløs kommunikasjon fordi den gir en betydelig økning i datakapasitet og rekkevidde uten behov for mer båndbredde og sendereffekt.

MIMO gir romlig diversitet. Flere antenner kan brukes for å fokusere energi (*beamforming*) eller for å generere flere parallelle kanaler for å sende unike datastrømmer, som romlig multipleksing. MIMO kan bli brukt til:

- Øke påliteligheten (redusere feilrate)
- Øke dataraten og dermed systemkapasiteten
- Øke dekningsområdet
- Redusere sendereffekt.

Disse egenskapene ”konkurrerer” med hverandre, og det må gjøres en avveining på hva men prioriterer.

Det mest vanlige i mobile nett, er at basestasjonen har flere antenner, mens mobilenheten har en. Dette minimerer kostnaden på mobilterminalen. Siden kostnadene for RF-komponentene i mobilterminalene går ned, vil det antakelig bli mer vanlig med to antenner også i mobil-enheten etter hvert. Foreløpig er dette mest vanlig i Wi-Fi-utstyr. Her har telefoner, laptop’er og andre enheter ofte to eller flere antenner.

I 802.16-standarden snakker man om *Matrix A, B* og *C*. Disse henviser til den økte dataraten man kan få ved ulike MIMO-teknikker. De henviser til at dataraten økes med henholdsvis faktoren 1, 2 og 4 ganger dataraten i forhold til å ikke bruke MIMO. Hvilken MIMO-konfigurasjon, definert først og fremst i IEEE 802.16e, som skal brukes blir avtalt dynamisk mellom BS og SS. MIMO-konfigurasjonene som er definert, er beskrevet under.

3.7.1 Space Time Code

IEEE 802.16 standarden støtter *multiple input and single output* (MISO)-teknikk som gir transmitter diversitet, ofte kalt *space time code* (STC). Med denne metoden er det to eller flere antenner på senderen og en antenne på mottakeren. Med transmit diversity rate = 1, som tilsvarer ”Matrix A” i standarden, blir forskjellige databit-konstellasjoner sendt på to forskjellige antenner under samme symbol. Den konjungerte og/eller inverse av de samme to konstellasjonene blir så sendt igjen på de samme antennene under neste symbol. Dataraten øker ikke ved å gjøre det på denne måten, men teknikken gir høyere robusthet på grunn av redundans.

3.7.2 Spatial Multiplexing

IEEE 802.16 standarden støtter også MIMO-teknikken *spatial multiplexing* (SMX), også kjent som *transmit diversity rate* = 2 (”Matrix B” i standarden). Istedenfor å sende samme bit over to antenner, sender denne metoden et databit fra den første antenna, og et annet bit fra den andre antenna. Mottakeren trenger flere enn en antenne. Denne formen for MIMO gir økte kostnader på både sender og mottaker, men hvis forholdene er tilstrekkelig gode blir dataraten dobbelt av hva den er for STC.

En spesiell anvendelse av SMX, er at brukere med tilstrekkelig gode signalforhold bruker SMX, slik at mindre tid blir brukt på brukere med gode kanalforhold. Man bruker da ikke MIMO til brukere som har dårlige kanalforhold. På denne måten kan operatøren tilby høyere datarate til

noen brukere og/eller håndtere flere brukere. Forhandlingsmekanismen mellom basestasjon og mobilenhet i WiMAX muliggjør dette.

3.7.3 WiMAX MISO/MIMO med fire antenner

IEEE 802.16 standarden støtter også tre konfigurasjoner med fire antenner. Mode 1 tilsvarer STC, men med dataene sendt fire ganger pr symbol. For hver gang er dataene konjungert og/eller invertert. Dataraten er 1, men signalet blir mer robust. I mode 2 er dataraten = 2, og dataene blir sendt to ganger. Både dataraten og robustheten øker derfor i forhold til en konvensjonell sender.

I ”Matrix C”-mode blir forskjellige bit sendt fra fire antenner per symbol. Raten er her 4.

3.7.4 WiMAX Uplink Collaborative MIMO

”WiMAX uplink collaborative MIMO” går ut på at brukere sender på samme tid på samme frekvens. Denne typen romlig multipleksing øker sektorkapasiteten uten behov for flere antenner på mobilenheten. Disse mobilenhetene samarbeider slik at begge enheter må bli synkronisert i tid og frekvens slik at overlappingen skjer kontrollert. De to datastrømmene vil interferere på hverandre, men så lenge signalkvaliteten er tilstrekkelig god, og mottakerantenna har minst to antenner, kan datastrømmene bli separert igjen. Denne teknikken kalles også *virtual spatial multiplexing*.

3.7.5 Andre MIMO-relaterte teknikker anvendt i WiMAX

En MIMO-relatert teknikk som kan bli brukt i WiMAX er kalt *adaptive antenna steering* (AAS) eller ”beamforming”. Flere antenner og flere signal blir brukt for å øke transmisjonen til en spesiell bruker. Resultatet er redusert interferens, fordi andre brukere mottar lavere signal.

En annen noe brukt teknikk er *cyclic delay diversity*. Kort fortalt går den ut på at ett eller flere av signalene blir forsinket før transmisjon. Denne teknikken ligger utenfor 802.16-spesifikasjonen, men blir allikevel noe brukt.

4 MAC – laget

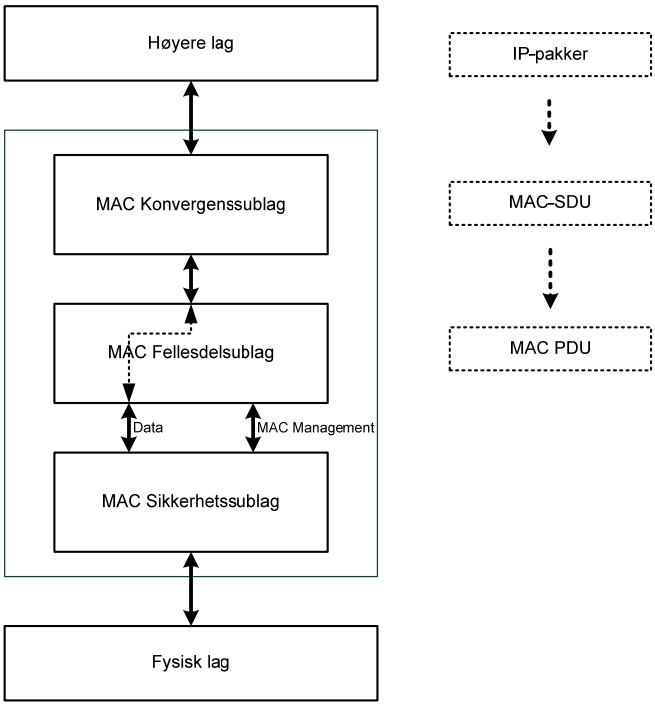
Mens det fysiske laget har ansvaret for å overføre informasjonsbit over lufta mellom BS og SS, har MAC-laget ansvaret for kontroll og multipleksing av disse informasjonsstrømmene. Viktige deler av protokollen for MAC-laget er basert på DOCSIS BPI+ (*Data over cable service interface spesifications: baseline privacy plus interface specification*) protokollen brukt i kabelmodemer. MAC-laget i WiMAX blir delt i tre sublag: MAC-konvergenssublag, MAC-fellesdelsublag og MAC-sikkerhetssublag.

MAC-laget er forbindelsesorientert, og oppretter en logisk forbindelse mellom BS og SS med en enveis *connection identifier* (CID). CID er forskjellig på opplink- og nedlink-forbindelser. Den kan bli sett på som en midlertidig og dynamisk lag 2-adresse mellom MAC-enheter, og blir brukt til å frakte data- og kontrollmeldingstrafikk. Hvilken CID som blir benyttet er ikke bare avhengig

av destinasjonsadressen, men også andre *quality of service* (QoS)-krav. Datatrafikk som skal til samme destinasjon kan derfor bli sendt over ulike forbindelser.

MAC konvergenssublag og –fellesdelsublag er beskrevet under, mens sikkerhetsfunksjonaliteten i WiMAX er nærmere beskrevet i kapittel 6. I tillegg inneholder kapitlet beskrivelser av hvordan WiMAX håndterer båndbreddetildeling, QoS, nettverkstilknytning og initialisering, effektsparing og mobilitetshåndtering. En oversikt over MAC-laget er vist i Figur 4.1.

Innholdet i dette kapitlet er først og fremst hentet fra [8].



Figur 4.1 MAC-laget i WiMAX.

4.1 MAC konvergenssublag

Konvergenssublaget er grensesnittet mellom MAC-laget og lag 3. Laget mottar pakker fra lagene over, som blir kalt MAC *service data unit* (SDU), og har ansvaret for operasjoner som er avhengig av høyere lags protokoller, slik som kompresjon av headere og mapping av adresser. Denne mappingen gjør at IEEE 802.16-standarden kan støtte et bredt spekter av trafikktyper på transportlaget og høyere opp. Standarden definerer konvergenssublag for pakkebaserte tjenester som IP, Ethernet *og asynchronous transfer mode* (ATM). WiMAX Forum har bare implementert IP og Ethernet konvergenssublag.

En av hovedoppgavene til konvergenssublaget er å minimere pakkeheadere. På senderen vil dette si å fjerne repeterende deler av headeren på hver SDU, for eksempel IP-adresser, mens i mottakeren vil det si å reinnsette de samme headerne. Denne protokollen er valgfri, men vil

sannsynligvis i de fleste tilfeller bli implementert, fordi nettverket blir mer effektivt og bedre egnet til å levere tjenester som for eksempel *voice over IP* (VoIP). Utførelsen av *packet header suppression* (PHS), er basert på *PHS-rule*, som angir alle parametre relatert til komprimering av headere.

Når en SDU ankommer, vil MAC-laget tilby en *service flow identity* (SFID), en CID og PHS relaterte parametre som skal brukes. Hva som kan fjernes av headeren, det vil si hvilken *PHS-rule* som blir benyttet, er ofte avhengig av type trafikk. Det er opp til høyere lag å danne *PHS-rule*, og BS og SS må være synkronisert med hensyn til hvilken PHS-rule som benyttes.

4.2 MAC Fellesdelsublag

Et sentralt element i den lagdelte arkitekturen er fellessublaget. Her blir MAC *protocol data unit* (PDU) konstruert, forbindelser etablert og båndbredder forvaltet. Fellesdelsublaget er uavhengig av høyere lags protokoller og utfører oppgaver som trafikkfordeling, QoS-kontroll, tildeling av båndbredde, modulasjon og valg av koderate.

Når SDUer ankommer dette sublaget blir de satt sammen til MAC PDUer. Dette er basisenheten på MAC- og fysisk lag. Avhengig av størrelsen på MAC PDU, vil flere SDU kunne slås sammen i en MAC PDU, eller en SDU vil fordeles på flere MAC PDUer. For å utnytte den fysiske forbindelsen effektivt kan flere MAC PDU med samme mottaker bli konkatenert, og sendt over samme transmisjonsmulighet. Hver MAC PDU er identifisert med en unik CID. Den fungerer som en peker til destinasjons- og innholdsinformasjonen på forbindelsesløs trafikk som IP.

Hver MAC PDU består av en header etterfulgt av nyttelast og en CRC. CRC blir beregnet på hele MAC PDU, både header og nyttelast. WiMAX har to typer PDUer med ulik headerstruktur. Det er den generelle MAC PDU som blir brukt for å frakte data og MAC-signalleringsmeldinger og båndbreddeforespørsel-PDU. Sistnevnte blir brukt av SS for å fortelle BS at det kreves mer båndbredde på opplink. Denne inneholder ikke payload eller CRC. I tillegg definerer WiMAX fem subheadere som kan bli brukt i den generelle MAC PDU.

Når MAC PDUer er konstruert, blir de overlevert til en trafikkfordeler, som fordeler MAC PDUer over den fysiske forbindelsen som er tilgjengelig. Fordeleren sjekker SFID og CID for å bestemme QoS-kravene. Basert på QoS-kravene til MAC PDUer med forskjellige CIDs og SFIDs, vil fordeleren finne den mest optimale resursfordelingen på fysisk lag. Fordelingsprosedyrene ligger utenfor definisjonsområdet til WiMAX-standarden og har blitt overlatt til utstyrsleverandørene å implementere. Ulike valg her vil gi store forkjeller mellom leverandører når det gjelder ytelse.

4.3 Båndbreddeforespørsel og -tildeling

På nedlink blir alle avgjørelser relatert til båndbredder til forskjellige SS tatt av BS, basert på ankommende MAC PDUer sine QoS-krav. Med en gang en MAC PDU har fått tildelt ressurser på fysisk lag for å kunne sende, blir SS informert om dette.

På opplink kan SS be om ressurser ved enten båndbreddeforespørsel-PDU, eller ved å sende med en forespørsel på en generell MAC PDU. Når SS ønsker mer båndbredde enn BS kan tilby, blir de tilbudte ressursene fordelt på de ulike CIDene på bakgrunn av deres QoS-krav. En SS kan ha flere CID.

4.4 Quality of Service

En av hovedfunksjonene til MAC-laget er å sørge for at QoS-kravene til ulike MAC PDUer tilhørende ulike tjenester, blir møtt på en best mulig måte. Dette medfører at egenskaper i forhold til QoS som tidsforsinkelse, variasjon av tidsforsinkelse, datarate, pakkefeilrate og systemtilgjengelighet må tilfredsstilles for de ulike forbindelsene. QoS-kravene til de ulike tjenestene kan variere mye.

QoS-kontroll blir oppnådd ved å bruke en forbindelsesorientert MAC-arkitektur hvor alle opp- og nedlink-forbindelser blir kontrollert av tilhørende BS. Før data blir overført må som tidligere nevnt BS og SS etablere en enveis logisk link, CID, mellom de to MAC-lags enhetene. Denne fungerer som en midlertidig adresse for datatransmisjon over linken. I tillegg til forbindelser for å overføre data, defineres også 3 management-forbindelser for management-meldinger med forskjellig QoS-behov:

- *Basic*-forbindelsen er den første forbindelsen som blir etablert. Den blir brukt til korte og tidskritiske meldinger
- *Primary*-forbindelsen blir også etablert med en gang. Her går det lengre meldinger som tåler en viss forsinkelse.
- *Secondary*-forbindelsen blir brukt til forsinkelsestolerante standardbaserte meldinger som for eksempel IP-managementtrafikk.

De to første blir etablert ved ranging, se delkapittel 4.5.

Som tidligere nevnt definerer WiMAX også en *service flow* (SF). Dette er en enveisflyt av pakker med et spesielt sett med QoS-parametre som blir identifisert med en SFID. Disse SFene kan bli bestemt gjennom management-systemet eller opprettet dynamisk gjennom definerte signalleringsmekanismer i standarden. Basestasjonen er ansvarlig for å utstede SFID og mappe den til unike CIDer.

Det er nødvendig med ulike mekanismer for å håndtere trafikk med forskjellig QoS-krav. MAC-laget i WiMAX har som tidligere nevnt en fordelingstjeneste for å håndtere SDUer og MAC PDUer med ulike QoS-krav. WiMAX definerer fem trafikkfordelingstjenester som skal bli støttet av basestasjonens trafikkfordeler på MAC-laget. Disse er:

- *The unsolicited grant service*: Støtter sanntidsapplikasjoner som generer periodiske datapakker med fast størrelse (for eksempel T1/E1 (telefontrafikk) og VoIP)
- *The real-time polling service*: Støtter sanntidsapplikasjoner som genererer periodiske datapakker med varierende størrelse (for eksempel MPEG-video)

- *The non-real-time polling service*: Samme som over, men ikke krav til sanntid (for eksempel FTP)
- *The best-effort service*: Tilbyr lite QoS-støtte. Data blir sendt når det er ledige ressurser, det vil si ikke i bruk av de andre fordelingstjenestene (for eksempel Web-browsing)
- *The extended real-time polling service*: Ny fordelinstjeneste som kom med IEEE 802.16e-standarden, og som bygger på de to første, men kan tilpasse seg datatjenester hvor kravene til båndbredde endrer seg over tid, men med minimal forsinkelse. (for eksempel VoIP med *silence suppression*.)

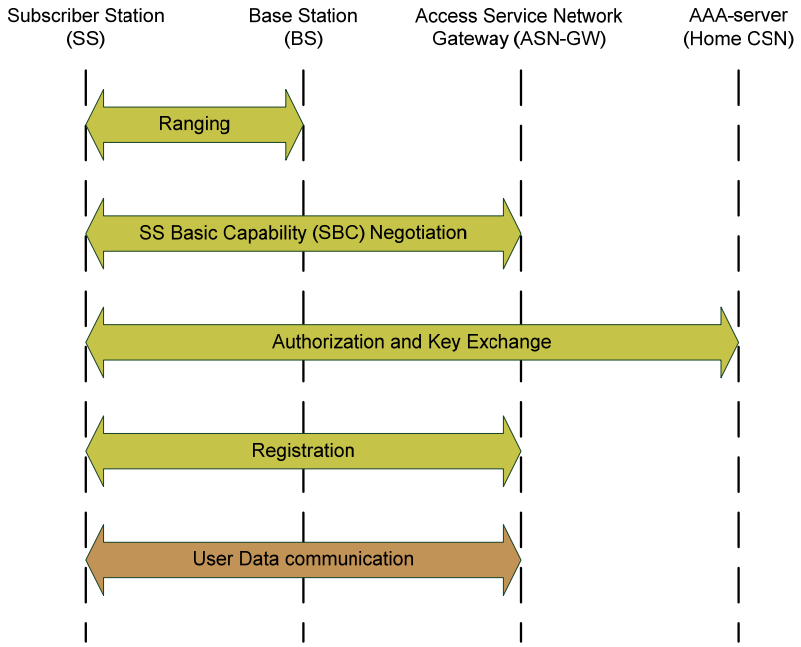
Prosedyren for å håndtere disse fem fordelingstjenestene ligger som tidligere nevnt utenfor WiMAX-standarden.

4.5 Nettverksaksess og -initialisering

Når en SS skal koble seg på nettet, foregår dette gjennom flere trinn. Prosessen for nettverksaksess foregår kort fortalt på følgende måte:

1. Starte SS
2. Lytt etter nedlink-kanaler
3. Synkroniser med nedlink på den BSen man ønsker å aksessere nettet fra
4. Motta opplink-parametre
5. *Ranging*, det vil si synkronisering i tid, samt justering av sendereffekt
6. Forhandle parametre for fysisk lag og båndbredderelaterte parametre
7. SS-autorisasjon og nøkkelhåndtering (se kapittel 6)
8. Registrering i nettverket, samt motta IP-adresse, *Time of Day* og andre parametre
9. Nettverket er klar til å overføre brukerdata

I Figur 4.2 er trafikkflyten som foregår i forbindelse med nettverksaksess og initialisering i WiMAX illustrert. De angitte elementene i nettverksarkitekturen blir nærmere omtalt i kapittel 5.



Figur 4.2 Trafikkflyt i forbindelse med nettverksaksess og initialisering i WiMAX.

4.6 Effektsparing

Sleep mode er en valgfri mode i WiMAX som innebærer at en SS med en eller flere aktive forbindelser avtaler med BS om midlertidig å kutte forbindelsen over lufta i en forhåndsavtalt tidsperiode for å spare batterikapasitet. Etter sleep mode etterfølges en *listen mode* hvor forbindelsen blir koblet opp igjen. Dette skjer for hver CID som SS har til BS. Lengden på hver mode blir avtalt mellom SS og BS og er avhengig av type effektsparingsklasse. Hvilken klasse som blir valgt er avhengig av trafikktypen som går på forbindelsen.

Idle mode er en mode som tillater SS å motta broadcastmeldinger fra BS uten å måtte registrere seg i nettverket. Støtte for denne moden er valgfri. Fordelen med denne moden er at man ikke behøver å foreta noen handover hvis ikke SS er involvert i en aktiv datasesjon.

Ellers benytter WiMAX automatisk effektkontroll i opplink fra brukerterminal. Det vil si at SS ikke sender med høyere effekt enn nødvendig. På denne måten spares ikke bare batteriet, men det er enklere å gjenbruke frekvenser og det reduserer interferens mellom brukere.

4.7 Mobilitetshåndtering

I mobil WiMAX trengs det prosedyrer for å kunne håndtere mobilitet, det vil si at mobiltelefonen flytter seg fra en BS til en annen, uten at forbindelsen brytes. Dette kalles handover og er nærmere beskrevet under.

Handover-prosedyren er ikke helt uproblematisk for IP-protokollen. Selv om IP-protokollen ligger over MAC-laget synes jeg det er på sin plass å ta med noe om problemstillingene rundt dette, se delkapittel 4.7.2.

Hvis man ønsker å koble seg til BS tilhørende en annen operatør kreves roaming og roaming-avtaler. Modeller for dette blir ikke beskrevet i denne rapporten.

4.7.1 Handover

Handoverprosedyren trenger støtte fra lag 1, 2 og 3 av nettverket. Avgjørelsen om handover blir tatt av lag 3, men lagene under spiller en viktig rolle når det gjelder innsamling av informasjon og utførelsen av selve handoveren.

BS allokerer tid for hver SS til å monitorere frekvensbildet og måle radioforholdene til de nærliggende BSer i det området som den befinner seg i. Denne prosessen kalles skanning. Skanningprosessen startes ved at BS sender melding om dette til SS. Denne inneholder lengden på skanningintervallet, lengden på intervallet med normal operasjon, og hvor mange ganger dette skal gjentas. I løpet av et skanningintervall måler SS *received signal strength indicator* (RSSI) og SINR. I løpet av disse intervallene er det også tillatt med innledende *ranging* med nabo-BS, men dette er valgfritt.

Hard Handover (HHO) er basiskonfigurasjonen i Mobil WiMAX. Den foregår ved en hurtig overgang fra en BS til en annen. Når avgjørelsen om handover er tatt, starter SS å synkronisere seg med nedlinktransmisjonen til den nye BS, foretar *ranging* hvis det ikke allerede er gjort under skanning, og deretter avsluttes forbindelsen med tidligere BS. Mulige uleverte MAC PDU'er ved tidigere BS blir tatt vare på en viss tid.

I tillegg kan det nevnes to valgfrie metoder for handover nevnes. Det er *fast base station switching* (FBSS) og *macro diversity handover* (MDHO). Ved disse metodene holder SS en gyldig forbindelse med flere BS samtidig. På denne måten oppnår man større redundans på den fysiske forbindelsen.

4.7.2 Problemstillinger rundt mobil IP

For at en applikasjon skal kunne fortsette under og etter en handover, må IP-adressen til SS ikke endre seg. Mobile IP (MIP) er gjeldende *Internet Engineering Task Force* (IETF)- løsning for IP-mobilitetsproblemet, og dette er designet spesielt til IPv4 for å støtte mobilitet fra et IP-subnett til et annet. Den er transparent både for applikasjonen og på sett og vis også nettverket. Det vil si at applikasjonen ikke trenger å vite at brukeren har skiftet IP-subnett, og at rutingspotokoller eller rutere ikke trenger å bli endret. For å få til dette blir ny og opprinnelig IP-adresse mappet. Det skjer ved hjelp av noen spesialiserte rutere kalt *home agent* (HA) i opprinnelig nettverk, og *foreign agent* (FA) i det besøkte nettverket.

MIP medfører triangulær ruting. Dette betyr at i tilfeller hvor HA og FA befinner seg langt fra hverandre, vil trafikken måtte rutes en lang omvei når trafikken skal til SS. Et eksempel er hvis en person med et norsk hjemme-nettverk vil oppsøke en amerikansk internettside mens han er i USA. Da vil denne trafikken fra internettsiden rutes via Norge. Dette problemet kan løses ved en teknikk kalt *route optimization*, men dette vil til gjengjeld øke kompleksiteten.

Et annet problem kan være at mange brannmurer ikke tillater at pakker kommer fra en topografisk uriktig opprinnelsesadresse. Den mobile noden vil bruke sin hjemmeadresse som *home address*, slik at pakkene vil bli stoppet når de da kommer fra det besøkte nettverket. Dette løses ofte med en teknikk kalt *reverse tunneling*, også her på bekostning av økt kompleksitet.

Mobile IP er ikke i utgangspunktet designet for å håndtere hurtig handover slik som kreves i for eksempel WiMAX, men ulike metoder finnes for å få til dette, som vist i eksemplene over. Den økte kompleksiteten kan imidlertid være et problem for forsinkelsessensitive applikasjoner som VoIP.

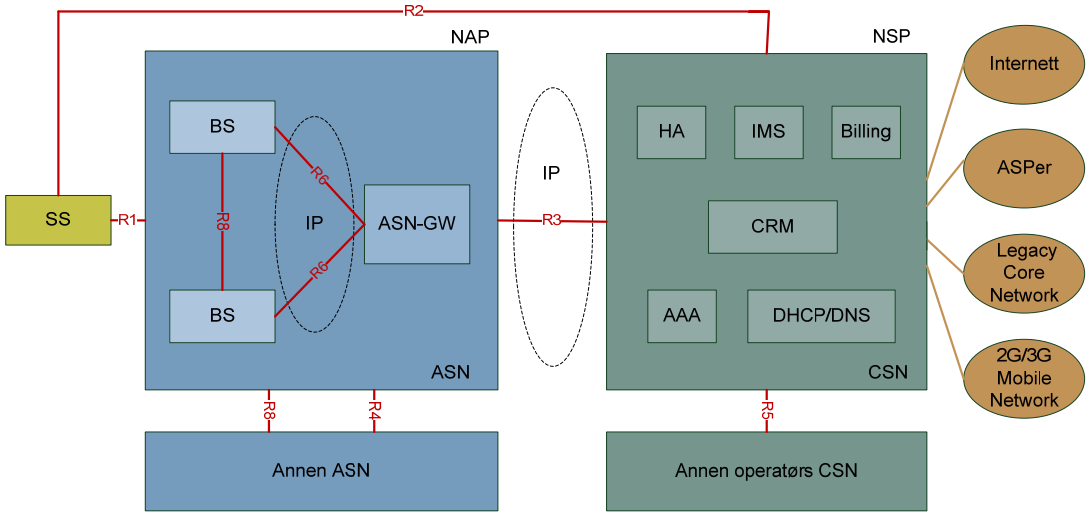
I IPv6 har designerne tenkt på mobilitet helt fra starten av. Dette har medført at IPv6 har bedre løsninger i forhold til mobilitet enn IPv4, hvor dette har blitt tilpasset etterpå. En av de største forbedringene er at *route optimization* er innebygd slik at man slipper triangulær ruting.

5 WiMAX – nettverksarkitektur

WiMAX Forum har utviklet og standardisert en referansemodell for et interoperabelt WiMAX-nettverk som håndterer ende-til-ende tjenester som IP-tilkobling, *session management*, sikkerhet, QoS og mobilitet [1]. Dette rammeverket går utover definisjonsområdet til IEEE 802.16-standarden.

Denne referansemodellen er en logisk representasjon av en WiMAX-nettverksarkitektur. Den identifiserer de funksjonelle enhetene i arkitekturen, og referansepunktene mellom de funksjonelle enhetene hvor det må være interoperabilitet, se Figur 5.1.

Referansemodellen differensierer mellom *network access provider* (NAP) og *network service provider* (NSP). NAP er et foretak som tilbyr infrastruktur for WiMAX radioaksess, mens NSP tilbyr IP-forbindelse og WiMAX-tjenester til WiMAX-abonnenter i henhold til avtalt tjenestenivå med en eller flere NAP. Nettverksarkitekturen tillater en NSP å ha avtaler med flere NAP, og en NAP å bli delt mellom flere NSP. I noen tilfeller vil NAP og NSP være samme foretak.



Figur 5.1 Referansemodell for WiMAX-nettverk.

Følgende forkortelser er benyttet i Figur 5.1:

Forkortelser på elementer i Referansemodellen for WiMAX-nettverk	
AAA	Authentication, Authorization and Accounting
ASN	Access Service Network
ASN-GW	ASN-Gateway
ASP	Application Service Provider
BS	Base Station
CRM	Customer Relationship Management
CSN	Connectivity Service Network
DHCP/DNS	Dynamic Host Control Protocol/Domain Name Server
HA	Home Agent
IMS	IP Multimedia System
NAP	Network Access Provider
NSP	Network Service Provider
SS	Subscriber Station

Som vi ser av referansemodellen, er denne delt i 3 logiske enheter som via CSN kobles til annen infrastruktur som for eksempel GSM og Internett. Videre i dette kapitlet er disse logiske enhetene beskrevet. Tilslutt er det vist en oversikt over de definerte grensesnittene mellom disse enhetene.

5.1 Subscriber Station

Subscriber Station (SS) er brukerterminalen som tilbyr trådløs forbindelse mellom en eller flere brukere og WiMAX-nettverket. Det kan som tidligere nevnt være en stasjonær PC tilkoblet et stasjonært WiMAX-nettverk via et WiMAX-modem, eller en mobil laptop eller smartphone tilknyttet et mobilt WiMAX-nettverk.

5.2 Access Service Network

Access service network (ASN) eies av en NAP og representerer et komplett sett med nettverksfunksjoner som tilbyr radioaksess til SS. Den kan bli implementert som en integrert ASN, hvor alle funksjoner er lokalisert i samme enhet, eller den kan dekomponeres i to separate noder, BS og *ASN-gateway* (ASN-GW). Sistnevnte er mest vanlig, og en slik dekomponert løsning består av en eller flere basestasjoner (BS) og minst en ASN-GW. BS inkluderer de radiorelaterte funksjonene av ASN, med radiogrensesnitt til SS i henhold til MAC- og fysisk lag definert av IEEE 802.16 spesifikasjonene. ASN-GW er en logisk enhet med ansvar for ASN-funksjonene relatert til QoS, sikkerhet og mobilitetshåndtering for alle forbindelser relatert til de BS knyttet til denne ASN-GW.

WiMAX Forum definerte i utgangspunktet tre ulike profiler for ASN, Profil A, B og C. Forskjellen ligger i hvor de ulike funksjonene i ASN ble lagt. Profil B er en distribuert ASN løsning hvor BS og ASN-GW er samlokalisert. Grensesnitt R6 faller derfor bort. I Profil A er *radio resource management* (RRM) splittet, med *radio resource agent* (RRA) i BS og *radio resource controller* (RRC) i ASN-GW. Denne profilen er fjernet i *WiMAX network release 1.5*. I Profil C er RRM ikke splittet og ligger i BS. Dette avviker fra hvordan man vanligvis gjør det i den mobile verden. Profil C ser ut til å være den profilen som flere og flere velger. Det at RRM ikke er splittet gjør det mulig å velge forskjellige leverandører til BS- og ASN-GW-utstyr, noe som er gunstig når det gjelder prisutvikling på utstyr. For å øke interoperabiliteten er derfor dette gunstig.

Flere store leverandører som Motorola har satset på profil B, men flere endrer nå dette til C, mens Alcatel-Lucent satset på Profil A. Små leverandører som bare vil utvikle enkelte komponenter, som for eksempel basestasjoner, er glad for at utviklingen går mot å velge Profil C.

5.3 Connectivity Service Network

Connectivity service network (CSN) er et sett av funksjoner som tilbyr IP-tjenester til WiMAX-abonnentene. CSN eies av en *network service provider* (NSP), som også håndterer abonnentene og leverer tjenestene. CSN kan innbefatte nettverkselementer som rutere, *authentication, authorization and accounting*-servere (AAA-servere), HAer og brukerdatabaser. Den kan også innbefatte *gatewayer* og/eller nettverksservere for å støtte *multicast*- eller *broadcasttjenester* og lokasjonsbaserte tjenester.

Noen av nøkkelfunksjonene til CSN er håndtering av IP-adresser, inneha AAA-proxy eller -server, abonnentfakturering, støtte for ASN-CSN-tunnelering og inter-CSN tunnelering ved *roaming*, opprettholde forbindelsen til internett, håndtere *IP multimedia services* (IMS) og lokasjonsbaserte tjenester.

Er abonnenten utenfor sitt hjemmenett blir denne betjent av CSN tilhørende den besøkte NSP. Home NSP er der brukeren abonnerer på WiMAX-tjenester. Den besøkte NSP og home NSP er den samme når man ikke har roaming.

5.4 Grensesnitt i nettverksarkitekturen

Mellom de logiske enhetene beskrevet over er det i referansemodellen for WiMAX-nettverk definert 8 grensesnitt. Disse er kort oppsummert i Tabell 5.1.

Grensesnitt	Endepunkter	Beskrivelse
R1	SS og ASN	Radiogrensesnitt
R2	SS og CSN	AAA, IP host-konfigurasjon, mobilitetshåndtering (logisk grensesnitt)
R3	ASN og CSN	AAA, håndheving av policy, mobilitetshåndtering
R4	ASN og ASN	Mobilitetshåndtering
R5	CSN og CSN	Samarbeid mellom den besøkte og home CSN, roaming
R6	BS og ASN-GW	IP-tunnel management for å etablere og ta ned SS forbindelse. Både kontroll- and brukerplanprotokoll. (Valgfritt)
R7	ASN-GW-DP og ASN-GW-EP	Grensesnitt mellom *ASN-GW-Decision point* og -*Enforcement point*. (Valgfritt)
R8	BS og BS	Handover (Valgfritt)

Tabell 5.1 Oversikt over definerte grensesnitt i referansemodell for WiMAX-nettverk.

WiMAX Network Release 1 fremtvinger interoperabilitet over grensesnittene R1, R2, R3, R4 og R5 for alle ASN-profilene. De andre referansepunktene er valgfrie. I Release 2 skal det være mulig med handover til andre systemer som Wi-Fi og 3G.

6 Sikkerhet

Hva man legger i ordet sikkerhet, er avhengig av temaet som diskuteres. Når det gjelder informasjonssikkerhet i informasjonsnettverk snakker man ofte om følgende tre grunnleggende sikkerhetsegenskaper:

- Konfidensialitet – sikre mot informasjonslekkasjer
- Integritet – sikre at informasjonen er korrekt og ikke endret
- Tilgjengelighet – sikre tilgang til tjenester og informasjon

En nettverksbruker og en nettverksoperatør vil ikke nødvendigvis være opptatt av de samme sikkerhetsegenskapene. Nettverksbrukeren vil være mest opptatt av personvern, dataintegritet, aksess til tjenester og at faktureringen blir riktig. Nettverksoperatøren derimot er opptatt av autentisering av bruker og enhet, og at brukeren er autorisert for tjenesten han benytter. I tillegg er også operatøren opptatt av riktig fakturering. Dette er oppsummert i Tabell 6.1 under. I høyre kolonne er også sikkerhetsløsningene i WiMAX mobil oppsummert. Disse vil bli nærmere beskrevet i dette kapitlet.

Interessent	Sikkerhetsinteresse	Kommentar	Løsning i WiMAX(e)
Nettverksbruker	Personvern	Beskyttelse mot avlytting	RSA-kryptering, EAP, PKM
	Dataintegritet	Beskyttelse mot endring av data	RSA-kryptering, EAP, PKM
	Aksess til tjenester	Bruker har de rette akkrediteringer	X.509, EAP
Nettverksbruker og -operatør	Riktig fakturering	Riktig og effektiv fakturering	AAA-arkitektur
Nettverksoperatør	Brukerautentisering	Er brukeren den han sier at han er?	X.509, EAP
	Enhetsautentisering	Er enheten den riktige enheten?	X.509, EAP
	Autorisasjon og aksesskontroll	Er brukeren autorisert for å motta ønsket tjeneste?	RSA-kryptering, EAP, PKM

Tabell 6.1 Tabell over ulike sikkerhetsinteresser rundt et WiMAX-system.

De sikkerhetsmekanismene som er beskrevet i IEEE 802.16 d/e standarden er omhandlet i *privacy and key management* (PKM) protokollen. Denne er beskrevet i delkapittel 6.1. Videre følger en beskrivelse av de teknikker og protokoller som PKM bygger på, det vil si X.509 sertifikatet, ulike krypteringsalgoritmer, *extensible authentication protocol* (EAP) og *hash-based message authentication Code* (HMAC).

Remote authentication dial in user service (RADIUS) protokollen blir også beskrevet selv om den ikke inngår i standarden. Dette er gjort fordi denne protokollen er den som oftest blir brukt mellom ASN-GW (autentikator) og AAA-serveren i WiMAX.

Tilslutt i dette kapitlet er sårbarhetene i WiMAX diskutert.

Innholdet i dette kapitlet er i hovedsak hentet fra [12], [13], [14], [15], [16], [17], [18] og [11].

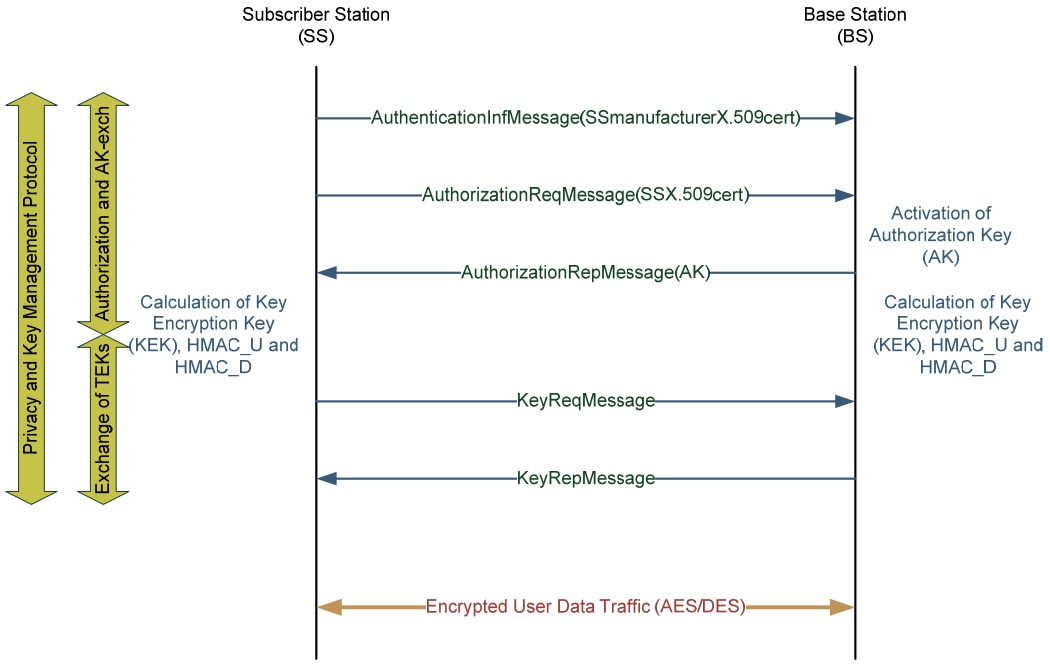
6.1 Privacy and key management (PKM) protokollen

Privacy and Key Management (PKM)-protokollen ligger i sikkerhetssublaget på MAC-laget og håndterer sikkerhetsmekanismene i IEEE 802.16-standarden, se Figur 4.1. Sikkerhetsfunksjonene i WiMAX har i hovedsak to mål. Dette er å tilby personvern, egentlig konfidensialitet, og aksesskontroll til nettverket. PKM er en klient-server modell for sikker utveksling av nøkkelmatriell mellom SS og BS. Det er to versjoner av protokollen, versjon 1, som blir brukt i stasjonær WiMAX, og versjon 2 som ble introdusert med mobil WiMAX. Sistnevnte støtter EAP.

PKM bruker *Security Associations* (SA) som inneholder sikkerhetstilstanden til en forbindelse. Det finnes to typer SA, data SA og autorisasjons SA. Data SA spesifiserer hvordan dataforbindelser mellom BS og SS skal krypteres, det vil si hvilke algoritmer og nøkler som skal

brukes og annen relatert informasjon. Ved å bruke forskjellige SA, kan ulike metoder for kryptering brukes på ulike typer brukertrafikk. Det finnes tre typer data SA: *primary*, *static* og *dynamic*. Det finnes en primary SA for hver tilkoblet SS. Den blir brukt på *secondary management*-forbindelsen og er valgfri, det vil si denne forbindelsen trenger ikke krypteres, og den deles bare mellom SS og BS. *Static* SA blir brukt ved initialisering av SS, mens *dynamic* SA blir opprettet og terminert underveis. Autorisasjons SA blir ikke eksplisitt definert i standarden, men inkluderer en *credential*, en *authorization key* (AK), *key encryption key* (KEK), hash-basert autentiseringskode for opp- og nedlink, og en liste over autoriserte data SAer.

PKM kan deles i to deler. Det ene er autorisasjon og AK-utveksling, og det andre er trafikknøkkel- utveksling, se Figur 6.1. Disse prosessene er nærmere beskrevet under. Etter at TEK er utvekslet, vil brukerdataene bli kryptert med en symmetrisk kryptoalgoritme. I stasjonær WiMAX er dette *Data Encryption Standard* (DES), mens det i mobil WiMAX også kan velges *Advanced Encryption Standard* (AES).



Figur 6.1 PKM versjon 1.

6.1.1 Autorisasjon og AK-utveksling.

PKM autorisasjon blir brukt til å utveksle en AK fra BS til SS. Når SS mottar en initiell autorisasjon, vil den deretter søke reautorisasjon periodisk. Autorisasjonen starter ved at SS sender BS en melding med fabrikantens X.509 sertifikat, se delkapittel 6.2. Denne meldingen kan BS velge å se bort fra, men noen BS kan være konfigurert slik at de bare tillater aksess fra tiltrodde fabrikanter. Den andre meldingen som går fra SS til BS blir sendt umiddelbart etter den første meldingen. Dette er en forespørsel om en AK, og en liste over *SA identities* (SAID) som identifiserer de SAene som SS er autorisert for å delta i. Meldingen inneholder 3

informasjonselementer; fabrikantutstedt X.509-sertifikat, kryptografiske algoritmer støttet av SS, og en SAID for sin *primary* SA.

BS bruker SS sitt sertifikat for å bestemme om SS er autorisert. Hvis dette er tilfelle, vil BS svare med en tredje melding. BS bruker SS sin offentlige nøkkel fått fra sertifikatet til å kryptere AK ved hjelp av RSA. Denne krypterte AKen blir sendt i en melding sammen med et sekvensnummer som skiller mellom suksessive AKer, nøkkelens holdbarhet, og en liste over SAIDer. Denne listen identifiserer de *static* SAer som SS er autorisert for.

6.1.2 TEK-utveksling

Etter at SS har blitt autorisert vil den etablere en SA for hver SAID i lista mottatt fra BS. Dette oppnås ved å initiere en *traffic encryption key* (TEK) utveksling. BS kan starte en slik nøkkelutveksling, men denne muligheten for fremtvingingen av ny nøkkel er ikke obligatorisk. Stort sett er det SS som starter en slik nøkkelutveksling når SS ønsker å fornye nøklene sine. SS sender da en melding som inneholder 3 deler: Sekvensnummeret som refererer til AK brukt i beregning av HMAC, tilhørende SAID og en HMAC som tillater BS å autentisere meldingen.

Hvis HMAC er gyldig vil BS svare med en ny melding. På samme måte som i første melding vil denne inneholde sekvensnummer, SAID og HMAC. I tillegg vil en gammel og en ny nøkkel være inkludert. BS krypterer både den gamle og den nye TEK med 3DES i *electronic code book* (ECB) mode (se kapittel 6.4) i versjon 1 (stasjonær WiMAX) og med KEK assosiert med SA. Krypteringen av TEK kan bli gjort på tre måter i mobil WiMAX. Det er henholdsvis 3DES, RSA(*Public-key Cryptography Standard* (PKCS) #1 v2.0) og AES.

Sikkerheten som ligger i IEEE 802.16-standarden omfatter bare forbindelser for brukerdata og secondary management-kanalen, men sistnevnte som blant annet omfatter IP-managementtrafikk er valgfri. Sikkerhetsmekanismene omfatter ikke basic og primary management-meldinger.

Nøkkellengden på AK og HMAC'ene er 160 bit. TEK er 128 bit (mobil WiMAX) eller 64 bit (stasjonær WiMAX), mens KEK er 128 bit.

6.2 X.509 – sertifikat

X.509-sertifikater er gitt av en *International Telecommunications Union Technical standards group* (ITU-T) standard og er spesifisert i IETF RFC 3280 [19]. I X.509 v3 består sertifikatet av følgende 3 deler:

- Sertifikatinnhold
  - Versjonsnummer
  - Et unikt serienummer tildelt av ansvarlig *certification authority* (CA)
  - Identifisering av signaturalgoritmen som brukes til å signere sertifikatet
  - Identiteten (ID) til CA som utleverte og signerte sertifikatet
  - Gyldighetsperioden
  - Enhet (bruker) ID

    - Offentlig nøkkel til enhet (bruker)
    - Mulige valgfrie utvidelser tillatt i v2 og v3
- Definisjonen av signaturalgoritmen som blir brukt av CA til å signere sertifikatet
- Signatur som garanterer autentisiteten av sertifikatet. Denne består av en hashed sertificate body kryptert med CA sin private nøkkel.

X.509 forutsetter et strengt hierarki av CAer for utstedelse av sertifikater.

6.3 RSA-kryptering

RSA er en algoritme for asymmetrisk kryptering. Det er den første kjente algoritmen som egner seg både til signering og kryptering, og var det første store fremskrittet i offentlig nøkkelkryptering. RSA står for *Rivest, Shamir og Adleman*, som er navnene på de som først beskrev den offentlig. De var alle tilknyttet *Massachusetts Institute of Technology*. Algoritmen består av tre trinn, som er nøkkelgenerering, kryptering og dekryptering.

Et asymmetrisk kryptosystem blir kalt semantisk sikkert hvis en angriper ikke kan skille to krypterte meldinger fra hverandre, selv om angriperen kjenner og har valgt de tilhørende klartekstene. RSA er ikke semantisk sikkert, da krypteringen er deterministisk og ikke har noen random-komponent. I praksis blir derfor ofte RSA brukt sammen med *padding*, for å forhindre visse typer angrep. *Paddingen* går ut på å fylle inn vilkårlige bit på en strukturert måte.

Krypteringen foregår på følgende måte:

$$c = m^e \bmod n,$$

mens ved dekryptering, beregnes

$$m = c^d \bmod n,$$

der m er den paddete klarteksten, c er den krypterte teksten, og n er produktet av to distinkte primtall. Den offentlige nøkkelen består av n og e, mens den private nøkkelen er d. Beregninger av e og d, er relativt komplisert. Å gå inn på detaljene vil ikke være hensiktsmessig i denne rapporten.

RSA skal være en sikker algoritme gitt at nøkkellengden er tilstrekkelig lang og at den er riktig implementert. RSA er mer resurskrevende enn for eksempel 3DES.

6.4 Data encryption standard (DES) og 3DES

Data encryption standard (DES) er den mest kjente databaserte krypteringsmetoden. Dette er en symmetrisk blokk-kryptering som ble introdusert av IBM i 1975, og ble valgt til en offisiell Federal Information Processing Standard (FIPS) for USA i 1976. Den har etter hvert fått en utstrakt anvendelse, selv om sikkerheten blir betegnet som svak. Nøkkellengden er 64 bit, mens bare 56 av disse blir brukt i kryptoalgoritmen, noe som blir betegnet som for kort. Den er knekkbar i løpet av noen timer ved hjelp av *brute force*-teknikker.

Kort fortalt går DES-algoritmen ut på at datablokken på 64 bit blir delt i to nye blokker på 32 bit. Disse blokkene blir kryptert (Exclusive OR) med 48 bits subnøkler vekselsvis. Litt enkelt kan man si at man bruker den ene halve datablokken til å modifisere den andre halve datablokken, deretter bytter de plass. Dette kalles et *Feistel nettverk*. Blokkene blir kjørt 16 runder før krypteringen er ferdig. Feistel-strukturen sikrer at kryptering og dekryptering blir veldig like prosesser. Eneste forskjellen er at subnøklene blir brukt i omvendt rekkefølge ved dekryptering. Subnøklene på 48 bit blir generert ut fra 64 bits nøkkelen.

I WiMAX brukes DES for kryptering av brukertrafikk i stasjonær WiMAX i cipher-block chaining (CBC) mode. CBC-mode innebærer at hver blokk med klartekst blir XORet med den forrige krypterte blokken, mens den første blokken blir XOR'et med en initialiseringsvektor. På denne måten vil to like klartekstblokker ikke gi samme krypterte blokk.

DES kan også velges i mobil WiMAX. Som tidligere nevnt er også AES mulig i mobil WiMAX, og det er god grunn til å anta at de fleste utstyrsleverandører velger AES som er betydelig mer sikker.

For å få en sterkere algoritme, men fortsatt kunne bruke hardware laget for DES, innførte man 3DES. Denne har fått navnet fordi den anvender DES tre ganger på samme blokk. 3DES bruker et knippe med tre DES nøkler, K_1, K_2 og K_3, hver på 56 bit. 3DES krypterer først klarteksten med K_1, deretter dekrypterer den dette med K_2, før den tilslutt krypterer dette igjen med K_3. Ved dekryptering reverseres denne prosessen, det vil si at man først dekrypterer den krypterte teksten med K_3, deretter krypterer med K_2, før det tilslutt dekrypteres med K_1. Hver trippelkryptering krypterer en datablokk på 64 bit.

3DES blir brukt blant annet av den elektroniske betalingsindustrien og av Microsoft i Outlook 2007. Selv om det er vist at algoritmen har noen teoretiske svakheter, fungerer den tilfredsstillende i praksis, og den er foreløpig ikke knekt ved *brute force*-teknikker.

Ved formidling av TEK, blir denne kryptert med 3DES i ECB- mode i stasjonær WiMAX. ECB-mode betyr at hver blokk blir kryptert for seg, og at to like blokker med klartekst vil gi samme krypterte blokk. 3DES er valgfritt i mobil WiMAX. Det benyttes en 128 bits KEK-nøkkel ved kryptering av TEK. Det vil si $KEK_1 = KEK_3$,og KEK_1 og KEK_2 er henholdsvis de første 64 bit fra venstre og de første 64 bit fra høyre av AK. Dette gir en nøkkellengde på til sammen 128 bit, men fordi denne moden er følsom for visse *known plaintext*-angrep, er den utpekt av *National Institute of Standards and Technology* (NIST) til bare å ha 80 bits sikkerhet [20].

Ofte blir DES benevnt med å ha 56 bits nøkkel fordi det bare er 56 av de 64 bitene som blir brukt i praksis.

Et annet navn på algoritmene er henholdsvis *data encryption algorithm* (DEA), og *triple data encryption algorithm* (TDEA). Algortimene er blant annet definert i [21] og [22].

6.5 Advanced encryption standard (AES)

Selv om 3DES hittil har vist seg motstandsdyktig mot kryptoanalyse i praksis, har den visse teoretiske svakheter. Det var derfor ønskelig med en omforent algoritme som kunne anvendes også fram i tid, og som blant annet hadde større blokklengde enn DES/3DES. Etter at NIST hadde hatt en utlysning angående forslag til ny *Advanced Encryption Standard* (AES) i 1997, ble Rijmen og Daemen sin algoritme valgt i 2001.

AES bruker en blokklengde på 128 bit og en nøkkellengde som kan være 128, 192 eller 256 bit. I mobil WiMAX er denne algoritmen et alternativ. Der er nøkkellengden 128 bit, både ved kryptering av TEK (KEK) og kryptering av brukerdata (TEK).
For en beskrivelse av hele standarden henvises det til [23]. Veldig kort fortalt består algoritmen av 4 trinn:

- Substitusjon av byte ved hjelp av en *substitution-box* (S-box)- hensikten er blant annet å rote til sammenhengen mellom kryptert tekst og nøkkel.
- Skift av rader – avhengig av rad flyttes byte et gitt antall plasser mot venstre.
- Mikse kolonner – en substitusjon som endrer hvert byte i en kolonne som en funksjon av alle bytene i kolonnen.
- XOR av gjeldende blokk med en utvidet nøkkel med samme størrelse som blokken.

AES definerer 10 runder for 128-bits nøkler, 12 runder for 192-bits nøkler og 14 runder for 256-bits nøkler. Det har ikke vært kjørt vellykkede angrep mot koden på implementasjoner med riktig antall runder. AES er den første offentlig tilgjengelige og åpne kryptoalgoritmen godkjent av NSA for høyt gradert informasjon.

I mobil WiMAX er følgende moder i bruk ved kryptering av trafikkdata:

- CBC – samme mode som også blir brukt på DES i stasjonær WiMAX
- *Counter encryption* (CTR) – denne moden gjør blokk-kryptering om til *stream*-kryptering, der neste *stream*-blokk blir generert ved å kryptere en teller
- *CTR med CBC meldingsautentiseringskode* (CCM)- klarteksten og meldingsautentiseringskoden blir kryptert i CTR-mode, mens meldingsautentiseringskoden blir laget med en variant av AES i CBC-mode

CTR-mode blir ansett for å være bedre enn CBC-mode, fordi den blant annet har mulighet til å parallellprosessere data, og den er enklere å implementere. CCM-mode har en fordel i at den i tillegg gir muligheten til å bestemme autentisiteten til en kryptert melding.

Ved kryptering av TEK brukes ECB-mode, den samme moden som ved kryptering av TEK med 3DES i stasjonær WiMAX.

6.6 Extensible authentication protocol (EAP)

Extensible authentication protocol (EAP) [24] er et autentiseringsrammeverk som blir mye brukt i trådløse nettverk og punkt-til-punkt forbindelser. Dette er et rammeverk og ikke en spesiell

autentiseringsmekanisme. Den tilbyr en standardmekanisme for å støtte ulike autentiseringsmetoder. Det tilbys om lag 40 ulike EAP-metoder.

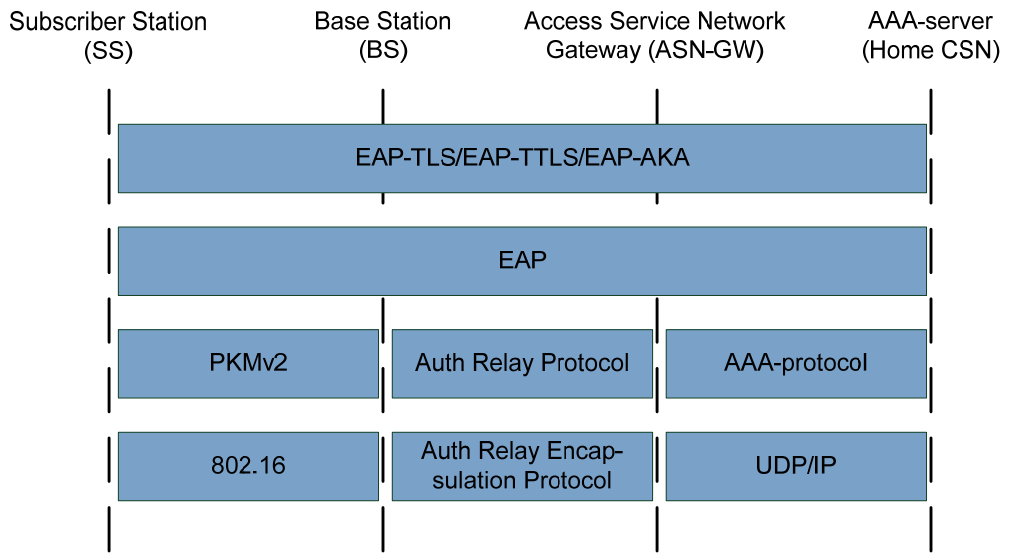
For å oppnå autentisering i forbindelse med link-etableringen, blir EAP-meldinger kodet direkte inn i management-meldinger. Det ble utviklet to nye PKM-meldinger: *PKM EAP request* og *PKM EAP* response, for å transportere EAP-data.

Med EAP-basert autentisering, blir SS autentisert enten gjennom et unikt operatørutstedt akkreditiv, som et SIM-kort, eller gjennom et X.509-sertifikat. WiMAX Forum foreslår en av de tre følgende metodene, og valget avhenger av operatørens implementeringer:

- EAP-AKA (*authentication and key agreement*) for *subscriber identity module* (SIM)-kortbasert autentisering [25].
- EAP-TLS (*transport layer security*) for X.509 basert autentisering [26].
- EAP-TTLS (*tunneled TLS*) for *Microsoft-Challenge Handshake Authentication Protocol* (MS-CHAPv2) [27].

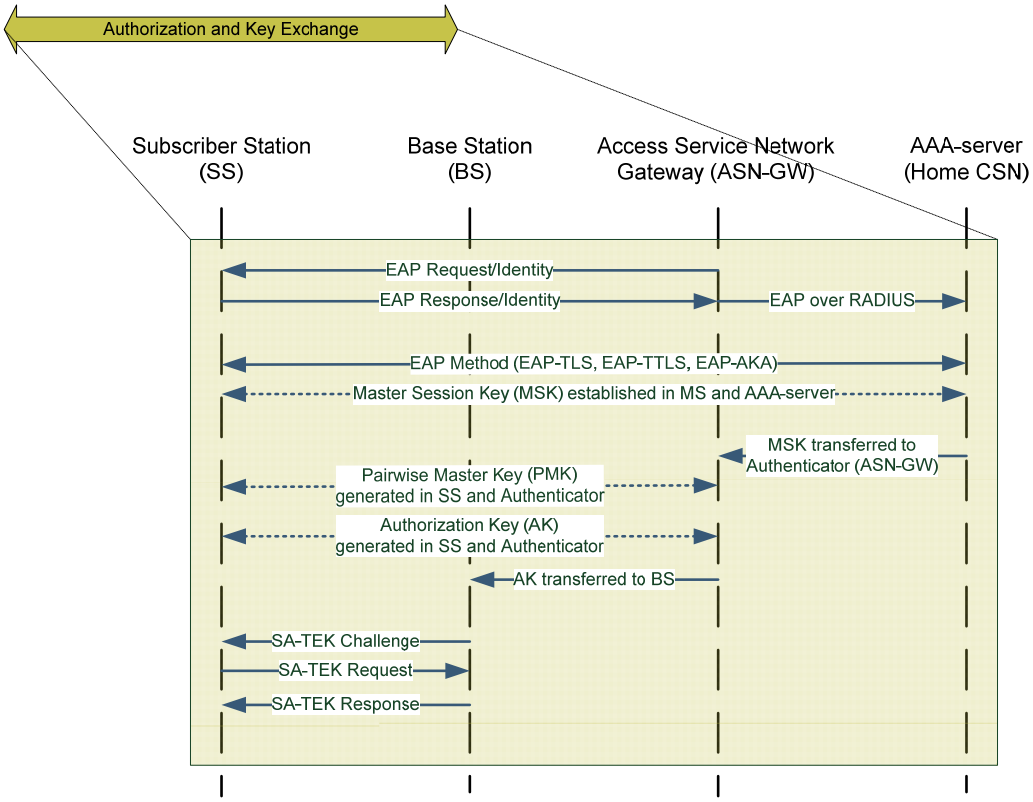
Førstnevnte blir også benyttet i UMTS. EAP-TLS bruker *Public Key Infrastructure* (PKI) for å sikre kommunikasjonen til en RADIUS autentiseringsserver eller en annen type autentiseringsserver. Den regnes for å være en av de mest sikre EAP-standardene tilgjengelig, og er den opprinnelige trådløse *local area network* (LAN) EAP-autentiseringsprotokollen. Den blir støttet av de fleste leverandører. En ulempe med metoden er mye overhead i forbindelse med klientsertifikatene. EAP-TTLS er like god som EAP-TLS, men enklere når flere klienter skal autentiseres.

EAP støtter seg på PKM versjon 2 mellom SS og BS, og AAA-protokollen mellom ASN-GW og AAA-server i CSN. Disse igjen ligger over henholdsvis IEEE 802.16-standarden og *User Datagram Protocol/ Internet protocol* (UDP/IP). Dette er vist i Figur 6.2.



Figur 6.2 EAP autentiseringsprotokoll.

Autorisasjon og nøkkelutveksling med EAP er en relativt komplisert prosess. En oppsummering av dette er skissert i Figur 6.3.



Figur 6.3 Autorisasjon og nøkkelutveksling med EAP.

6.7 Hashed message authentication code (HMAC)

Hashed message authentication code (HMAC) blir brukt for å autentisere meldinger. IEEE 802.16-standarden spesifiserer at *basic* og *primary* MAC management meldinger blir sendt i klartekst i forhold til å forenkle registrering, *ranging* og normal drift av MAC. Det er derfor viktig med autentisering av MAC-meldinger.

Ved å bruke HMAC kan mottaker verifisere hvem som sendte meldingen, samt at meldingen ikke er endret. Dette er mulig fordi sender beregner en HMAC av meldingen han ønsker å sende med en nøkkel som bare sender og mottaker vet. Når mottaker får meldingen beregner han sin egen HMAC av meldingen ved å bruke den samme nøkkelen, og sammenligner resultatet med den han mottok fra senderen. Hvis HMACene er identiske, så er senderen bekreftet, samt at selve meldingen ikke er endret. I IEEE 802.16e-2005 er det også mulig å bruke *cipher-based message authentication code* (CMAC) som et alternativ til HMAC.

HMAC-nøklene blir beregnet i SS og BS ut fra AK, og i WiMAX er det *Secure hash algorithm* (SHA-1) [28] og *Message digest algorithm 5* (MD5) [29] som blir benyttet.

6.8 Remote authentication dial in user service (RADIUS)

Den mest vanlige brukte standarden for kommunikasjon mellom autentikator/aksesserver (ASN-GW) og autentiseringsserveren i WiMAX er RADIUS. Dette er en nettverksprotokoll som tilbyr sentraliserte AAA-tjenester for maskiner som ønsker å koble seg til og bruke nettverkstjenester. RADIUS er en klient-server protokoll på applikasjonslaget som bruker UDP som transporttjeneste. Nettverksaksesserveren som kontrollerer aksessen til nettverket har en RADIUS klientkomponent som kommuniserer med en RADIUS server. RADIUS tilbyr tre funksjoner:

- Autentisere bruker eller enhet for å få aksess til nettverket
- Autorisere disse brukerne eller enhetene for gitte nettverkstjenester
- Beregne kostnadene ved bruk av disse tjenestene.

Autentiseringen og autoriseringen foregår på følgende måte:

1. Bruker eller enhet sender en forespørsel til aksesserveren (ASN-GW) for å få aksess til en gitt nettverksressurs ved å bruke aksessakkreditiver (passord, smartkort, sertifikat og lignende).
2. Deretter sender aksesserveren en RADIUS *access request*-melding til RADIUS-serveren. Dette er en forespørsel om autorisasjon via RADIUS-protokollen. Denne forespørselen inkluderer akkreditiver, samt annen informasjon som kan være interessant, for eksempel nettverksadresse.
3. RADIUS-serveren sjekker at informasjonen er riktig. Brukerens identifiseringsbevis blir verifisert sammen med annen informasjon relatert til forespørselen. Tidligere kontrollerte RADIUS-serveren denne brukerinformasjonen mot en lokalt lagret flat fildatabase. Moderne RADIUS servere kan også gjøre dette, men de kan også referere til eksterne kilder. Vanligvis er dette *Structured query language* (SQL), Kerberos, *Lightwight*

directory access protocol (LDAP) eller *Active Directory*-server for å verifisere akkreditivene.

4. RADIUS serveren returnerer en av tre responser:
    - *Access reject* – bruker nektes aksess til alle ønskede nettverksressurser
    - *Access challenge* – ingen avgjørelse tatt, serveren trenger mer informasjon
    - *Access accept* – bruker får aksess til alle ønskede nettverksressurser
5. Når brukeren har fått aksess, sender aksesserver en *accounting start* til RADIUS serveren. Deretter vil aksesserveren kunne sende *interim update* -pakker for å oppdatere bruken av nettverket. Tilslutt når nettverkstilgangen lukkes sendes en *accounting stop*.

Autentisering og autorisering i RADIUS er beskrevet i [30], mens *accounting* er beskrevet i [31]. RADIUS blir ofte også brukt ved *roaming* mellom ISPer.

RADIUS-protokollen sender ikke passord i klartekst mellom aksesserveren og RADIUS-serveren. En delt nøkkel sammen med en MD5-hashfunksjon [29] blir brukt for å kryptere passordet. Siden dette ikke blir vurdert til å være en god beskyttelse av brukerens akkreditiver, blir ofte andre metoder brukt i tillegg, for eksempel *IPsec-tunnel*, for å beskytte disse dataene mellom aksesserveren og RADIUS-serveren. Dette gjelder også mellom RADIUS-servere ved *roaming*. Det er bare sikkerhetsakkreditivene som blir beskyttet i RADIUS. Andre brukerspesifikke egenskaper som kan bli sendt sammen med autorisasjonen fra RADIUS-serveren blir ikke beskyttet. Eksempler på dette er *virtual local area network* (VLAN)-medlemskap og *layer 2 tunneling protocol* (L2TP) tunnel-group ID som blir brukt av *virtuelle private nettverk* (VPN).

Hvordan WiMAX-operatører velger å autentisere og autorisere brukere er som tidligere nevnt ikke gitt av standarden. Siden alle de andre sikkerhetsmekanismene bygger på at dette blir gjort riktig, er det viktig at operatørene velger tilfredsstillende her.

6.9 Sårbarheter

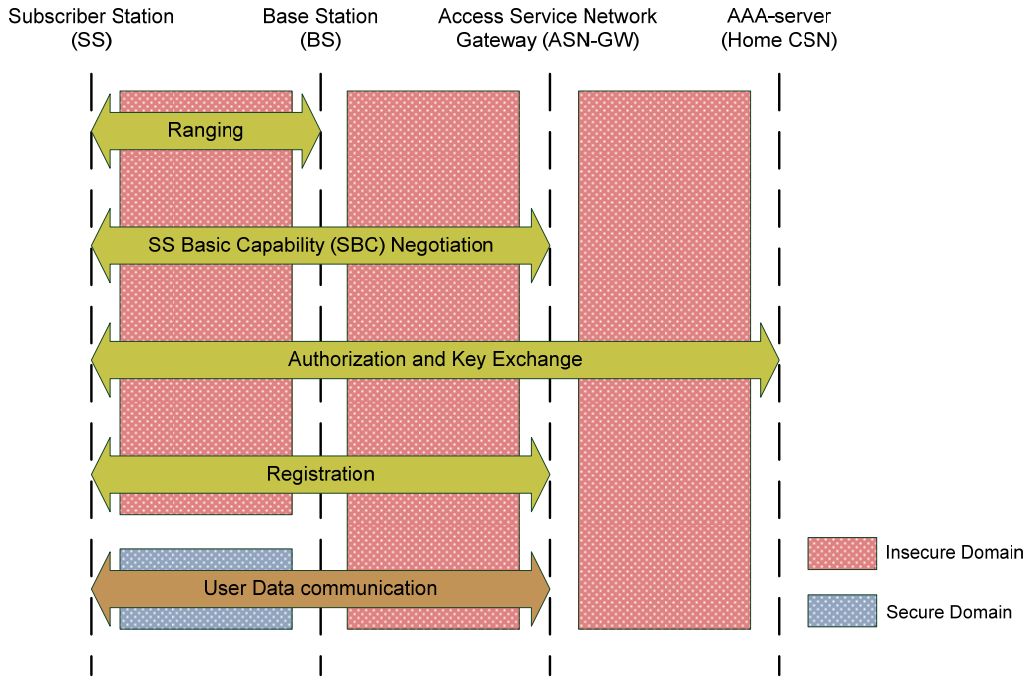
Til tross for ulike sikkerhetstiltak, inneholder WiMAX flere sårbarheter. Hvilke sårbarheter som vil være de største truslene mot sikkerhetsinteressene som er listet opp i Tabell 6.1, er oppsummert i dette delkapitlet.

Den største sårbarheten i både stasjonær og mobil WiMAX er antakelig at managementmeldingene er ubeskyttet. Alt som går på *basic*- og *primary*-kanalen går som tidligere nevnt alltid ukryptert, mens kun *secondary*- managementkanalen kan krypteres hvis ønskelig. Dette er valgt for å effektivisere nettverksoperasjonene. Før man utveksler AK, og man dermed får generert HMAC-nøkler er det heller ingen integritetskontroll. Dette gjør WiMAX-systemene sårbare mot ulike typer trusler. Noen av disse muliggjør:

- *Tracking* av bevegelse og posisjon
- *Denial of service* (DOS)-angrep i forbindelse med nettverkstilgang, for eksempel ved å sende *ranging failed* hele tiden, slik at SS vil fortsette med *ranging* og aldri klare å koble seg på nett.

- Sending av falske meldinger under *SBC Negotiation*, der det påstås at SS kun støtter dårligste form for kryptering. På denne måten tvinger man SS og BS til å kommunisere med for eksempel DES som er relativ enkel å knekke.
- Sending av ulike typer falske management-meldinger som får SS til å sende hele tiden, slik som for eksempel i punktet over. Dette vil senke batterilevetiden.
- *Replay*-angrep hvor for eksempel angriperen får tak i *authorization request*-meldingen fra SS, og resender denne til BS kontinuerlig. BS vil da bli forvirret av disse gjentatte forespørslene, og sette *authorization response* til feilet.

Når det gjelder konfidensialitetsbeskyttelse, så er dette oppsummert i Figur 6.4. Her ser vi at det kun er mellom SS og BS, og kun brukertrafikken som krypteres. Også brukertrafikken går i klartekst mellom for eksempel BS og ASN-GW.



Figur 6.4 Oversikt over sikre og usikre domener i WiMAX når det gjelder konfidensialitetsbeskyttelse.

En annen stor sårbarhet ligger i at TEK-identifikatoren, som angir hvilken nøkkel som blir brukt til å kryptere meldingene, bare er 2 bit lang. Dette gjør at identifikatoren skifter fra 3 til 0 for hver 4. nøkkel. Det er derfor mulig å utføre *replay*-angrep ved å sende tidligere sendte pakker med denne nøkkelen. Dette kan unngås i mobil WiMAX ved å benytte AES-CCM. Her vil den unike telleren som blir benyttet ved kryptering av hver pakke gi integritetsbeskyttelse.

Det er generelt flere sårbarheter i stasjonær WiMAX, enn i mobil WiMAX. De største er følgende:

- Mangel på sertifikat i BS som hindrer gjensidig autentisering. SS kan ikke være sikker på at autorisasjonsmeldingen som den mottar fra BS er fra den virkelige basestasjonen. Dette gjør SS sårbar for falske BS og *man-in-the-middle*-angrep.
- Kun DES CBC-kryptering av brukerdata. Denne har flere dokumenterte svakheter, og blir ikke lenger anbefalt.
- TEK krypteres med 3DES i ECB-mode. Hvor lange TEK er gyldig, varierer fra 30 min. til 7 dager, med default ½ dag. Med stor datatrafikk og lang gyldighetsperiode vil det være mulig å knekke denne.

Som alle andre trådløse systemer er også stasjonær og mobil WiMAX sårbar for jamming og *scrambling* [9]. Sistnevnte går ut på å jamme i veldig korte øyeblikk for å ta ut enkeltpakker eller deler av disse. Typiske mål kan være kontroll- og management-meldinger. Siden det både er vanskelig og kostbart å beskytte seg mot trusler på fysisk lag, er det ikke vanlig at sivile systemer beskyttes mot dette.

I tillegg er det generelle sårbarheter som går på implementasjon av de ulike sikkerhetsmekanismene. Det er blant annet viktig at det brukes en tilstrekkelig god *random-numbergenerator* til å spesifisere AK og TEK, slik at disse nøklene er kryptografisk forskjellig fra de foregående.

Det er først og fremst brukeren som vil bli rammet av disse truslene i form av dårligere tjenestetilbud på grunn av ulike DoS-angrep og dårligere personvern. Operatøren vil kunne bli rammet mer indirekte på grunn av misfornøyde kunder.

7 Lokasjonsbaserte tjenester

Lokasjonsbaserte tjenester (LBT) er informasjons- og underholdningstjenester tilgjengelig på mobile enheter som tar i bruk den geografiske posisjonen til mobilenheten. Tjenesten har ufattelig mange bruksområder som for eksempel oppslag for å finne nærmeste minibank, navigering til en bestemt adresse, sporing av varer og personer og lokasjonsbestemt annonsering. Nødetatene er dessuten interessert i å kunne spore nødanrop så nøyaktig som mulig.

Med bakgrunn i den enorme veksten lokasjonsbaserte tjenester har vist den siste tiden har vi valgt å beskrive hvordan dette foregår i WiMAX. Først i kapitlet beskrives de ulike teknikkene som blir brukt for å finne geografisk posisjon. Deretter følger to delkapitler som beskriver henholdsvis SS-styrt- og nettverkstyrt lokaliseringsrammeverk, slik det fremgår av LBT-rammeverket i WiMAX [32].

7.1 Teknikker for posisjonsbestemmelse

I WiMAX-nettverk er det ulike metoder for å kunne bestemme den geografiske posisjonen. Disse er følgende:

- *Assisted Global Positioning System (GPS)* – GPS med nettverksbaserte metoder som forbedrer både sensitiviteten i forhold til satellittsignalet og *time to first fix* (TTFF)
    - *SS-Based* som passer best for kontinuerlig posisjonering ved navigering i for eksempel bil
    - *SS-Assisted* som passer best ved en nøyaktig posisjonering, for eksempel ved nødanrop
- *Mobile scan report* – baserer seg på standardparametre som RSSI, *round-trip delay* (RTD), and *relative delay* (RD). Sammen med posisjonen til BSer i området gir dette grunnlag for ulike trianguleringsberegninger.
- *Database lookup* – baserer seg på å få celle-identiteten til BS som SS er koblet til (*serving BS*), og deretter slå opp i en statisk database og finne posisjonen. Metoden har ikke stor nøyaktighet, men kan bli brukt som første estimat på lokasjon ved nødanrop og ved visse søk og annonseringsapplikasjoner.

Assisted GPS har størst nøyaktighet, mens *database lookup* har dårligst. Hvilken metode som blir valgt er avhengig av flere forhold, blant annet hvor nøyaktig man ønsker posisjoneringen.

7.2 SS-styrt lokaliseringsrammeverk

Ved SS-styrt lokalisering mottar SS en lokaliseringsforespørsel fra en applikasjon på enheten eller fra et annet sted i nettverket, og bestemmer deretter posisjonen som den formidler tilbake til applikasjonen. SS kan bestemme posisjonen ved hjelp av en egen enhet, for eksempel et *Global navigation satellite system* (GNSS), eller ved hjelp av broadcastmeldinger utsendt fra BSer i samme område.

For å muliggjøre SS-styrt lokalisering, sender hver BS ut periodiske broadcastmeldinger på lag 2 som definert i standarden IEEE 802.16-2009. Disse meldingene, kalt *LBS-ADV*, tilbyr ulike informasjonselementer relevant for lokalisering, blant annet eksakt posisjon tilhørende serving BS, samt andre BSer i nærheten. Denne informasjonen kan brukes til ulike trianguleringsberegninger for å bestemme posisjon, eller som en initiell grovposisjonering for å forbedre GPS-estimatet. *LBS-ADV* kan også inneholde informasjonselementer som GPS tid- og frekvensnøyaktighet. På denne måten kan SS når som helst og så ofte som ønsket foreta lokalisering uten mer støtte fra nettverkets side. SS leverer lokaliseringsinformasjonen til en applikasjon på SS eller til en applikasjonsserver i nettverket gjennom signalering på høyere lag.

Den eksakte algoritmen som blir brukt til å bestemme posisjonen ligger utenfor fokuset til standarden. Ved SS-styrt lokalisering er det ikke behov for noen spesifikk funksjonell støtte for lokasjonsbaserte tjenester i hverken ASN eller CSN, bortsett fra broadcastmeldingene som sendes fra BS.

Det er vanskelig å finne informasjon om at applikasjonen som forespør lokasjonen til SS blir autentisert eller autorisert før lokasjonen blir bestemt. Det står heller ingenting om at meldingen med lokasjonen blir sikret spesielt i tilfeller hvor applikasjonen ikke ligger i SS.

7.3 Nettverksstyrt lokaliseringsrammeverk

Ved nettverksstyrt lokalisering er ulike deler av nettverket involvert for å bestemme posisjonen. Det brukes samme referansemodell som i vist i kapittel 5, men referansepunktene R1 – R8 er forsterket i forhold til LBT. I tillegg er det innført følgende enheter:

- *Location requester* (LR): Enhet eller funksjon som ønsker lokaliseringsinformasjon om en bestemt SS. LR kan ligge utenfor WiMAX-nettverket eller i SS.
- *Location Server* (LS): LS fastsetter lokaliseringen til en SS, og formidler denne til LR. LS ligger i CSN.
- *Location Controller* (LC): Etter forespørsel fra LS, starter lokaliseringsmålingene av SS. LC har ansvaret for koordineringen av dette og å sende måleresultatene tilbake til LS. LC ligger i ASN.
- *Location Agent* (LA): LA ligger i BS. Den har ansvar for måling, innsamling og rapportering av lokaliseringsrelaterte data til LC over grensesnitt R6. LA-funksjonen kommuniserer med SS over R1 når den forespør eller samler inn måleresultater.
- SS: Utfører ulike prosedyrer relatert til LBT. SS kommuniserer både over grensesnitt R2 med LS og over grensesnitt R1 med LA. Over R2 kan det for eksempel gå forespørsel om posisjon hvis LR ligger i SS, og *assisted GPS*-data hvis SS har behov for dette. Over grensesnitt R1 kan det for eksempel gå *mobile scan report*-data fra SS.

Lokaliseringsprosedyren starter med en innkommende forespørsel fra LR. Forespørselen kommer alltid til LS ved nettverksstyrt lokalisering. Den kan inneholde krav til QoS, som nøyaktighet og forsinkelse.

LR blir autentisert og autorisert før nettverksprosedyrene starter. Når autentiseringen er godkjent initierer LS lokaliseringen. LS velger da mellom kontrollplan-, brukerplan- og miksplan-prosedyrer, avhengig av QoS-kravet til lokaliseringen. Miksplan vil si at både kontroll- og brukerplan brukes. Dette vil koste mye i forhold til signalering og forsinkelse. Til gjengjeld vil man oppnå høyere nøyaktighet. Dette kan være aktuelt innendørs, der GPS-posisjonering alene kan være vanskelig. Kontrollplan- og brukerplanprosedyrene blir beskrevet tilslutt i dette delkapitlet.

Når prosedyrene er utført, og målingene sendt tilbake til LS, blir lokaliseringen bestemt. Hvis SS kan beregne lokaliseringen lokalt, kan denne sende resultatet direkte tilbake til LS. Dette er valgfritt. Tilslutt sender LS SS sin lokasjon tilbake til LR på en sikker måte.

SS lokalisering kan også bestemmes under roaming, både ved at LS i det besøkte nettverket gjør beregningene og sender dette til LS i hjemme-nettverket som sender det videre til LR, eller at beregningene gjøres av LS i hjemme-nettverket, basert på målingene gjort i det besøkte nettverket.

Hvordan autentiseringen og autoriseringen av LR foregår, samt på hvilken sikker måte lokasjonen blir sendt fra LS til LR er det vanskelig å finne noe om. Det står heller ingenting om at lokaliseringsinformasjonen blir sikret over grensesnittene R2, R3 og R6, se Figur 5.1.

7.3.1 Støtte for LBT i kontrollplanet

Den grunnleggende ideen bak lokasjon i kontrollplanet er at grensesnitt R3 blir brukt av LS for lokasjonsbestemmelser. Det vil si at LS påkaller ulike elementer i ASN for å bestemme lokasjonen. Det er støtte for 3 typer av lokasjon i kontrollplanet:

- *Serving base station identity* (BSID)
- Nedlink signalanalyse basert på *mobile-scan-report*
- Opplink signalanalyse basert på *BS measurement report*

Disse tilnærmingene tilbyr ulik grad av forsinkelse og nøyaktighet på lokasjonen. LS velger metode ut fra avveiningen gjort for den gitte forespørselen. Den kontakter så LC i ASN med måleforspørselen, som igjen kontakter LAene som trengs for å få målingene tilbake til LC. Ved bruk av BSID er det ikke nødvendig med noen målinger. LC skal generelt ha oversikt over hvilken BS SS er koplet opp mot, og vil returnere dette umiddelbart til LS. LS slår opp i en database og finner koordinatene til BS, og sender disse tilbake til LR.

Ved nedlink signalanalyse, vil SS måle nedlinksignalet fra *serving BS* og andre BSer i området. SS rapporterer dette tilbake til LA i den BS den er koblet opp mot, deretter videre til LC, og så til LS som foretar beregningene. Tilslutt blir lokasjonen returnert tilbake til LR.

For opplink signalanalyse, vil serving BS koordinere med andre BS i samme område for å måle opplinksignalet fra SS på et gitt punkt i tid og frekvens. Målingene fra disse BSene blir så sendt serving BS, som sender alle målingene tilbake til LC. LC sender det videre til LS som foretar beregningene og sender resultatet til LR.

Fordelen med LBS i kontrollplanet er at SS ikke trenger egen IP-adresse. Kontrollplanlokasjon baserer seg på MAC-lagsforbindelsen med SS.

7.3.2 Støtte for LBT i brukerplanet

Brukerplanet bruker referansepunkt R2 direkte mellom LS og SS. Det vil si at LS sender en forespørsel direkte til SS om enten *mobile scan report* eller GPS-målinger, hvis SS har GPS. Hvis SS kan foreta egne lokasjonsberegninger blir lokasjonen returnert, hvis ikke er det målingene som blir returnert. WiMAX har ingen egen brukerplan-lokasjonsprotokoll, men bruker istedet to ferdige tilgjengelige protokoller, *Open mobile alliance Secure user plane for location* (OMA SUPL) og *Internet Engineering Task Force HTTP enabled location delivery* (IETF HELD).

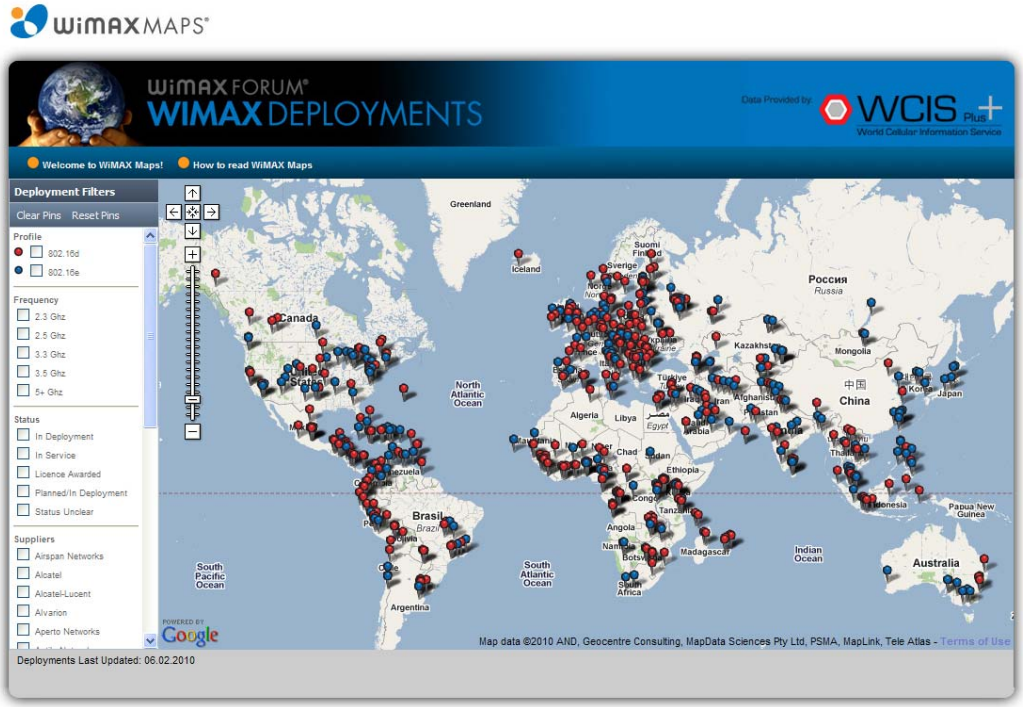
Fordelen med LBT i brukerplanet er at signaleringen over de ulike referansepunktene blir minimert. Men, for å få til dette må SS ha en IP-adresse og være registrert hos LS, og i tillegg må det være støtte på applikasjonslaget for dette i SS. En annen ulempe med brukerplanet er at det i

visse tilfeller kan fungere dårlig, for eksempel innendørs og med GPS, fordi GPS har dårlig dekning i bygninger.

8 WiMAX – utbygging

WiMAX har allerede rukket å bli bygd ut over store deler av verden. I mai 2010 var det registrert 598 nettverk i verden fordelt på 148 land [4]. Dette gjelder nettverk som er i drift eller er under utbygging. Hvor disse befinner seg er vist i Figur 8.. Figuren er hentet fra en internettside utarbeidet av WiMAX Forum [6] og viser stasjonær og mobil WiMAX med henholdsvis røde og blå ”knappenåler”. På internettsiden kan man krysse av på type standard (stasjonær eller mobil), ulike frekvenser, status på nettverket (i drift, under utbygging og så videre) og ulike leverandører, og kun få markert disse nettverkene på kartet. Ved å klikke på et knappenålshode får man opp hvilken operatør dette gjelder samt noen nøkkelopplysninger. Det ser ut til at kartet blir oppdatert flere ganger i måneden.

Ulempen med kartet er imidlertid at posisjonen på knappenålshodet er posisjonert der operatøren har sitt hovedkontor i landet, og ikke på det området WiMAX-nettverket har dekning. WiMAX Forum ønsker etter hvert også å kunne vise dekningsområdet. Mange operatører har imidlertid lagt ut sine dekningskart på internett. Ved å gå inn på Wikipedias liste over WiMAX-operatører i ulike land [33], kan man klikke seg direkte til operatørenes hjemmesider og se på eventuelle dekningskart.



Figur 8. Oversikt over WiMAX-nettverk i verden som er utbygd eller under utbygging.

Hvordan disse nettverkene er fordelt i forhold til verdensdel er vist i Tabell 8.1. I forhold til folketall er det Latin-Amerika som har den største dekningen per innbygger. Her er dekningen ca

20 %. Deretter følger Europa med ca 16 %. Nord-Amerika og Afrika har en noe mindre dekning, mens Midtøsten og Asia-Stillehavslandene har lavest dekning med ca 6 %.

Region	Antall utbygde WiMAX-nett	Antall land med utbygd WiMAX-nett	Antall innbyggere med WiMAX-dekning (mill)
Vest-Europa	79	17	32.5
Øst-Europa	85	21	82.9
Nord-Amerika	53	2	47.0
Latin-Amerika	116	32	113.2
Asia-Stillehavslandene	113	23	237.1
Afrika	117	43	81.3
Midtøsten	29	10	27.4

Tabell 8.1 WiMAX-utbygging i de ulike verdensdelene.

Tallene for antall innbyggere med WiMAX-dekning er fra februar 2010, og viser at da hadde mer enn 621 mill mennesker i verden WiMAX-dekning. Det er ventet at tallet vil stige til 800 millioner innen utgangen av 2010, og 1 milliard ved utgangen av 2011. Når det gjelder antall abonnenter så steg dette med 75 % i 2009 til tross for finanskrisa, og ved utgangen av 2009 var det mer enn 10 millioner abonnenter i verden. Man forventer at veksten vil fortsette i 2010, med store utbygginger i blant annet USA, Japan, Russland og India.

I mange år var det stasjonær WiMAX som hadde flest abonnenter. Det var også helt naturlig siden denne teknologien kom først. 3Q 2009 gikk imidlertid mobil WiMAX forbi stasjonær WiMAX når det gjelder antall abonnenter, og i dag er det for det meste mobil WiMAX som blir bygd ut.

WiMAX har et bredt anvendelsesspekter. Noen former for utbygging er ikke rettet mot personer som ønsker bredbånd, og vil heller ikke gi bidrag til lista over antall abonnenter. Et eksempel på det finner vi i Tyrkias nest største turistby, Bodrum. Der bruker politiet WiMAX-teknologi for å knytte sammen 70 video-overvåkningskameraer. Ved å bruke WiMAX alternativt til leide linjer regner politiet med at de sparer ca $ 60 000 i måneden. Å legge fiber ville ført til uforholdsmessig høye utgifter, i tillegg til at det ville påført den historiske byen store ødeleggelser [34].

Det blir imidlertid spennende å se hvor mange operatører som velger LTE fremfor WiMAX når LTE-teknologien begynner å bli mer moden for utbygging. Russlands største WiMAX operatør, Yota, som har det største mobile WiMAX-nettverket i dag, har sagt at de kommer til å gå for LTE når denne teknologien er klar. En rimelig antakelse er at LTE vil bli valgt av store vestlige operatører som allerede har bygd ut *High Speed Packet Access* (HSPA) og/eller UMTS, blant annet fordi LTE trolig vil kunne integreres tettere i denne infrastrukturen. Mindre operatører med mindre ressurser og liten arv med tanke på HSPA/UMTS vil imidlertid i større grad kunne velge WiMAX, fordi WiMAX-nettverk er rimeligere å bygge ut og enklere å drifte. Hva som velges av

WiMAX og LTE er ofte også et lisensspørsmål ut fra den del av spekteret en operatør har tilgang til.

Når det gjelder WiMAX-utstyr, så hadde WiMAX Forum i mai 2010 sertifisert til sammen 60 basestasjoner og 152 ulike typer brukerutstyr [4]. I løpet av det siste året har det også kommet flere typer mobiltelefoner med WiMAX på markedet. Både HTC og Samsung har allerede to hybrid-modeller hver som i tillegg støtter GSM, UMTS eller CDMA.

9 Oppsummering

WiMAX er en trådløs aksessteknologi for bredbåndstilknytning. Det er to versjoner av denne teknologien som blir bygd ut i verden i dag, og de blir vanligvis omtalt som stasjonær og mobil WiMAX. De baserer seg på henholdsvis IEEE 802.16d- og IEEE 802.16e-standardene.

I denne rapporten har vi beskrevet noen av de viktigste teknikkene brukt i disse standardene. Karakteristisk ved disse er at de bidrar til høy spektrumsutnyttelse og gode egenskaper med tanke på interferens og flerbaner. Sistnevnte blir lett et problem ved høye frekvenser, og spesielt i urbane strøk med mange reflekterende bygninger. De viktigste teknikkene her er OFDM og MIMO. Tilsvarende blir MAC-laget beskrevet.

Videre i rapporten blir WiMAX Forum sin referansemodell for nettverksarkitektur beskrevet, og hva som ligger i de forskjellige elementene i denne modellen. Det som er karakteristisk er at den har en flat struktur, og er beregnet for kun pakkebaserte data. Det første er med på å gi kort forsinkelse.

Sikkerhet blir også tatt opp som et eget tema. Her blir de viktigste protokollene beskrevet, og det følger også en vurdering av WiMAX sine sårbarheter. Denne vurderingen viser at WiMAX har en del sårbarheter, men at mobil WiMAX har bedre sikkerhetsegenskaper enn stasjonær WiMAX.

Siden lokasjonsbaserte tjenester er i ferd med å få enorm popularitet, og at bruken av slike tjenester forventes å øke også i tiden fremover, har vi beskrevet de to rammeverkene som blir brukt i WiMAX for å kunne bestemme geografisk posisjon. Dette er rammeverk for SS-styrt og nettverksstyrt lokalisering.

Tilslutt i rapporten blir status på WiMAX-utbygging gjengitt. Den viser at antall WiMAX-nettverk og antall WiMAX-abonnenter nå øker kraftig. For eksempel økte antall abonnenter med 75 % i fjor, til tross for finanskrisen. Den samme veksten forventes også i 2010. Det blir imidlertid spennende å se hvordan WiMAX og LTE kommer til å dele markedene mellom seg, når utbyggingen av LTE kommer ordentlig i gang om et par års tid.

10 Referanser

[1] "http://www.wimaxforum.org," 2010.

[2] IEEE Standard 802.16-2004, "IEEE Standard for Local and Metropolitan Area Networks-Part 16: Air Interface for Fixed Broadband Wireless Access Systems," 2004.

[3] IEEE Standard 802.16e-2005, "IEEE Standard for Local and Metropolitan Area Networks-Part 16: Air Interface for Fixed Broadband Wireless Access Systems - Physical and Mwdium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands," 2006.

[4] "WiMAX Forum Industry Research Report May 2010, http://www.wimaxforum.org," 2010.

[5] IEEE Standard 802.11, "IEEE Standard for Local and Metropolitan Area Networks-Part 11: Wireless LAN Medium Access Control (MAC) and Phusical Layer (PHY) specifications," 2007.

[6] "http://www.wimaxmaps.org," 2010.

[7] F. Wang, A. Ghosh, C. Sankaran, P. J. Fleming, F. Hsieh, and S. J. Benes, "Mobile WiMAX Systems: Performance and Evolution," *IEEE Communications Magazine*, vol. 46 Oct.2008.

[8] J. G. Andrews, A. Ghosh, and R. Muhamed, *Fundamentals of WiMAX* Prentice Hall, 2007.

[9] J. Kårstad and A. Slåstad, "WiMAX bredbånds radioaksess - en sårbarhetsvurdering,"FFI-rapport 2006/00367 BEGRENSET, 2006.

[10] J. E. Voldhaug, J. Sander, and L. E. Bråten, "WiMAX for Forsvaret,"FFI-rapport 2008/00087 BEGRENSET, 2008.

[11] "http://www.wikipedia.org," 2010.

[12] S. Ahson and M. Ilyas, *WiMAX Standards and Security* CRC Press, 2008.

[13] T. Z. N. Han, Liu Kaiming, and B. L. Y. Tang, "Analysis of Mobile WiMAX Security: Vulnerabilities and Solutions,"IEEE 1-4244-2575-4/08, 2008.

[14] Y. Yang, "Toward WiMAX Security,"IEEE 978-1-4244-4507-3/09, 2009.

[15] T. Shon and W. Choi, "An Analysis of Mobile WiMAX Security: Vulnerabilities and Solutions,"2007.

[16] P. Renguraju, C. H. Lung, and Y. Qu, "Analysis on Mobile WiMAX Security,"IEEE TIC-STH, Information Assurance in Security and Privacy, 2009.

[17] F. A. Ibikunle, "Security Issues in Mobile WiMAX (IEEE 802.16e),"IEEE 978-0-7695-3719-1/09, Mobile WiMAX Symposium, 2009.

[18] M. Barbeau, "WiMAX/802.16 Threat Analysis,"Q2SWinet'05, Oct.2005.

[19] Internet Engineerng Task Force, "RFC 3280: Internet X.509 Public Infrastructure: Certificate and Certificate Revocation List (CRL) Profile, http://www.ietf.org/rfc/rfc3280.txt," 2002.

[20] National Institute of Standards and Technology, "Special Publication 800-57: Recommendation for Key Management - Part 1: General (Revised)," 2007.

[21] U.S.Department of Commerce/ National Institute of Standards and Technology, "Federal Information Processing Standards Publication (FIPS PUB) 46-3: Data Encryption Standard (DES)," 1999.

[22] National Institute of Standards and Technology, "Special Publication 800-67: Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher," 2008.

[23] U.S.Department of Commerce/ National Institute of Standards and Technology, "Federal Information Processing Standards Publication (FIPS PUB) 197: Announcing the Advanced Encryption Standard (AES)," 2001.

[24] Internet Engineerng Task Force, "RFC 3748: Extensible Authentication Protocol (EAP), http://www.ietf.org/rfc/rfc2865.txt," 2004.

[25] Internet Engineerng Task Force, "RFC 4187: Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)," 2006.

[26] Internet Engineering Task Force, "RFC 5216: The EAP-TLS Authentication Protocol,".

[27] Internet Engineering Task Force, "RFC 5281: Extensible Authentication Protocol Tunneled Transport Layer Security Authentication Protocol Version 0," 2008.

[28] National Institute of Standards and Technology, "FIPS PUB 180-1: Secure Hash Standard," 2010.

[29] Internet Engineering Task Force, "RFC 1321: The MD5 Message-Digest Algorithm, http://www.ietf.org/rfc/rfc1321.txt," 1992.

[30] Internet Engineerng Task Force, "RFC 2865: Remote Authentication Dial In User Service (RADIUS), http://www.ietf.org/rfc/rfc2865.txt," 2000.

[31] Internet Engineerng Task Force, "RFC 2866: RADIUS Accounting, http://www.ietf.org/rfc/rfc2866.txt," 2000.

[32] M. Venkatachalam, K. Etamed, W. Ballantyne, and B. Chen, "Location Services in WiMAX Networks," *IEEE Communications Magazine*, vol. 47 Oct.2009.

[33] "http://en.wikipedia.org/wiki/List_of_deployed_WiMAX_networks," 2010.

[34] R. Henshaw, "WiMAX for security: How WiMAX is Enabling the Surge in Video Surveillance," *The WiMAX guide, wimax. com*, Apr.2009.

Forkortelser

AAA – Authentication, authorization and accounting
AAS – Adaptive antenna steering
ADSL – Asymmetric digital subscriber line
AES – Advanced encryption standard
AK – Authorization key
AMC – Adaptive modulation and coding
ASN – Access service network
ASN-GW – Access service network gateway
ASN-GW-DP – Access service network gateway decision point
ASN-GW-EP – Access service network gateway enforcement point
ASP – Application service provider
ATM – Asynchronous transfer mode
BS – Basestasjon
BSID – Serving base station identity
CA – Certification authority
CBC – Cipher-block chaining
CCM – CTR med CBC meldingsautentiseringskode
CDMA – Code division multiple access
CID – Connection identifier
CMAC – Cipher-based message authentication code
COFDM – Coded orthogonal frequency division multiplexing
CRC – Cyclic redundancy check
CRM – Customer relationship management
CSN – Connectivity service network
CTR – Counter encryption
DAB – Digital audio broadcasting
DEA – Data encryption algorithm
DES – Data encryption standard
DHCP/DNS – Dynamic host control protocol/Domain name server
DMT – Discrete multi-tone modulation
DOCSIS BPI+ – Data over cable service interface spesifications: baseline privacy plus interface specification
DOS – Denial of service
DSL – Digital subscriber line
DVB-H – Digital video broadcasting Handheld
DVB-T – Digital video broadcasting Terrestrial
EAP – Extencible authentication standard
EAP-AKA – Extencible authentication protocol authentication and key agreement
EAP-TLS – Extencible authentication protocol transport layer security

EAP-TTLS – Extencible authentication protocol tunneled transport layer security
ECB – Electronic code book
EKOM – Elektronisk kommunikasjon
FA – Foreign agent
FBSS – Fast base station switching
FCC – Federal Communications Commission
FDD – Frekvensdelt dupleks
FDM – Frekvensdelt multipleksing
FEC – Forward error correction
FEMA – Federal Emergency Management Agency
FFT – Fast fourier transform
FIPS – Federal Information Processing Standard
FTP – File transfer protocol
FUSK – Full usage of subchannels
GNSS – Global navigation satellite system
GPS – Global positioning system
GSM – Global system for mobile communicatuions
HA – Home agent
HARQ – Hybrid automatic repeat request
HHO – Hard handover
HMAC – Hash-based message authentication code
HSPA – High speed packet access
ID – Identiteten
IETF – Internet Engineering Task Force
IETF HELD – Internet Engineering Task Force HTTP enabled location delivery
IFFT – Invers fast fourier transform
IMS – IP multimedia system
IP – Internet protocol
ISP – Internet service provider
ITU-T – International Telecommunications Union Technical standards group
KEK – Key Encryption key
L2TP – Layer 2 tunneling protocol
LA – Location agent
LAN – Local area network
LBT – Lokasjonsbaserte tjenester
LC – Location controller
LDAP – Lightweight directory access protocol
LDCP – Low-density parity-check
LR – Location requester
LS – Location server
LTE – Long Term Evolution
MAC – Media access control
MCM – Multi carrier modulation

MD5 – Message-digest algorithm 5
MDHO – Macro diversity handover
MIMO – Multiple input multiple output
MIP – Mobile internet protocol
MISO – Multiple input single output
MPEG – Moving Picture Experts Group
MP-MP – Multipunkt-til-multipunkt
MS-CHAP – Microsoft-challenge handshake authentication protocol
NAP – Network access provider
NIST – National Institute of Standards and Technology
NSA – National Security Agency
NSP – Network service provider
OFDM – Orthogonal frequency division multiplexing
OFDMA - Orthogonal frequency division multiple access
OMA SUPL – Open mobile alliance Secure user plane for location
PDU – Protocol data unit
PHS – Packet header suppression
PKCS – Public-key cryptography Standard
PKI – Public key infrastructure
PKM – Privacy and key management
PMP – Punkt-til-multipunkt
PUSK – Partial usage of subchannels
QoS – Quality of service
RADIUS – Remote authentication dial in user service
RD – Relative delay
RRA – Radio resource agent
RRC – Radio resource controller
RRM – Radio resource management
RSA – Rivest Shamir and Adleman
RSSI – Received signal strength indicator
RTD – Round trip delay
SA – Security association
SAID – Security association identification
S-box – Substitution box
SDU – Service data unit
SF – Service flow
SFID – Service flow identity
SHA – Secure hash algorithm
SIM – Subscriber identity module
SINR – Signal-to-interference-plus-noice ratio
SMX – Spatial multiplexing
SOFDMA – Scalable orthogonal frequency division multiple access
SQL – Structured Query Language

SS – Subscriber station
STC – Space time code
TCP/IP – Transport control protocol/Internet protocol
TDD – Tidsdelt dupleks
TDEA – Triple data encryption algorithm
TEK – Traffic encryption key
TTFF – Time to first fix
UDP/IP – User datagram protocol / internet protocol
UMTS – Universal Mobile Telecommunications System
VLAN – Virtual local area network
VoIP – Voice over Internet protocol
VPN – Virtuelle private nettverk
WiMAX – Worldwide Interoperability for Microwave Access