Mobilt bredbånd med LTE
– teknologi, sikkerhet, tjenester og utbygging

Anne Pernille Hveem

Forsvarets forskningsinstitutt (FFI)

05. april 2011

FFI-rapport 2011/00709

1126

P: ISBN 978-82-464-1939-8
E: ISBN 978-82-464-1940-4

Emneord

LTE

EPC

OFDM

Sikkerhet

Godkjent av

Kjell Olav Nystuen	Prosjektleder
Vidar Stensrud Andersen	Avdelingssjef

Sammendrag

”Long Term Evolution” (LTE) er en ny standard for mobiltelefonsystemer som er utviklet av ”3rd Generation Partnership Project” (3GPP). 3GPP er en frivillig organisasjon mellom operatører og industri fra hele verden. LTE er en trådløs radioaksessteknologi for bredbåndstilknytning med teoretiske bredbåndshastigheter på 100 og 50 Mbit/s henholdsvis ned og opp til basestasjonen, og med frem og tilbake forsinkelse på mindre enn 10 ms. ”Evolved Packet Core” (EPC) er et IP-basert fastnett som knytter LTE-basestasjonene sammen. LTE etterfølger UMTS som igjen etterfølger GSM/EDGE. Det er stor satsning på LTE per dags dato i Europa, Nord-Amerika og Asia. Satsningen på LTE begrunnes først og fremst med at standarden skal gjøre det billigere per megabyte for mobiloperatørene å produsere mobilt bredbånd ved å gjenbruke eksisterende IP-nett, i tillegg til at den også skal levere lavere forsinkelse og høyere båndbredder til kundene. Mange operatører velger LTE også på grunn av sømløs mobilitet mellom GSM/EDGE, UMTS og LTE. Netcom og Telia var de første operatørene i verden som i 2009 satte i drift et LTE-nett. 17 kommersielle LTE-nett er siden satt i drift i 2010. 180 operatører i 70 land investerer i LTE, hvorav det er gjort forpliktende løfter om utbygging av 128 LTE-nett i 52 land.

LTE er et rent IP-basert ”Orthogonal Frequency Division Multiple Access” (OFDMA) bredbåndssystem, med høyere datahastigheter, forbedret spektraleffektivitet og redusert forsinkelse som de viktigste egenskapene. Rapporten beskriver ny teknologi og utfordringer på radioaksessdelen, hvor det er lagt vekt på ”Orthogonal Frequency Division Multiplexing” (OFDM) og ”Multiple Input Multiple Output” (MIMO). Begge teknikkene bidrar til høy spektrumsutnyttelse. I tillegg beskriver rapporten det pakkebaserte IP-kjernenettverket EPC og protokollstrukturen til LTE/EPC. Det er fokus på radioaksess og sikkerhet i rapporten. Til slutt får vi innblikk i tjenester, utbygging og utvikling av LTE, og kort om utviklingen av LTE-Advanced som etterfølger LTE.

English summary

Long Term Evolution (LTE) is a new standard for mobile telephone systems developed by the 3rd Generation Partnership Project (3GPP). 3GPP is a voluntary organization of operators and industry from around the world. LTE is a wireless radio access technology for broadband connections with theoretical broadband speeds of 100 and 50 Mbit/s, respectively downlink and uplink, and with round-trip delay of less than 10 ms. Evolved Packet Core (EPC) is an IP-based fixed network that interconnects LTE base stations. LTE is the successor of UMTS which follows the GSM/EDGE. There is considerable focus on LTE today in Europe, North America and Asia. The focus on LTE is because the standard will make it cheaper per megabyte for mobile operators (reusing existing IP networks) to produce mobile broadband; in addition it will deliver lower delay and higher bandwidths to customers. Another main reason to choose LTE is its seamless mobility with GSM/EDGE and UMTS. Netcom and Telia were the first operators in the world to put into operation a LTE network in 2009. 17 commercial LTE networks have been in operation since 2010. 180 operators in 70 countries are investing in LTE, of which commitments for development of 128 LTE networks in 52 countries has been made.

LTE is a pure IP packet-based “Orthogonal Frequency Division Multiple Access” (OFDMA) broadband system, with higher data speeds, improved spectral efficiency and reduced delay as the most important properties. The report describes the new technology and challenges on the radio access, where the emphasis is on “Orthogonal Frequency Division Multiplexing” (OFDM) and “Multiple Input Multiple Output” (MIMO). Both techniques contribute to the high spectrum utilization. In addition the report describes the packet-based IP core network EPC and protocol structure of the LTE/EPC. The report has focus on the radio access and security. Finally it looks into services, construction and development of LTE and a short introduction of the development of LTE-Advanced, the LTE successor.

Innhold

1 Innledning

Det pågår i dag en rivende utvikling innen infrastruktur for offentlig elektronisk kommunikasjon (EKOM). I dette bildet er det blant annet 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 1126 UNET på FFI gjøres sammenfattende beskrivelser av noen utvalgte relevante sivile EKOM-systemer og – teknologier. I denne rapporten beskrives LTE/EPC. I en tidligere FFI-rapport er WIMAX beskrevet [1].

1.1 Målsetting med rapporten

Rapportens målsetting er å gi en innføring i teknologien til både ”Long Term Evolution” (LTE) på radioaksessiden og kjernenettverket ”Evolved Packet Core” (EPC). LTE/EPC representerer ”state of the art” innen mobilkommunikasjon og er et komplekst system. Rapporten kan i tillegg til opplæring av leser innenfor emne, gi innspill til problematikken med håndtering av overganger mellom hierarkiske systemer. Det er lagt fokus på å beskrive ny teknologi og utfordringer på radioaksessen, i tillegg til realisering av sikkerhet i systemet. Rapporten beskriver, i tillegg til andre temaer, det pakkebaserte IP kjernenettverket EPC.

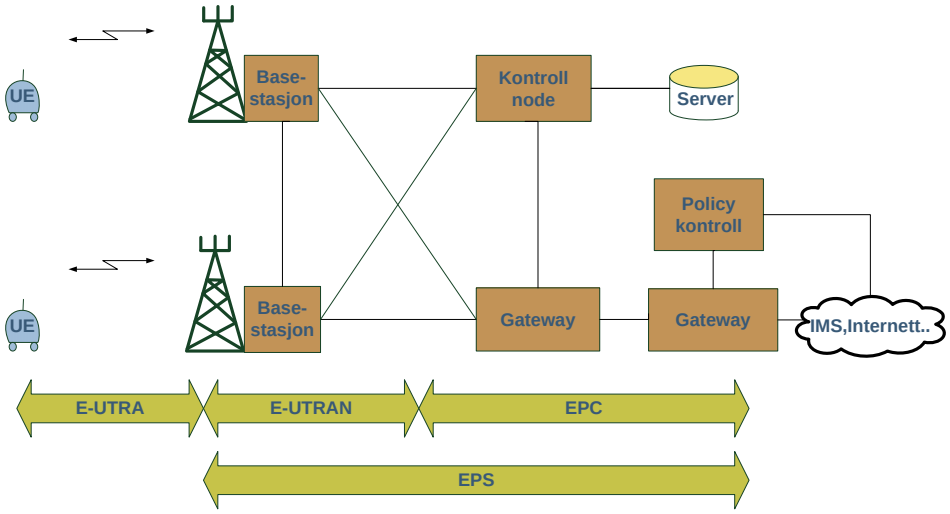
1.2 Rapportens oppbygging

I neste kapittel gis en kort introduksjon til LTE og EPC. De sentrale teknologiene på radioaksessiden; ”Orthogonal Frequency Division Multiplexing” (OFDM) og ”Multiple Input Multiple Output” (MIMO) blir beskrevet i kapittel 3. Kapittel 4 tar for seg hele nettverket, hvor mobilterminalen, radioaksess- og kjernenettverket inngår. Protokollstrukturen for LTE/EPC kommer i kapittel 5, med fokus på protokollene som går mellom mobilterminalen UE og basestasjonen eNB. Mobilitet og tjenesteegenskaper er beskrevet i henholdsvis kapittel 6 og kapittel 7. Sikkerhet er tema i kapittel 8. Kapittel 9 og 10 tar for seg henholdsvis tjenester og utbygging og utvikling av LTE. I kapittel 11 får vi en kort introduksjon til det som hittil er gjort innenfor utvikling av LTE-Advanced, som er en videreutvikling av LTE. Til slutt følger en oppsummering i kapittel 12.

2 Long Term Evolution (LTE)/Evolved Packet Core (EPC)

Navnet ”Long Term Evolution” (LTE) ble gitt til et prosjekt innenfor standardiseringsorganet 3GPP hvor hensikten var å forbedre UMTS-standarden for å møte fremtidige behov. Resultatet fra dette prosjektet var et nytt sett av standarder som definerte funksjonalitet og krav til et videreutviklet pakkebasert radioaksessnettverk og en ny radioaksess. Det nye radioaksessnettverket har fått navnet ”Evolved Universal Terrestrial Radio Access Network” (E-UTRAN), og den nye radioaksessen ”Evolved Universal Terrestrial Radio Access” (E-UTRA). LTE er imidlertid blitt værende som et navn på både E-UTRA og E-UTRAN. I parallell til og koordinert med LTE-prosjektet ble det opprettet et prosjekt som skulle ta for seg kjernenettverket.

Dette prosjektet fikk navnet ”System Architecture Evolution” (SAE) og skulle standardisere det nye ”Evolved Packet Core” (EPC). Kombinasjonen av E-UTRAN og EPC har fått navnet ”Evolved Packet System” (EPS), se figur 2.1 [2]. Rapporten bruker begge navnene.



Figur 2.1 EPS systemoversikt [2]

2.1 Introduksjon

LTE innfrir den langsiktige visjonen til 3GPP om et rent IP-basert ”Orthogonal Frequency Division Multiple Access” (OFDMA) bredbåndssystem, med høyere datahastigheter, forbedret spektraleffektivitet og redusert forsinkelse. I tillegg har fokus vært på forenkling av nettverkstrukturen, kostnadsreduksjon og fleksibilitet. Nettverksiden (EPC) har en flat IP-struktur som bidrar til redusert forsinkelse [2;3]. Sømløs mobilitet mellom LTE, GSM/EDGE og UMTS, og bedre integrasjon med andre åpne standarder slik som WiMAX og CDMA2000 er realisert. Høyere datahastigheter og lav forsinkelse vil åpne for flere avanserte tjenester som blant annet multimediatjenester og online spill. Spektraleffektivitet vil si hvor godt systemet utnytter frekvensbåndet, det vil si hvor mye systemet klarer å overføre av informasjon over den tilgjengelige båndbredden. Innholdet i kapittelet er hovedsakelig hentet fra [2-4].

Fleksibiliteten i LTE gjør det mulig for operatøren å bruke forskjellige frekvensbånd med forskjellige båndbredder, hvor systembåndbredden kan skaleres opp fra 1,4 MHz til maks 20 MHz. En operatør kan da bygge ut LTE selv om han ikke har 20 MHz båndbredde tilgjengelig, og kan øke båndbredden på systemet når operatøren får mer båndbredde [2]. LTE støtter både paret ”Frequency Division Duplexing” (FDD) og uparet ”Time Division Duplexing” (TDD) spektrumstildelinger. I FDD-varianten brukes forskjellige frekvenser på opp- og nedlink, mens med TDD-varianten brukes den samme frekvensen både i opp- og nedlink adskilt i tid. Rapporten tar for seg FDD-varianten fordi den antakelig vil bli mest utbredt.

2.2 LTE/EPC Systemkarakteristikk

Ved design av mobilkommunikasjonssystemstandarder er det alltid en avveiing mellom mer kompleksitet i mobilterminalen (effektbruk, prosesseringskraft, kostnad), nettverkskompleksitet (radiogrensesnitt, ressursforbruk, nettverkstopologi) og oppnåelig ytelse for systemet. Under følger noen av kravene som er blitt satt til det nye LTE/EPC systemet [2]:

- Maksimal teoretisk oppnåelig datarate på minst 100 Mb/s i nedlink og 50 Mb/s i opplink (antatt 20 MHz system båndbredde)
- Kontrollplanforsinkelse; tid for mobilterminalen å gå fra idle til aktiv tilstand. Kravet er at den skal være mindre enn 100 ms. Aktiv tilstand vil si at UE har en forbindelse med nettverket og kan sende og motta data.
- Brukerplanforsinkelse; krav til ”round trip time” fra mobil til basestasjon er 10 ms og ende til ende 25 ms.
- Optimalisert for lave kjøretøyhastigheter (0-15 km/t), støtter også høyere kjøretøyhastigheter (15-120 km/t) med høy ytelse. Mobiliteten skal bli opprettholdt mellom 120-350 km/t (opp til 500 km/t avhengig av frekvensbånd)
- Dataraten og mobiliteten som er nevnt over skal bli møtt ved celler med 5 km radius, med en viss degradering for celler på størrelse med 30 km. Det skal være mulig med cellestørrelser på opp til 100 km.
- E-UTRA skal kunne operere i forskjellige spektrumallokeringer med forskjellige frekvensbåndstørrelser; 1.4, 3, 5, 10, 15 og 20 MHz både i opplink og nedlink. Det skal være støtte for operasjon både i paret (FDD) og uparet (TDD) spektrum.
- E-UTRAN skal kunne operere i samme geografiske området og kunne samlokaliseres med ”GSM EDGE Radio Access Network” (GERAN)/ ”Universal Terrestrial Radio Access Network” (UTRAN) på nabofrekvens. E-UTRAN-mobilterminaler som også kan bruke GERAN- og UTRAN-nettene skal kunne ta handover til og fra GERAN/UTRAN. UTRAN er navn på UMTS-nettet med oppgraderinger, navnene brukes omhverandre.
- Arkitekturen i E-UTRAN skal være pakkebasert og samtidig støtte sanntidstale-trafikk
- Ønsker lav kompleksitet ved å minimalisere antall muligheter og redusere overflødige obligatoriske egenskaper

Det er kun mulig å oppnå maksimalt teoretisk hastighet eller bedre, under gode radioforhold og med en bruker i cella. Operatørene lover derfor ikke maksimal teoretisk hastighet, men legger seg på rundt 20 Mbit/s nedlink og 10 Mbit/s opplink.

3 Radioaksess

Dette kapittelet tar for seg sentrale teknologier på radiogrensesnittet; ”Orthogonal Frequency Division Multiplexing” (OFDM) og ”Multiple Input Multiple Output” (MIMO).

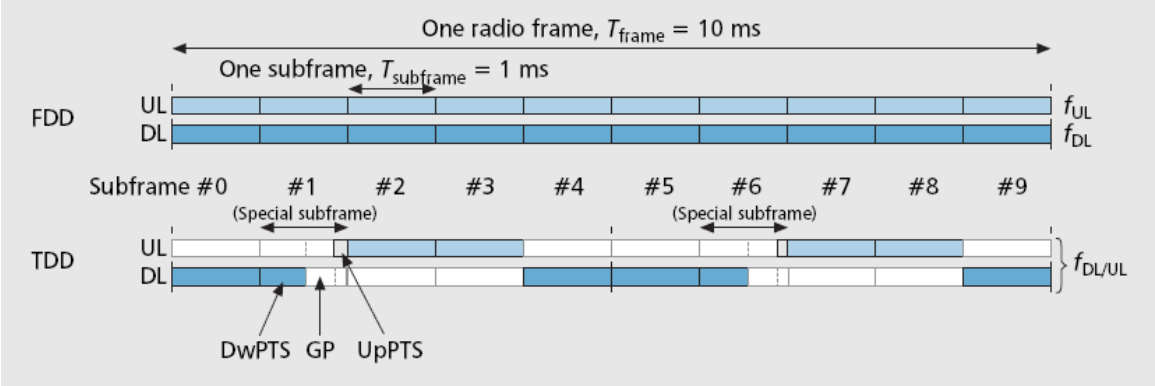
OFDM-teknologien ble først introdusert på Bell Lab i 1966. OFDM-implementeringen ble kosteffektiv da ”Discrete Fourier Transform” (DFT) ble tatt i bruk i 1971, som i 1981 ble

forbedret med ”Fast Fourier Transform” (FFT). Det første mobilkommunikasjonssystemet basert på OFDM-teknologi ble foreslått i 1985. Siden da har prosesseringskraften til moderne digitale signalprosessorer økt betraktelig, noe som har gjort OFDM-teknologien realiserbar i LTE.

Enkle flerantennesystemer har eksistert i over 50 år for å oppnå diversitet. Det som har muliggjort utviklingen av MIMO for mobilkommunikasjon i dag, er produksjonen av rimelige høyhastighets ”Digital Signal Processors” (DSPs) og betydningsfulle gjennombrudd i informasjonsteori det siste tiåret. DSP brukes for å implementere faseskiftere i basisbånd slik at dyre RF-faseskiftere unngås.

3.1 OFDM

Radioaksessen E-UTRA bruker ”Orthogonal Frequency Division Multiplexing” (OFDM) teknologi på nedlink. OFDM er en digital multicarrier modulasjonsmetode, som sprer brukerdataene som skal sendes over mange tettpakkede smalbåndede ortogonale subcarriers. Hver subcarrier har en båndbredde på 15 KHz. I LTE er signalet organisert inn i subrammer med 1 ms varighet. En subramme består av 12 eller 14 OFDM-symboler. 10 subrammer utgjør en radioramme, se figur 3.1 under. En bruker får tildelt en eller flere blokker med 12 ortogonale subcarriers over et tidsrom på 1 ms, såkalt ”Physical Resource Block” (PRB), se kapittel 3.2. OFDM-symbolet som sendes fra basestasjonen er en summasjon av alle subcarriers i den tilgjengelige båndbredden når etterspørselen er like stor som kapasiteten. OFDM-symbolet inneholder informasjon til flere brukere [2].



Figur 3.1 LTE-rammestruktur [5]

I OFDM vil en høy bitrate-datastrøm til mobilterminalen (UE) bli splittet i basestasjonen (eNB) til lav bitrate-datastrømmer ved hjelp av et stort nummer smalbåndet subcarriers. Hver subcarrier blir modulert med en konvensjonell modulasjonsmetode (for eksempel 16QAM) med lav bitrate. Dette fører til en økning av symbollengden til hver subcarrier. Økning av symbollengden og bruk av et guardinterval CP gjør at OFDM kan takle lange refleksjoner; ”Intersymbol Interference” (ISI). ISI er et generelt problem i mobilkommunikasjon, og robusthet mot ISI er en stor fordel og hovedgrunnen for at OFDM ble valgt for LTE-systemet. Se kapittel 3.4 for informasjon om ISI og CP. De mottatte parallelle datastrømmene (subcarriers) blir demultiplekset av mobilterminalen (UE) for å regenerere den originale høye bitrate-datastrømmen [2;3].

En ulempe med OFDM-teknologien er at et OFDM-signal har en varierende envelope og sender ut et høyt "Peak to Average Power Ratio" (PAPR). Det fører til en ineffektiv utnyttelse av effektforsterkere og dermed til høyt energiforbruk. Dette er ikke noe problem for basestasjonen, men blir et problem for batterikapasiteten i mobilterminalen. E-UTRA-systemet bruker derfor en variant av OFDM for opplinktransmisjon som reduserer PAPR og dermed forlenger batterilevetiden. Denne varianten av OFDM er kalt "Single Carrier Frequency Division Multiple Access" (SC-FDMA) og har single carrier egenskaper og beskrives senere [2;3].

OFDM-systemet, med mange svært smalbåndede kanaler, er veldig sensitivt for frekvensforskyvninger. Frekvensforskyvninger kan være et resultat av dårlig frekvenssynkronisering eller dopplerskift. Doppler fører til at fasen endrer seg i løpet av et symbol og jo lengre symbollengde vi har jo større fasefeil får vi i mottaker. Subcarriers vil ikke lenger være ortogonale og vi vil få "Inter-Carrier Interference" (ICI). Symbollengden i OFDM-systemet vil derfor være en avveiing mellom å motvirke ISI og doppler. Se kapittel om ortogonalitet (3.1.2), frekvenssynkroniseringsfeil (3.1.3) og doppler (3.1.4) for mer informasjon om frekvensforskyvningsproblematikk.

3.1.1 Parameterdimensjonering av OFDM/OFDMA-system

Visse nøkkelparametre bestemmer ytelsen til OFDM/OFDMA-systemet. Kompromisser må bli gjort ved definering av disse parametrene for å maksimere systemets spektraleffektivitet, og samtidig opprettholde robusthet mot propagasjonsforringelse. De viktigste propagasjonsegenskapene som må bli tatt hensyn til ved utforming av OFDM-systemet er den maksimale forsinkelse T_d (lengste refleks), og den maksimale dopplerfrekvensen $f_{dmax} = f \times (v_{max}/c)$, hvor v_{max} er maksimal kjøretøyshastighet, c er lyshastigheten og f er senterfrekvensen. Disse legger begrensning på valg av CP-lengden og avstand mellom subcarriers. CP må være lenger enn kanalimpulsresponsen for å sikre robusthet mot ISI. For å maksimalisere spektraleffektiviteten må OFDM-symbolperioden T_u være stor relativt til CP-lengden T_{CP}, men liten nok for å være sikker på at kanalen ikke varierer innenfor et OFDM-symbol.

$T_u = NT_s$ — T_u – symbolperioden, T_s – sampling perioden, N – data

$\Delta f = 1/T_u$ — Δf – subcarrier avstand

Valg av en stor T_u vil gi en mindre subcarrier avstand Δf, som har direkte innvirkning på systemets sensitivitet til dopplerskift og andre kilder for frekvensforskyvning.
Under følger tre viktige designkriterier [3]:

$T_{CP} \geq T_d$ - for å motvirke intersymbolinterferens

$f_{dmax}/\Delta f << 1$ - for å forhindre interkanalinterferens

$T_{CP} \times \Delta f << 1$ - for spektraleffektivitet

Et annet kriterium er hvor lang en OFDM-blokk ($T_u = NT_s$) kan være, før kanalen bør estimeres på nytt. Dette er gitt av samplingsteoremet;

$$T_u = NT_s < 1/(2\, f_{dmax})$$

LTE bruker en subcarrieravstand på $\Delta f = 15$ kHz og CP = 5,2 µs i opplink og nedlink. Subcarrieravstanden er et kompromiss mellom spektraleffektivitet og sensitivitet til frekvensforskyvning. $\Delta f = 15$ kHz er tilstrekkelig stor for å tolerere dopplerskift på grunn av høy mobilitet (350 km/t) og frekvensskift på grunn av implementeringsdefekter [3;4].

3.1.2 Ortogonalitet

I tradisjonelle FDM-systemer ble forskjellige brukere tildelt forskjellige frekvenser for transmisjon. Det var et guardbånd mellom disse frekvensene for å unngå at de interfererte på hverandre. Behovet for et guardbånd fører til en ineffektiv bruk av frekvenser.

I OFDM er frekvensene valgt ortogonale, det vil si at de ikke interferer med hverandre. Demodulatoren for en subcarrier ser ikke modulasjonen til de andre subcarriers, slik at det ikke blir krysstale mellom subcarriers, selv om frekvensspekteret deres overlapper noe. Dette fører til at vi kan pakke subcarriers mye tettere enn ved tradisjonell FDM, og dermed øke spektraleffektiviteten. For å sikre ortogonalitet må alle subcarriers ha samme frekvensavstand som den inverse av varigheten til OFDM-symbolet, også kalt den aktive symbolperioden hvor mottakeren demodulerer signalet. Denne frekvensavstanden er dimensjonert til 15kHz i E-UTRA. SC-FDMA som blir brukt for LTE-opplink er også designet for å være ortogonal i frekvensplanet mellom forskjellige UEer, slik at interferens innad i cella blir eliminert [3]. Tap av ortogonalitet fører til støy fra andre subcarriers, det gir bitfeil som til en viss grad kan rettes opp av feilkorrigerende kode. E-UTRA bruker turbokoding som feilkorrigerende kode. På grunn av ortogonalitet vil LTE-systemet være mest begrenset av likekanalsinterferens fra naboceller.

Hele spekteret til en ”Fast Fourier Transform” (FFT) kanal må være med for at ortogonaliteten skal være intakt. For kraftig filtrering med skarpe filterkanter enten i sender eller mottaker vil fjerne sidelober til noen subcarriers, og dermed ødelegge ortogonaliteten. For å unngå skarpe filterkanter må det settes av mer båndbredde enn båndbreddebehovet til hver enkelt kanal.

3.1.3 Frekvenssynkroniseringsfeil

Frekvenssynkroniseringsfeil fører til tap av ortogonalitet. Frekvenssynkroniseringsfeil kan oppstå som følge av små forskjeller i de lokale oscillatorene, som blir brukt til frekvensgenerering i sender og mottaker. Når det i mottakeren integreres over en gitt subcarrier for å gjenvinne signalet, vil en frekvensforskyvning mellom det innkomne signalet og signalet i mottakeren føre til en fasefeil som øker over integreringsperioden. I tillegg vil du få bidrag fra nærliggende subcarriers, da frekvensen i mottakeren og de innkomne frekvensene ikke lenger har en 15kHz frekvensavstand og derfor ikke lenger er ortogonale. Frekvenssynkroniseringsfeilen blir kompensert for ved at mottakeren ved hjelp av pilotsignalet i OFDM kontinuerlig følger frekvensforskyvningen, som da kan rettes opp i mottakeren.

3.1.4 Doppler

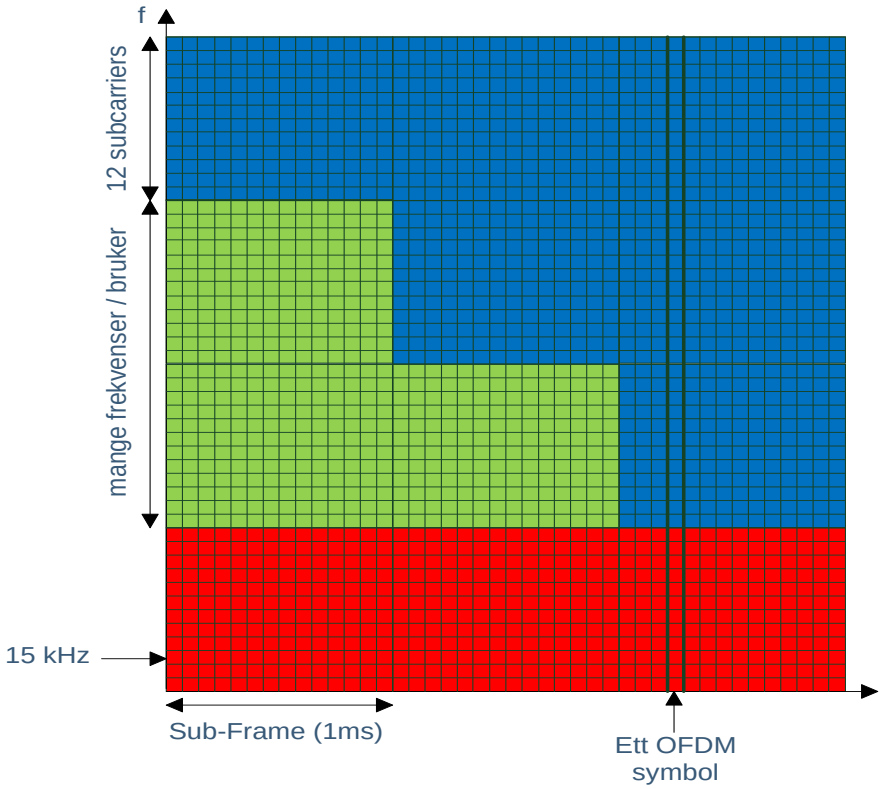
Dopplerskift er endring i frekvens for et signal som følge av den relative kjøretøyhastigheten mellom sender og mottaker. Når UE beveger seg, vil kjøretøyhastigheten til UE forårsake et skifte i frekvens for hver signalkomponent som går over ulike propagasjonsveier. Når signalkomponentene som går over ulike propagasjonsveier får forskjellig dopplerskift, fordi fasen endres med forskjellig hastighet, får vi dopplerspread.

Generelt kan vi si at LTE er designet for å tillate kjøretøyhastigheter opp til 350 km/t (høyhastighetstog), med degradering av ytelse (datahastighet) [3;4]. Doppler kan kompenseres for av kanalestimeringsalgoritmene. Nøyaktig estimering av ett enkelt dopplerskift er mulig, mens det er svært vanskelig å estimere dopplerspread nøyaktig. Dopplerproblemet øker med økende dopplerfrekvens, det vil si når den relative hastighet mellom sender og mottaker øker og ved økende subcarrier frekvens. Til tross for gode dopplerkompensasjonsmekanismer i mottageren, vil alle kommunikasjonssystemer ha redusert ytelse ved høye kjøretøyhastigheter på grunn av doppler. Dette skyldes at dopplerhastigheten ikke kan bestemmes helt nøyaktig for hver enkelt refleks, og dette problemet øker med økende kjøretøyhastighet. Mottageren vil regne ut en midlere dopplerhastighet som brukes til å estimere doppler på alle reflekser. Jo høyere dopplerfrekvens vi får desto større vil dopplerspredningen bli og dermed vil midlingen gi en større feil i estimering av doppler for hver refleks. Når mottakeren ikke kan kompensere for dopplereffekten vil vi få en degradering av ytelse i systemet. Dopplerskift:

$$f_d = f_c \times (v/c), f_d \text{ – dopplerfrekvens, } f_c \text{ – subcarrier frekvens}$$
$$v \text{ – kjøretøyhastighet, } c \text{ – lyshastigheten}$$

3.2 OFDMA/SC-FDMA: Subcarriers og multipleksing

E-UTRA bruker multipleksmetoden OFDMA i nedlink og ”Single Carrier Frequency Division Multiple Access” (SC-FDMA) i opplink. OFDMA er en utvidelse av OFDM for å realisere et flerbrukerkommunikasjonssystem. SC-FDMA er en variant av OFDM for å unngå for høy PAPR. OFDM og SC-FDMA har forskjellig signalgenerering og i tillegg vil OFDM-symbolet kunne inneholde informasjon til flere brukere, mens SC-FDMA-symbolet inneholder informasjon fra kun en bruker. På nedlink vil det da sendes ett OFDM-symbol og på opplink vil det sendes flere SC-FDMA-symbol for hver tidsenhet. Se kapittel 3.2.1 og 3.2.2 og figur 3.3 og 3.4 for mer informasjon om OFDM- og SC-FDMA-signalgenerering [3]. Alle brukere i en celle deler på de tilgjengelige subcarriers både i frekvens- og tidsdomene. I opplink blir brukerne tildelt sammenhengende fysiske ressursblokker (PRBs) for å muliggjøre singelcarrier-transmisjon, se figur 3.2. I nedlink kan brukerne få tildelt fysiske ressursblokker fra forskjellige deler av frekvensspekteret. Det er også mulig å bruke frekvenshopping for å redusere frekvensselektiv fading, eller kanalavhengig fordeling for å utnytte kanalforholdene optimalt [2].

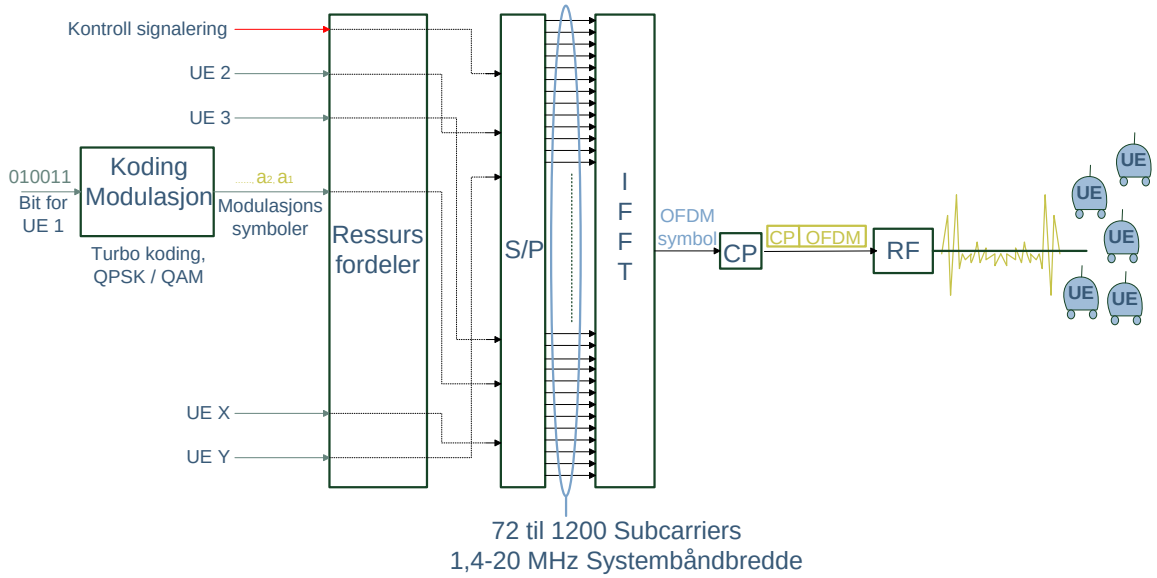


Figur 3.2 OFDMA eksempel med 3 brukere (rød, grønn og blå)[2]

3.2.1 OFDM-signalgenerering for nedlink

Nedenfor er det beskrevet en måte å generere et OFDM-signal for nedlink i E-UTRA [2], se også figur 3.3. For å gjøre systemet enda mer robust mot refleksjoner benyttes syklisk prefiks (CP). Dette er ikke obligatorisk og filtrering/utjevning av bærebølgen (RF prosessering) kan bli gjort på mange forskjellig måter.

- Koding og modulasjon: E-UTRA bruker turbokoding (for feilretting) og modulasjonsmetodene QPSK, 16QAM eller 64QAM.
- Seriell til Parallell: Like mange modulasjonssymboler som tildelte subcarriers er matet i parallell til ”Invers Fast Fourier Transform” (IFFT).
- IFFT: Hvert modulasjonssymbol modulerer en subcarrier, som fungerer som en kompleks vekt som bestemmer amplituden og fasen til subcarrier. De modulerte subcarriers blir summert og danner et OFDM-symbol. Hvis mange subcarriers har sine maksimum samtidig vil det føre til et stort maksimum i total amplitude til signalet (høy PAPR).
- Syklisk Prefiks (CP): Et guardbånd er laget ved at siste delen i OFDM-symbolet blir kopiert og føyet til i starten av det samme symbolet.
- RF prosessering: OFDM-symbolet modulerer bærebølgefrekvensen. På dette stadiet kan også flere pulsformingsteknikker og filtreringsteknikker bli benyttet.



Figur 3.3 OFDM for nedlink [2]

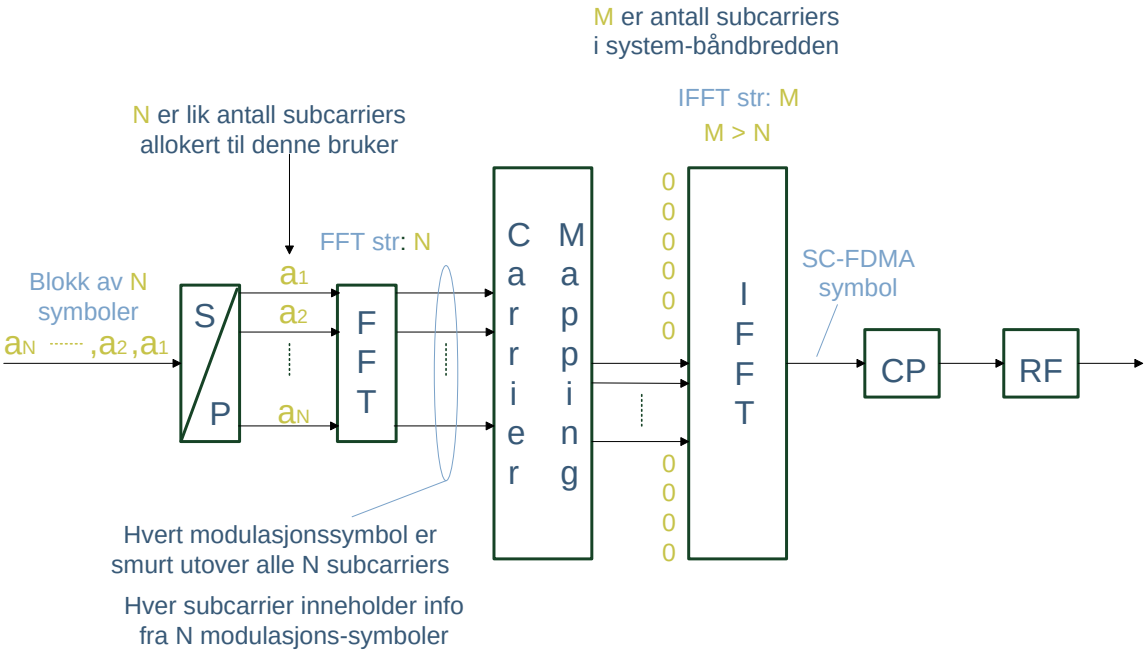
Mottakersiden går gjennom samme prosess bare i motsatt rekkefølge. IFFT-prosessen må bli invertert for å få tak i informasjonsinnholdet i de individuelle subcarriers. Dette gjøres med en "Fast Fourier Transform" (FFT).

3.2.2 SC-FDMA signalgenerering for opplink

Nedenfor følger en beskrivelse av SC-FDMA-signalgenerering for opplink [2], se også figur 3.4. Hvis vi sammenligner med generering av OFDM-symbolet er to nye steg innført i prosesseringskjeden; en FFT transform og en subcarrier-mapping (se figur 3.4). Den reelle forskjellen er at modulasjonssymbolene blir spredt utover alle subcarriers før summering av subcarriers, istedenfor 1-til-1 mapping som brukes i OFDM. Når en subcarrier blir modulert av alle modulasjonssymbolene samtidig, vil amplituden på subcarrier bli dempet og ved summasjon vil vi ikke få veldig høye PAPR. Resultatet ved å innføre FFT-trinnet er at det genererte signalet innehar singelcarrier-egenskaper.

- Koding og modulasjon: E-UTRA bruker turbokoding (for feilretting) og modulasjonsmetodene QPSK eller 64QAM.
- Seriell til parallell: En blokk av modulasjonssymboler er matet i parallell inn i FFT.
- FFT-prosessen sprer modulasjonssymbolene over alle subcarriers, det vil si at hvert enkelt modulasjonssymbol modulerer alle subcarriers.
- Mapping: Mater FFT-resultatet til et subset av IFFT-innganger, med alle andre innganger satt til null. FFT har størrelse N og IFFT har størrelse M, hvor M > N. M er lik størrelsen på båndbredden for systemet, mens N er lik størrelsen på tildelt subcarriers til bruker.
- IFFT: De modulerte subcarriers blir summert og resultatet blir et SC-FDMA-symbol.
- Et guardbånd (CP) er laget ved at siste delen i SC-FDMA-symbolet blir kopiert og føyet til i starten av symbolet.

RF prosessering: SC-FDMA-symbolet modulerer bærebølgefrekvensen. På dette stadiet kan også flere pulsformingsteknikker og filtreringsteknikker bli benyttet.



Figur 3.4 SC- FDMA for opplink [2]

3.3 Fading

Fading eller flerbaneinterferens er raske endringer i kvaliteten på radiokanalen som funksjon av tid, rom og frekvens. Flerbaneinterferens skyldes reflekser fra fysiske objekter langs radiosignalets propagasjonsvei, hvor refleksene vil føre til gangtidsforskjell. Hvis forskjellen i gangavstand mellom det direkte signalet og refleksjonen er en halv bølgelengde eller multippel av denne, vil signalene kunne utligne hverandre og vi får en sterk dempning. Dette fenomenet kalles ”fading” og er frekvensavhengig. Flerbanene vil også kunne føre til en forsterkning av signalet, som kan være gunstig for dekningen. LTE kan med OFDM-teknologien bruke kanalavhengig ressursfordeling både i tids- og frekvensdomenet for å utnytte slike raske kanalendringer istedenfor å undertrykke dem, og dermed oppnå mer effektiv utnyttelse av radioressursene. Hvis flerbaneinterferens allikevel skulle inntre i et OFDM-system, vil den opptre som flat fading over en subcarrier og det forsvinner bare noen symboler. Disse kan til en viss grad gjenvinnes ved å ha redundans og feilrettende koder.

Generelt kan vi si at en bredbåndsmottaker som håndterer flerbaner fungerer bedre enn en smalbåndsmottaker som ikke kan se forskjell på dem. Desto mer bredbåndet en mottaker er jo mer diversitet vil en oppnå ved forekomst av flerbaner, fordi hver refleks utgjør en nyttig signalkomponent. Ulempen er at mottakeren blir mer kompleks. Selv om hver bærebølge er smalbåndet i OFDM, er det mange bærebølger som gjør mottageren bredbåndet. En LTE-mottaker vil derimot ikke kunne utnytte refleksene i kanalen som beskrevet over, da OFDM opererer med mange smalbåndede subcarriers. Disse refleksene vil tilsvare frekvensavhengig

fading. Vi vil få en gevinst ved at informasjonen i OFDMA er spredt over mange subcarriers, som fader forskjellig, slik at bare få symboler forsvinner (frekvensdiversitet).

3.4 Intersymbol Interferens

Vi får "Intersymbol Interference" (ISI) når gangveisforskjellen mellom direkte og reflektert signal er blitt så stor at det nærmer seg eller er større enn et symbols varighet. Hvis symbol nr.*n-1* blir forsinket med tilnærmet et symbols varighet, vil det komme samtidig med symbol nr.*n* inn i mottakeren og lage støy for symbol nr. *n*. Med lengre symbollengde er LTE-systemet mindre utsatt for ISI, da den maksimale forsinkelsen av signalet som regel vil være mindre enn symbolvarigheten til OFDM-symbolet.

For å beskytte informasjonen ytterligere forlenger vi OFDM-symbolet med et guardintervall ("preamble"). Lav symbolrate gjør det økonomisk mulig å bruke et guardintervall, som vil si at hvert OFDM-symbol blir sendt over en lenger symbolperiode enn den aktive symbolperioden. Når vi legger til et guardintervall reduserer vi samtidig datakapasiteten tilsvarende lengden av guardintervallet. For å unngå å slå av og på sender er det flere måter å fylle guardintervallet på. Når syklisk prefiks (CP) brukes vil et forsinket ekko på grunn av flerbaner skape interferens bare i CP-delen av symbolet. Mottakeren vil se bort fra CP-delen av OFDM-symbolet og fjerne det før demodulering av informasjonen. Bruk av CP gir et periodisk signal, som gir pene fourierkoeffisienter slik at vi kan klare oss med en enklere utjevner. E-UTRA har definert en normal- og en utvidet lengde på CP, for å imøtekomme forskjellige krav for små eller store celler.

3.5 Kanalavhengig fordeling (channel-dependent scheduling)

Både opplink- og nedlinktransmisjon er kontrollert av fordeleren som er lokalisert i basestasjonen. Fordeleren er viktig og bestemmer i stor grad systemets ytelse på nedlink, spesielt i svært trafikkerte nettverk. Fordeleren bruker kanalinformasjon for dynamisk tildeling av subcarriers utfra kvaliteten på kanalen, slik at hver mobilterminal blir tildelt det mest optimale sett av subcarriers der det oppleves minst mulig interferens. Hver logiske kanal i LTE har et tilhørende "Quality of Service" (QoS) behov, som den kanalavhengige fordeleren må ta hensyn til ved fordeling av ressurser [3]. Fordeleren bestemmer for hvert 1 ms subframe hvilke brukere som kan sende, på hvilken frekvens de kan sende og med hvilken datarate. Den korte subframevarigheten på 1 ms tillater fordeleren å følge relativt raske kanalvariasjoner [5].

En viktig begrensning for basestasjonens fordelingsalgoritme er tilgjengeligheten til og nøyaktigheten av kanalkvalitetsinformasjonen for de aktive UE i cella. Denne kanalkvalitetsinformasjonen må være frekvensspesifikk for å støtte ressursfordeling av frekvenser. For å støtte fordeleren i sin avgjørelse om fordeling av subcarriers på nedlink, blir den momentane kanalkvaliteten ved mobilterminalen beregnet og "Channel Quality Indicator" (CQI) blir sendt tilbake til basestasjonen, helst så ofte som hver subframe. Dette gjøres blant annet ved hjelp av et cellespesifikt referansesignal som blir sendt på nedlinken. CQI er en indikasjon på dataraten som kan bli støttet av kanalen, tatt i betraktning "Signal-to-Interference plus Noise Ratio" (SINR) og egenskapene til UE sin mottaker. I opplink vil eNB beregne kanalkvaliteten ut

fra et ”sounding” referansesignal eller andre signaler som er sendt av mobilterminalene. Kvaliteten på det mottatte signalet ved basestasjonen blir brukt som grunnlag for kanalavhengig opplinkfordeling.

I tillegg til informasjon om kanalen trenger fordeleren også informasjon om databufferstatus både på opp- og nedlink for å kunne imøtekomme QoS-kravene [3;5]. Basestasjonen tilpasser dataraten på informasjonen som skal sendes for hver bruker over radiolinken dynamisk, for å matche den gjeldende radiokanalkapasiteten. Basestasjonen velger da forskjellige modulasjonsskjemaer (QPSK, 16-QAM og 64QAM) og kanalkoderater etter input fra prediksjon av kanalstatus både på opp- og nedlink (”sounding” referansesignal og CQI). Den optimale kombinasjonen av modulasjonsskjemaer og koderater avhenger blant annet av brukers QoS-behov og overføringskapasitet i cella [3].

Kanalavhengig fordeling kan være vanskelig å få til å fungere godt i praksis på grunn av den raskt skiftende kanalen, som gjør det vanskelig å få nøyaktig nok kanalinformasjon.

3.6 Ressursfordelingsstrategi

Basestasjonen i LTE-systemet er ansvarlig for å håndtere ressursfordeling for både opp- og nedlinkkanaler. Målet med ressursfordelingen er å gi så mange brukere som mulig den QoS som deres respektive tjenester behøver. I tillegg til å optimalisere ytelsen med hensyn på trafikkgjennomstrømning, spektraleffektivitet per bruker og spektraleffektivitet totalt. Til dette formålet brukes forskjellige ressursfordelingsalgoritmer som støtter forskjellige ressursfordelingsstrategier. Det er opp til hver operatør å velge hvilken fordelingsstrategi som skal benyttes til enhver tid. Ressursfordelingsstrategiene er begrenset av basestasjonens totale uteffekt på nedlinken og av interferens mellom celler på opplinken [3].

Fordeling etter tur er en fordelingsstrategi som kan bli brukt ved tildeling av ressurser til bruker. Det er en rettferdig fordeling av ressurser, men utnytter ikke kanalinformasjon fra mobilterminalene og maksimaliserer derfor ikke gjennomstrømningen. En annen fordelingsstrategi heter ”Maximum Rate Scheduling” og gir ressursene til de brukerne som har best signal-til-støy forhold [3]. Brukere som er nærmest basestasjonen vil som oftest ha best kanalforhold, og for å kjøre mest mulig trafikk i cella er det gunstig å gi ressurser til disse brukerne. Dette vil maksimere gjennomstrømningen i cella, men kan oppleves som urettferdig av brukere med dårligere signal-til-støyforhold i randsonen av cella. Sannsynlig vil operatørene velge en fordelingsalgoritme som balanserer total trafikkgjennomstrømming med rettferdig fordeling av ressurser. Det kan også være at det blir mulig å variere fordelingsstrategi adaptivt etter hvor stor last cella har.

3.7 Interferenshåndtering og effektjustering

Innholdet i dette kapittelet er hovedsakelig hentet fra [5], [4], [6], [3] og [7]. Siden LTE-systemet tåler mye interferens er det mulig med en frekvensgjenbruksfaktor lik 1. Det vil si at hele frekvensbåndet blir gjenbrukt i alle celler. Brukere i samme celle vil dele på antall subcarriers

som er tilgjengelig ved en gitt båndbredde. Da subcarriers i samme celle er ortogonale vil det ideelt sett ikke være interferens mellom transmisjon i samme celle, så sant vi ikke får intra-cell interferens på grunn av dopplerskift eller frekvenssynkroniseringsfeil. Brukere i forskjellige celler vil kunne få tildelt samme subcarriers samtidig og det vil derfor være fare for likekanalinterferens mellom cellene. Dette problemet berører mest brukere i utkanten av cella. Ytelsen til LTE-systemet med hensyn på spektrumseffektivitet og tilgjengelige hastigheter er dermed begrenset av interferens fra andre celler (”Inter-Cell Interference”). Det er derfor viktig i LTE å håndtere interferens mellom celler på en god måte. Ytelsen til WCDMA/HSPA er begrenset av interferens fra andre likekanalsbrukere i samme celle. ”High-Speed Packet Access” (HSPA) er en oppgradering av UMTS for å få raskere hastigheter, så med HSPA menes UMTS-nettet.

LTE tilbyr verktøy for dynamisk interferenskoordinering mellom celler. Interferensbegrensende teknikker som opplink power control og ”Inter-Cell Interference Coordination” (ICIC) blir benyttet. Disse vil tillate en effektiv avveining mellom ytelsen til mobilterminalene i randsonen og den gjennomsnittlige spektraleffektiviteten for hele cella. ICIC og opplink power control vil kunne tilføre betydelig gevinst til brukere i utkanten av cella med hensyn på blant annet datarate. Hvis alle mobilterminaler skulle sende med maksimal effekt i et nett med gjenbruksfaktor lik 1, ville mobilterminalene kunne generere betydelig interferens i nabocellene, som igjen ville begrense bitraten til mobilterminalene i utkanten av cellene og dermed den totale nettverkskapasiteten. Både opplink- og nedlinkstrategier for interferenskoordinering mellom celler vil ha nytte av informasjon om posisjonen til mobilterminalen i forhold til naboceller [3;5].

De standardiserte ICIC-metodene baserer seg først og fremst på deling av frekvenser mellom celler og justering av uteffekt. ICIC-metodene er kategorisert i reaktive og proaktive metoder. Reaktive metoder baserer seg på allerede utførte målinger, som blir brukt til å overvåke kvaliteten på kanalen. Hvis det blir oppdaget for høy interferens, vil egnede tiltak bli igangsatt for å redusere interferensen til et akseptabelt nivå. Tiltak for å redusere interferens mellom cellene kan være reduksjon av sendereffekt eller strategier for fordeling av pakker. Standardisert signalering for interferens- og ressursfordelingsinformasjon går på X2-grensesnittet mellom basestasjonene. Med proaktive metoder vil en prøve å unngå i forkant at interferens oppstår. En eNB vil informere nabo eNBer hvordan den planlegger å fordele frekvensressurser til brukerne sine i fremtiden, via X2-grensesnittet, slik at nabo eNBer kan ta hensyn til denne informasjonen ved egen ressursfordeling [4].

3.7.1 Interferenskoordinasjon på nedlink

Interferenskoordinering mellom celler (ICIC) på nedlink ved gjenbruk lik 1 forutsetter restriksjoner av effekt i visse deler av frekvensspekteret. Dynamisk interferenskoordinering på nedlink, som er en proaktiv ICIC-metode, støttes av indikatoren ”Relative Narrowband Transmit Power” (RNTP). Indikatoren RNTP blir sendt fra eNB til nabo eNBer via X2-grensesnittet. RNTP indikerer den maksimale forventede sendereffekt per ”Physical Resource Block” (PRB) på nedlink i eNBen. RNTP gjør det mulig for nabo eNBer å ta med i beregningen forventet interferens i hver PRB når de fordeler frekvensressurser på nedlink til UE i egen celle. Hva eNB velger å gjøre hvis den skulle motta indikasjon om høy sendereffekt i en PRB i nabocella er ikke

standardisert, men sannsynlig vil den la være å tildele slike PRBer til UEer i randsonen. Da RNTP vil gi nabo eNBer informasjon om hvilke PRBer en celle planlegger å bruke mest effekt i, vil det åpne for at forskjellige effektmønstre kan bli brukt i nabocellene for å bedre den samlede ”Signal-to-Interference plus Noise Ratio” (SINR) [3-5].

3.7.2 Interferenskoordinasjon på opplink

For å støtte interferenskoordinering mellom celler (ICIC) på opplinken definerer LTE to indikatorer som blir utvekslet mellom basestasjonene over X2-grensesnittet; ”High-Interference Indicator” (HII) og ” Overload Indicator” (OI). HII er en proaktiv indikator som gir informasjon til naboceller om hvilken del av opplinkfrekvensbåndet som cella vil fordele til mobilterminaler i randsonen av cella. Forskjellige HII-meldinger kan bli sendt fra serving cell til forskjellige naboceller. For å unngå interferens fra cella som sendte HII-meldingen, kan nabocellene la være å bruke den samme delen av opplinkfrekvensbåndet på sine mobilterminaler i randsonen [3-5].

Nabocella kan isteden bruke de interferensutsatte frekvensene til mobilterminaler i sentrum av cella som behøver mindre sendereffekt og som da vil støye mindre. Mobilterminaler i sentrum av cella er også mindre utsatt for interferens fra naboceller. Alternativt kan nabocella la være å bruke frekvensene forutsatt at cella ikke går med full kapasitet. HII gir størst gevinst for tilfeller med lastfordeling hvor mobilterminalene bare sender på et subset av tilgjengelige PRBer i cella. OI er en reaktiv indikator som gir informasjon om interferensnivået på opplinkfrekvensressurser (PRBer) til cella som sender indikatoren. Basestasjonen til cella måler interferens pluss støy på PRBene, og lager OI-indikatorer basert på disse målingene. OI-indikatoren kan være av verdi lav, medium eller høy. Celler som mottar OI kan da redusere interferensen ved å bruke andre opplinkfrekvenser på mobilterminaler i randsonen mot cella som har interferensproblemer [3-5].

3.7.3 Power control på opplink

Power control vil generelt si å regulere uteffekt adaptivt på sendere, basestasjoner på nedlink og mobilterminaler på opplink, med mål om å forbedre systemkapasitet, datarate og redusere effektforbruket. I UMTS blir effekten endret i intervaller på 1 s, mens intervallene er lengre i LTE (ca. 3 s). Grunnen til de korte intervallene i UMTS er for å kunne ta hensyn til raske endringer av kanalforhold på grunn av likekanalinterferens i cella. I LTE er det bare power control i opplink.

I et mobilsystem vil opplink power control ha en viktig rolle ved å balansere behovet for tilstrekkelig sendereffekt per bit for å oppnå nødvendig ”Ouality-of-Service”, mot å minimalisere interferens for andre brukere av systemet. I tillegg vil opplink power control ønske å maksimalisere batterilevetiden til mobilterminalen. For å oppnå denne balansen må opplink power control tilpasses radiokanalens karakteristikker, som ”pathloss”, ”shadowing” og ”fast fading”, i tillegg til å overvinne interferens fra andre brukere i egen celle og naboceller. Da LTE er ortogonal i design vil interferens fra mobilterminaler i naboceller være dominerende [3].

LTE bruker ”Fractional Power Control” i opplink, som tillater høyere ”Signal-to- Interference plus Noise Ratio” (SINR) for mobilterminaler som har liten pathloss, det vil si mobilterminaler som er nær sin egen basestasjon. Mobilterminalenes SINR er satt slik at den øker når pathloss

minker, det vil si når den kommer nærmere egen basestasjon. Høyere sendereffekt på mobilterminaler som forårsaker lite interferens på naboceller, gir økt bit/s og dermed kan høyere spektraleffektivitet oppnås. Økningen av SINR er kontrollert med en faktor α av nettverket. Nettverket vil ved hjelp av faktoren α gjøre en avveining mellom cellas totalkapasitet i opplink og opplinkbithastigheter i randsonen av cella. Jo mer effekten blir skrudd ned på opplink, jo mindre interferens i randsonen og dermed høyere bithastighet for mobilterminaler i randsonen. Samtidig vil det bli oversendt mindre bit/s på de resterende mobilterminalene nær basestasjonen da effekten også til en viss grad blir skrudd ned her. Simuleringsresultater indikerer at den fraksjonelle kompenseringen kan forbedre bitraten for mobilterminaler i celleranden med opp til 20 % for en gitt gjennomsnittsbitrate [6].

3.8 Multiple antenne systemer

MIMO går ut på å ha flere signalveier mellom basestasjon og mobil, som kan brukes til enten å overføre mer informasjon eller håndtere flere brukere i cella. For å oppnå flere signalveier på nedlink, må vi ha minst to senderantenner på basestasjonen og to mottakerantenner i mobilterminalen. Foreløpig kreves det litt for komplisert prosessering i mobilterminalen til å generere flere signalveier i opplink, men det forskes på det i LTE-Advanced. MIMO-teknikken vil bli brukt i LTE-nettet og høyst sannsynlig for å forbedre kapasitet eller kvalitet i UMTS-nettet.

Et av de viktigste bidragene for å øke datarater i LTE er introduksjon av MIMO. Et trådløst kommunikasjonssystem med en senderantenne (TX) og en mottagerantenne (RX) sies å operere i ”Single Input Single Output” (SISO) mode. For å øke enten overføringshastigheten eller påliteligheten til systemet kan en legge til flere antenner. Systemer med multiple TX/RX blir delt opp i disse termene ”Single Input Multiple Output” (SIMO), ”Multiple Input Single Output” (MISO) eller ”Multiple Input Multiple Output” (MIMO) [2].

3.8.1 SIMO og MISO

I et SIMO-system har en sender en antenne og mottaker har to eller flere fysisk separerte antenner. Den fysiske separasjonen har en direkte relasjon til bølgelengden til signalet, som igjen muliggjør mottakerdiversitet (RX-diversitet). Med for eksempel to mottakerantenner får mottakeren inn to versjoner av det samme signalet. Mottakeren kan da enten velge det beste signalet fra en av antennene eller kombinere signalene fra begge antennene, med for eksempel ”Maximum Ratio Combining” (MRC). RX-diversitet med MRC blir brukt under vanskelige radioforhold med svakt direktesignal og mange refleksjoner [2].

I et MISO-system har sender to eller flere fysisk separerte antenner, og mottaker har en antenne. Dette muliggjør senderdiversitet (TX-diversitet). Senderen sender to like signaler til mottaker og håper at i hvert fall ett av signalene skal komme frem i god nok tilstand til pålitelig dekoding av signalet. ”Space-Time Coding” (STC) er en måte å realisere TX-diversitet på. Da sendes de to like signalene adskilt både i rom og tid, i tillegg til at signalet som kommer sist i tid blir kodet [2].

RX-diversitet og TX-diversitet fører til en mer pålitelig kanal, men øker ikke direkte systemdataraten. Likevel vil en mer pålitelig datakanal trenge mindre uteffekt, som igjen fører til høyere systemkapasitet. Istedenfor å senke effekten kan en også velge å bruke en mindre robust kanalkoding, som gir høyere datarate.

3.8.2 MIMO

I et MIMO-system har både sender og mottaker to eller flere antenner. MIMO-teknikken kan brukes til å forbedre signal-til-støyforhold (diversitet), eller den kan fungere som en romlig multiplekser og bruke de ekstra signalveiene til å overføre mer informasjon. I begge tilfeller vil overføringskapasiteten i cella øke. Romlig diversitet gir økt signal-til-støyforhold (S/N), som øker overføringskapasiteten ved at en kan bruke mer avanserte modulasjonsteknikker. Økt S/N gjør også mobilsignalet mer robust mot flat fading, det vil si lik dempning på alle frekvenser samtidig. Det er mest aktuelt å bruke MIMO for diversitetsgevinst i randsonen av cella eller innendørs. I resten av cella vil MIMO høyst sannsynlig fungere som en romlig multiplekser [2].

De første LTE-terminalene vil sannsynlig ha minst 2 mottagerkanaler og en senderkanal, mens basestasjonen vil minst ha 2 mottakerkanaler og 2 senderkanaler. Kanalene må være ukorrelerte, noe som igjen påvirker kravet til avstand mellom antennene. Praktisk kapasitetsgevinst i urbane områder vil ligge rundt 20-50 % for 2X2 MIMO. For 4X4 MIMO, det vil si 4 TX- og 4 RX-antenner, kan vi teoretisk få fire ganger så høy overføringshastighet. Prisen blir økt kompleksitet.

For å spre brukerdata over senderantennene brukes matriseligninger, som utnytter kanalens forskjellige egenskaper. Signalene blir definert i 3 dimensjoner; tid, frekvens og rom. På mottakersiden må de forskjellige signalene fra hver antenne bli identifisert og dekodet separat før de blir satt sammen igjen. Denne matematiske teknikken gjør det mulig å separere forskjellige signalveier over radiogrensesnittet. Dette gjør det mulig for et MIMO-system å sende multiple signaler samtidig med samme frekvens [2].

3.8.2.1 Antenneseparasjon

For god MIMO-operasjon er det ønskelig at kanalene er ukorrelerte. Avstanden mellom antennene påvirker graden av korrelasjon. Tilstrekkelig avstand mellom antenner for å få ukorrelerte kanaler, avhenger av hvilket frekvensbånd vi opererer i. Dette kan bli et problem i praksis for små terminaler som opererer i 700 MHz frekvensbåndet. Små terminaler, som smarttelefoner, har en størrelse som bare tillater noen få centimeters separasjon mellom de to antennene. Ved lave frekvenser vil denne avstanden mellom antennene resultere i høy korrelasjon mellom signalene mottatt ved hver antenne, som igjen vil minske diversitetsgevinsten. Små terminaler vil også på disse lave frekvensene få problemer med at hånden eller hodet vil påvirke antennas strålingsdiagram, som også vil føre til dårligere diversitetsgevinst. Større innretninger som bærbar PC og mini PCer vil ha stor nok avstand mellom antennene, slik at MIMO-diversitet blir oppnådd selv ved lave frekvenser. I høyere frekvensbånd vil avstanden mellom antennene på smarttelefoner være tilstrekkelig for å garantere god MIMO-operasjon [4].

3.9 MIMO teknikker

MIMO-teknikken ”romlig multipleksing” (SM) øker dataoverføringshastigheten, mens ”Space-Time Coding” (STC) vil gi økt diversitetsgevinst. SU-MIMO og MU-MIMO begrepene viser til om det er informasjonen til henholdsvis en eller flere brukere som går over radiogrensesnittet. SU-MIMO kan brukes i kombinasjon med SM eller STC, mens MU-MIMO bruker SM. Informasjon om MIMO-teknikker er hentet fra [2].

3.9.1 Romlig multipleksing (SM)

”Spatial Multiplexing” (SM) øker spektraleffektiviteten ved å bruke dataprosesseringsalgoritmer for å utnytte flerveispropagasjonen på kommunikasjonslinken til MIMO-systemet. Individuelle datastrømmer, som bruker samme tid-frekvens ressurs, blir sendt over forskjellige senderantenner. Mottakeren kan separere de forskjellige datastrømmene ved å bruke kjent kanalinformasjon om hver propagasjonsvei. De forskjellige datastrømmene av en SM-overføring må, for å unngå alvorlig interferens, være ortogonale i forhold til hverandre. For å oppnå ortogonalitet blir de sendte signalstrømmene multiplisert med en lineær forhåndsutfylt matrise (linear precoding matrix). Romlig multipleksing oppnår høyere datarater ved å gjenbruke den samme frekvensressursen over multiple romlige signalveier. Med for eksempel to sender- og mottakerantenner kan vi sende to separate datastrømmer på 5 Mb/s og få i teorien en resulterende datahastighet på 10 Mb/s. Antall mottakerantenner må være likt antall ønskede separate datastrømmer.

3.9.2 Space-Time Coding (STC)

STC-teknikken gir diversitetsgevinst ved å sende to like signaler adskilt både i rom og tid, hvor det siste signalet blir kodet. Flere antenner både på sender- og mottakersiden gir ytterligere uavhengige signalveier, som igjen øker oppnåelig maksimal diversitetsgevinst. Noen MIMO-systemer tillater dynamisk svitsjing mellom de to metodene SM og STC.

3.9.3 SU-MIMO og MU-MIMO

SU-MIMO er singelbruker MIMO. Alle datastrømmene i SU-MIMO bærer data til og fra samme bruker. Når SU-MIMO blir brukt sammen med STC øker kanalkvaliteten til en enkelt bruker. SU-MIMO i kombinasjon med romlig multipleksing øker datahastigheten til en enkelt bruker. Mottakeren må kunne separere en antennestrøm fra den andre for å kunne utføre effektiv kombinering. I SU-MIMO gjøres dette med et ”Code Division Multiplexing” (CDM) system.

MU-MIMO er multibruker MIMO. Data til forskjellige brukere blir multiplekset inn på en enkel tid-frekvens ressurs. Med for eksempel 2x2 antenne MU-MIMO konfigurasjon, kan to mobilterminaler sende og motta sine datastrømmer samtidig ved å bruke den samme fysiske ressursen. Det vil si at de to mobilterminalene sender på samme frekvens samtidig. Ved bruk av MU-MIMO økes kapasiteten i cella og operatøren kan betjene flere kunder uten å endre systembåndbredden. I MU-MIMO markerer mobilterminalen signalet det sender til basestasjonen med et referansesignal, slik at basestasjonen vet hvem som har sendt signalet. Både bruken av et

referansesignal og senderspesifikke koder (som i SU-MIMO) muliggjør nøyaktig beregning av overføringskanalen, noe som er viktig for MIMO-systemer.

3.9.4 MIMO for E-UTRA (LTE)

E-UTRA støtter opp om alle MIMO-teknikkene som er nevnt over; SM, STC, SU-MIMO, MU-MIMO. Den forventede minimumskonfigurasjonen vil bli to senderantenner på basestasjonen og to mottakerantenner på mobilen.

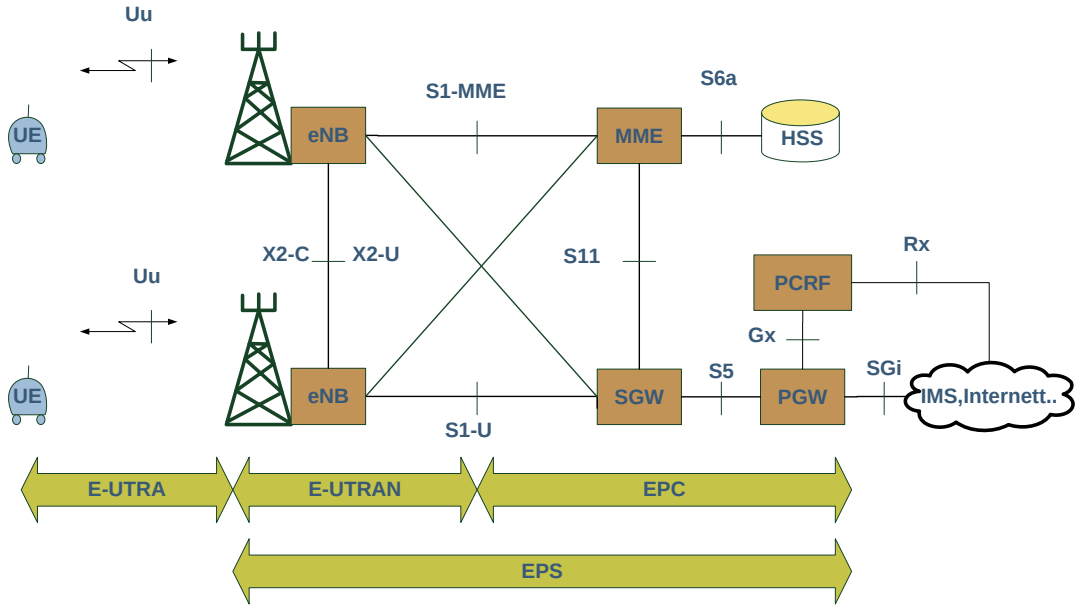
Det er forventet en fortsatt stor utvikling av MIMO på algoritmefronten. For å gjøre implementering av eventuelle nyutviklinger lettere er MIMO ikke spesifisert til den minste detalj i spesifikasjonene av E-UTRA. LTE-standarden tillater svitsjing mellom SU-MIMO og MU-MIMO modus, med mobilen som utgangspunkt. Både SU- og MU-MIMO i LTE bruker kodebøker med forhåndsutfylte matriser som er kjent både av eNB og UE. UE rapporterer hvilken matrise den ønsker å bruke til eNB, men er ikke sikret at eNB vil bruke den. Derfor må eNB sende informasjon om den valgte matrisen som skal brukes til UE.

Hvilken MIMO-modus som kan brukes av UE er avhengig av antall mottakerantenner hos UE. Ved lave datahastigheter gir det lavere feilrate å bruke en singel datastrøm med romlig diversitet til overføring, fremfor å bruke romlig multipleksing. Derfor vil LTE bruke singel datastrømoverføring for lave datarater og romlig multipleksing for høyere datarater. Kryssningspunktet hvor det blir mer effektivt å bruke romlig multipleksing istedenfor romlig diversitet avhenger av mange faktorer. Antall mottakerantenner hos UE vil være en faktor og avstand mellom sender og mottaker en annen. Generelt vil romlig multipleksing (SM) være mest effektiv når avstanden mellom sender og mottaker er relativt liten, når feltstyrken er relativt høy.

Det er knyttet store forventninger til MIMO på grunn av mulighetene til praktisk implementering og lovende teoretiske resultater. Allikevel er det hittil ikke vært mulig å se at forventningene er innfridd i praktiske systemer, siden bare konvensjonelle diversitetsgevinster er demonstrert. Dette skyldes at det kreves svært nøyaktig kanalestimering og rask utveksling av denne informasjonen mellom mottager og sender for å høste gevinstene. Implementeringen er enda ikke demonstrert.

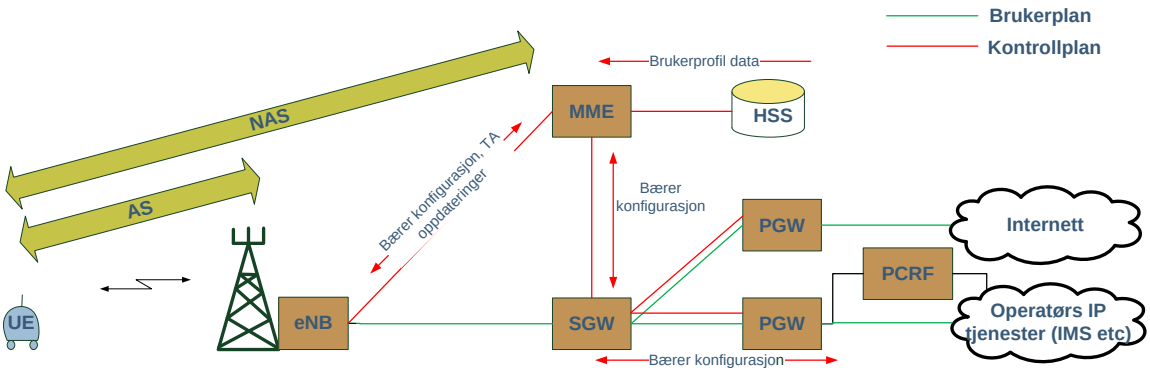
4 Nettverk

Dette kapittelet tar for seg de forskjellige nodene i ”Evolved Packet System” (EPS), som består av radioaksessnettverk (E-UTRAN) og kjernenettverk (EPC), se figur 4.1, og ansvaret nodene har i forbindelse med flyt av kontrollsignalering og brukerdata. Innholdet i kapittelet er i hovedsak hentet fra [4], [3] og [2]. I tillegg beskriver kapittelet også hva som må til for å sende IP-pakker over nettet med et eksempel på en oppkobling initiert av UE. UE, E-UTRAN og EPC representerer til sammen ”Internet Protocol (IP) Connectivity Layer”, og er optimalisert for å fremskaffe IP-tilkobling.



Figur 4.1 Nettverkstruktur i Evolved Packet System (EPS) [2]

I arkitekturen snakker vi om ett kontrollplan (CP) og ett brukerplan (UP), hvor henholdsvis kontrollsignalering og brukerdata flyter, se figur 4.2. Brukerplanet består av brukerdata (IP-trafikk) som oppstår eller ender hos bruker. Kontrollplanet består av kontrollsignalering enten for en brukersesjon eller uavhengig av noen bestemt bruker. Brukerdata flyter mellom UE, eNB, S-GW og P-GW. I tillegg vil det også kunne gå brukerdata direkte mellom eNBer ved handover (X2-U). Kontrollsignalering flyter mellom UE, eNB og MME, og i tillegg vil det kunne gå kontrollsignalering mellom MME/S-GW og P-GW/S-GW og mellom eNBer (X2-C). Forbindelsen mellom UE og eNB blir kalt ”Access Stratum” (AS) og den logiske forbindelsen mellom UE og MME blir kalt ”Non Access Stratum” (NAS), se figur 4.2.



Figur 4.2 AS, NAS og flyt av kontrollsignalering og brukerplan data [2]

IP Multimedia Subsystem” (IMS), se Figur 4.2, er en kjernenettverksarkitektur som gjør det mulig for operatører å tilby brukere IP-baserte multimediatjenester, som for eksempel VoIP. IMS er uavhengig av aksessteknologi og ligger utenfor selve EPS-systemet [4;8]

4.1 Mobilterminalen-UE

UE er terminalen som sluttbruker kommuniserer med. UE kan enten være en håndholdt innretning (smarttelefon), en USB dongel eller datakort innebygd i en PC. UE inneholder ”Universal Subscriber Identity Module” (USIM), som er plassert i et demonterbart smartkort ”Universal Integrated Circuit Card” (UICC). USIM tar hånd om autentisering og utregning av noen sikkerhetsnøkler, mens resten av sikkerhetsnøklene utledes i UE, se kapittel 8.4 og 8.5. UE signalerer med nettverket for å sette opp, holde ved like eller fjerne forbindelsen som sluttbruker trenger for å kommunisere. Dette omfatter ”mobility management” funksjoner som blant annet handover og rapportering av terminalens posisjon, noe UE gjør etter instruksjon fra nettverket.

4.2 Radioaksessnettverk-E-UTRAN

Radioaksessnettverket (E-UTRAN) består av et nettverk av basestasjonsnoder (eNBer), som tilsvarer UMTS sin NodeB (NB) og ”Radio Network Controller” (RNC). Ved at E-UTRAN integrerer radiokontrollfunksjonen i eNB muliggjør radioaksessnettverket tettere interaksjon mellom forskjellige protokollag, som reduserer forsinkelse og forbedrer yteevnen. E-UTRAN-arkitekturen er flat. Protokollene over radiogrensesnittet mellom eNB og UE heter ”Access Stratum” (AS) protokoller, se kapittel 5.

E-UTRAN kan ses på som et maskenett av eNBer koblet sammen gjennom et X2-grensesnitt, for blant annet å unngå tap av data ved handover, se figur 4.1. Det er basestasjoner, med sannsynlighet for handover, som blir koblet sammen via X2-grensesnittet. E-UTRAN har i tillegg to grensesnitt mot kjernenettverket EPC; S1-MME-grensesnittet mot MME-noden og S1-U-grensesnittet mot S-GW-noden, se figur 4.1.

E-UTRAN er ansvarlig for alle radiorelaterte funksjoner, deriblant radioressursforvaltning. Radioressursforvaltning er funksjoner relatert til radiobærerne som radiobærerkontroll, tilgangskontroll og mobilitetskontroll. En viktig del av radioressursforvaltning er basestasjonens fordeling og dynamisk allokering av ressurser til UE både i opplink og nedlink. Hvor basestasjonen baserer seg på informasjon om nødvendig ”Quality of Service” (QoS) og konstant overvåking av ressurssituasjonen [4]. Kontrollsignaleringen som går mellom eNB og UE over radiogrensesnittet heter ”Radio Resource Control” (RRC), se kapittel 5.3 for mer informasjon.

Innenfor dekningsområdet vil eNB betjene flere UE, hvor hver UE er knyttet opp mot bare en eNB. En eNB kan bli betjent av flere MME/S-GWer, slik at UEer tilhørende en eNB kan bli delt mellom flere kontrollnoder. Dette muliggjør lastfordeling og eliminerer ”single point of failure” for MME/S-GW nodene. Et sett av MME/S-GW noder, som betjener et felles område med eNBer, kalles en MME/S-GW pool. Området som dekkes kalles ett poolområde. En UE vil bli betjent av bare en MME/S-GW om gangen innenfor dekningsområdet til basestasjonen, og UE kan først endre MME/S-GW ved handover til en ny eNB. UE vil være tilknyttet en bestemt MME for all dens kommunikasjon så lenge den befinner seg innenfor poolområde [3].

4.3 EPC-kjernenettverk

”Evolved Packet Core” (EPC) er et rent pakkesvitsjet IP-basert kjernenettverk som består av tre hovednoder; ”Mobility Management Entity” (MME), ”Serving Gateway” (S-GW) og ”Packet Data Network Gateway” (P-GW). EPC har flat IP-struktur som bidrar til redusert forsinkelse.

4.3.1 Mobility Management Entity (MME)

”Mobility Management Entity” (MME) er hovedkontrollnoden i EPC og vil typisk være en server plassert i en sikker lokasjon i operatørens egne lokaler. MME eksisterer utelukkende i kontrollplanet (CP), det vil si at MME sender og mottar kun kontrollsignalering. Hovedfunksjonene som MME tar ansvar for er funksjoner relatert til registrering av UE i nettverket, og funksjoner relatert til forvaltning av EPS-bærer. Hver MME vil bli konfigurert til å kontrollere et sett av S-GWer og eNBer. Både S-GWene og eNBene kan også være tilknyttet andre MMEer. MME er koblet til eNB via S1-MME-grensesnittet og til S-GW via S11-grensesnittet. MME har også en direkte logisk kontrollplanforbindelse til UE, som blir kalt ”Non Access Stratum” (NAS), se figur 4.2. Forbindelsen blir brukt som den primære kontrollkanalen mellom UE og kjernenettverket, og kontrollsignaleringen mellom UE og MME heter NAS-signalering. For informasjon om ”Non Access Stratum” (NAS) protokollen se kapittel 5.1. Kontrollsignaleringen som går over S1-MME-grensesnittet er ”S1 Application Protocol” (S1AP) signalering. S1AP håndterer UEs kontroll- og dataforbindelse mellom E-UTRAN og EPC. MME har et grensesnitt mot SGSN, som blir brukt til signalering ved mobilitet mellom EPS og andre 3GPP-teknologier som UMTS og GPRS [2-4].

4.3.2 Serving Gateway (S-GW)

”Serving Gateway” (S-GW) er koblet til E-UTRAN og P-GW via henholdsvis S1-U- og S5-/S8-grensesnittene, og er en del av nettverksinfrastrukturen som sannsynlig er plassert i operatørens lokaler. S-GW sitt viktigste ansvar er ruting og fremsending av IP-pakker. S-GW bringer videre data mellom eNB og P-GW som skal til og fra UE. S-GW har en liten rolle med hensyn på kontrollfunksjoner, hvor den bare er ansvarlig for allokering av egne ressurser på anmodning fra MME, P-GW og ”Policy and Charging Rules Function” (PCRF). Kontrollfunksjonene handler om behovet for å sette opp, modifisere eller koble ned bærere for UE. Hvis anmodningen er mottatt fra P-GW eller PCRF, vil S-GW også videresende kommandoen til MME, slik at den kan kontrollere datatunnelen mellom S-GW og eNB. Likeledes vil S-GW videresende kontrollsignaleringen som kommer fra MME videre til P-GW eller PCRF [4].

Ved mobilitet mellom eNBer vil MME be S-GW om å koble om datatunnelen fra en eNB til en annen. S-GW er ruteren mellom ”Evolved Packet System” (EPS) og UMTS og GPRS. Når UE er i idle tilstand, vil ressursene i eNB være frigitt og datalinken vil være terminert i S-GW. Hvis S-GW mottar IP-pakker fra P-GW når UE er i idle tilstand vil S-GW bufre IP-pakkene og be MME om å initiere ”paging” av UE. ”Paging” vil føre til at UE kobler seg opp mot nettverket og når tunnelene er reetablert, vil de bufrede IP-pakkene bli sendt videre til UE. S-GW vil monitorere brukerdataene i tunnelene og kan også samle informasjon som er nødvendig for regnskapsføring og betaling. I tillegg har S-GW funksjonalitet som kan brukes til lovlig overvåking, det vil si

muligheten til å overlevere de monitorerte brukerdataene til myndighetene for videre inspeksjon. S-GW skal ha mulighet til å koble seg til enhver P-GW i hele nettverket, da P-GW ikke endres under mobilitet, mens S-GW kan bli omallokert når UE forflytter seg [4].

4.3.3 Packet Data Network Gateway (P-GW)

I likhet med S-GW vil ”Packet Data Network Gateway” (P-GW) være lokalisert i operatørens lokaler sentralt. P-GW er forbundet med S-GW via S5-grensesnitt, eller S8-grensesnittet hvis S-GW og P-GW er i forskjellige ”Public Land Mobile Networks” (PLMNs), og til eksterne pakkedatanettverk (eller IMS) via SGi-grensesnittet. P-GW eksisterer både i kontroll- og brukerplan, det vil si at det går både kontrollsignalering og brukerdata til og fra P-GW. Når en UE beveger seg fra en S-GW til en annen, vil P-GW få beskjed fra den nye S-GW om å koble bærerne fra den gamle S-GW til den nye S-GW. P-GW er ruteren mellom ”Evolved Packet System” (EPS) og eksterne pakkedatanettverk, som for eksempel CDMA2000 og WiMAX-nettverk [4].

P-GW er ansvarlig for å tilordne en IP-adresse til UE, som bruker den til å kommunisere med andre IP-hosts i eksterne nettverk, som for eksempel Internett. P-GW er også ansvarlig for håndheving av QoS og betalingsbelastning, i henhold til regler gitt av ”Policy and Charging Resource Function” (PCRF). P-GW inneholder en ”Policy Control Enforcement Function” (PCEF), som utfører signalutvelging og filtreringsfunksjoner bestemt av policyprofilen til UE eller den aktuelle tjenesten. I tillegg vil PCEF samle og rapportere relatert betalingsinformasjon. P-GW filtrerer nedlinks IP-pakker til bruker via forskjellige QoS-baserte bærere, og håndhever QoS for ”Guaranteed Bit Rate” (GBR) bærere [3;4].

4.3.4 Home Subscriber Server (HSS)

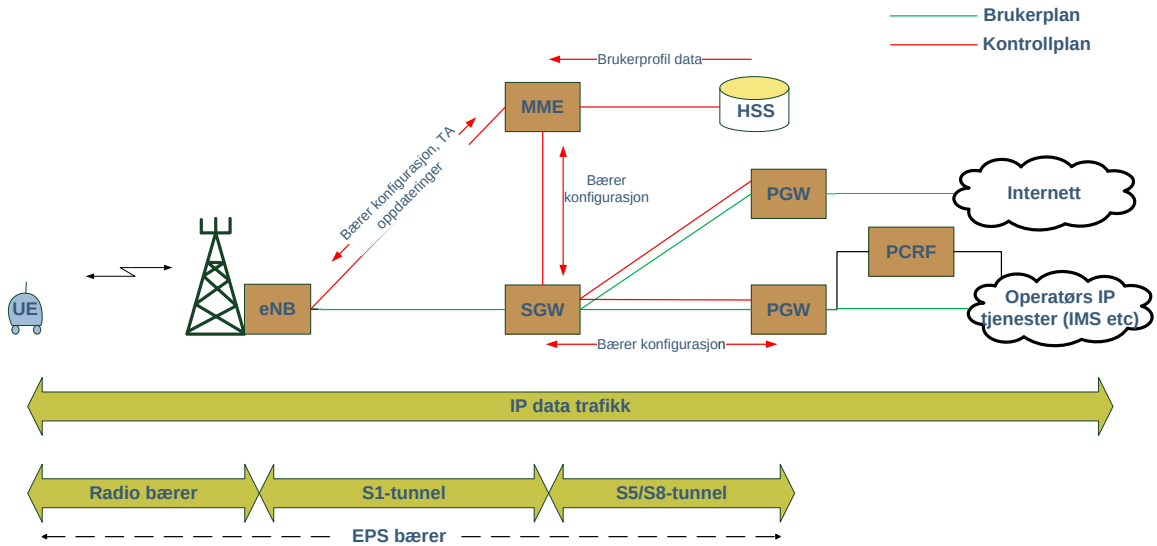
”Home Subscriber Server” (HSS) inneholder abonnentprofiler og sikkerhetsrelaterte parametre. Abonnentprofilen inneholder informasjon om hvilke tjenester som er tilgjengelig for bruker, tillatte ”Packet Data Network” (PDN) forbindelser og ”roaming” avtaler [4].

4.3.5 Policy and Charging Rules Function (PCRF)

”Policy and Charging Rules Function” (PCRF) node er ansvarlig for policykontrollavgjørelser, i tillegg til å kontrollere betalingsbelastningfunksjonalitetene i ”Policy Control Enforcement Function” (PCEF), som er en del av P-GW. PCRF gir, i overensstemmelse med brukers abonnementprofil, tillatelse til hvilken QoS (QoS klasseidentifikator og bitrate) PCEF kan bruke på en bestemt datastrøm. PCRF er en server som vanligvis er samlokalisert med andre kontrollnodeelementer i operatørens svitsjingsenter. PCRF håndterer også signalering mellom EPS og eksterne pakkedatanettverk, som for eksempel CDMA2000 og WiMAX-nettverk, og mot IMS når den blir brukt [3].

4.4 Dataoverføring

For å kunne sende IP-pakker i nettverket, det vil si at UE går over i aktiv tilstand, må det settes opp en EPS-bærer. En EPS-bærer består av en radiobærer, en S1-tunnel og en S5/S8-tunnel. Radiobæreren går over luftgrensesnittet fra UE til eNB, S1-tunnelen går fra eNB til S-GW og S5/S8-tunnelen går fra S-GW til P-GW, se fig 4.3. Når UE går tilbake i idle tilstand, vil radiobærer og S1-tunnelen frigjøres, mens S5/S8-tunnelen består. Det at S5/S8-tunnelen består fører til en raskere aktivering av UE ved senere behov [2].



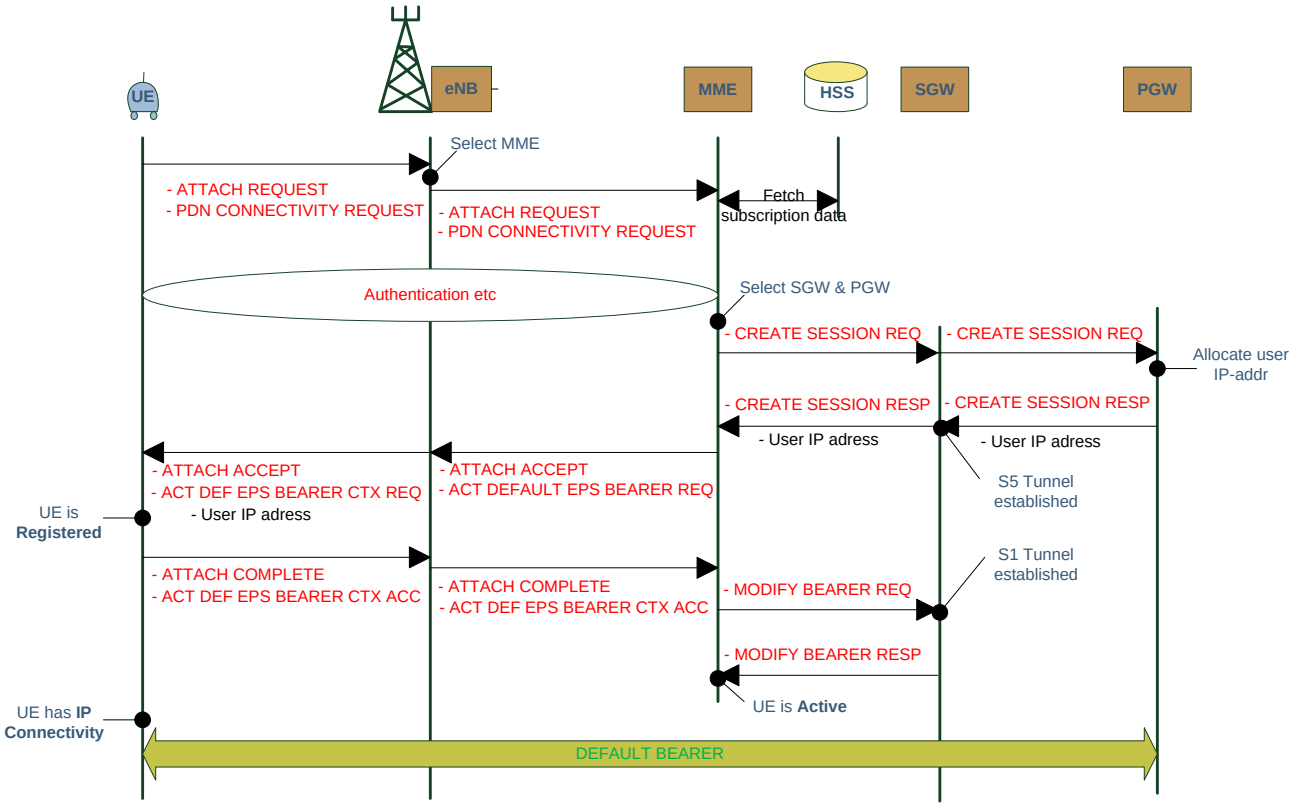
Figur 4.3 EPS-bærer - Radiobærer + S1-Tunell + S5/S8-Tunell [2]

Tunnelprinsippet går ut på at de opprinnelige IP-pakkene blir innkapslet i nye IP-pakker og sendt mellom P-GW og eNB for overføring til UE. En 3GPP-spesifikk ”tunneling” protokoll, kalt ”GPRS Tunneling Protocol” (GTP), blir brukt over grensesnittene S1 og S5/S8 i kjernenettverket for dette formålet [3]. Se kapittel 5 for mer informasjon om protokoller. Tunnelprinsippet er en fordel både med hensyn på sikkerhet og effektivitet.

EPS-bærere er klassifisert i to kategorier basert på hva slags QoS de kan tilby; ”Minimum Guaranteed Bit Rate” (GBR) og non-GBR bærere. ”Minimum Guaranteed Bit Rate” bærere har en tilhørende GBR-verdi, hvor dedikerte transmisjonsressurser blir tildelt permanent ved etablering eller modifikasjon av EPS-bærer. GBR-bærer kan for eksempel bli brukt til applikasjoner som ”Voice over IP” (VoIP). Men siden EPS-systemet bare tilbyr en bærer med en viss QoS, vil kontroll av multimediaapplikasjoner som VoIP bli utført av ”IP Multimedia Subsystem” (IMS), som ligger utenfor selve EPS-systemet. Det er mulig å få tildelt høyere bitrater enn det GBR-bærer garanterer, hvis radioressurser er tilgjengelig. Da vil en ”Maximum Bit Rate” (MBR) parameter sette en øvre grense for hva slags bitrate det er mulig å oppnå fra en GBR-bærer. Non-GBR bærer har ingen båndbredderessurser permanent allokert og kan derfor

ikke garantere noen bestemt bitrate. Non-GBR-bærere blir brukt til applikasjoner som for eksempel webbrowsing eller ”File Transfer Protocol” (FTP) overføringer [3].

Den første EPS-bæreren som blir satt opp ved nettverksoppkobling er en defaultbærer. Se figur 4.4 for en forenklet oppkobling av defaultbærer, initiert av mobilen. Defaultbæreren er etablert så lenge bruker har nettverkstilkobling, for å skaffe bruker en ”always-on” IP-tilkobling til nettverket. Defaultbæreren er alltid en non-GBR bærer, fordi den er permanent etablert og kan derfor ikke garantere en bestemt bitrate. Hvis brukeren ønsker tjenester som krever høyere hastigheter, må det etableres en dedikert bærer i tillegg til defaultbæreren. Den dedikerte bæreren kan enten bli initiert av nettverket, etter ønske fra IMS-domenet, eller fra bruker selv [3].

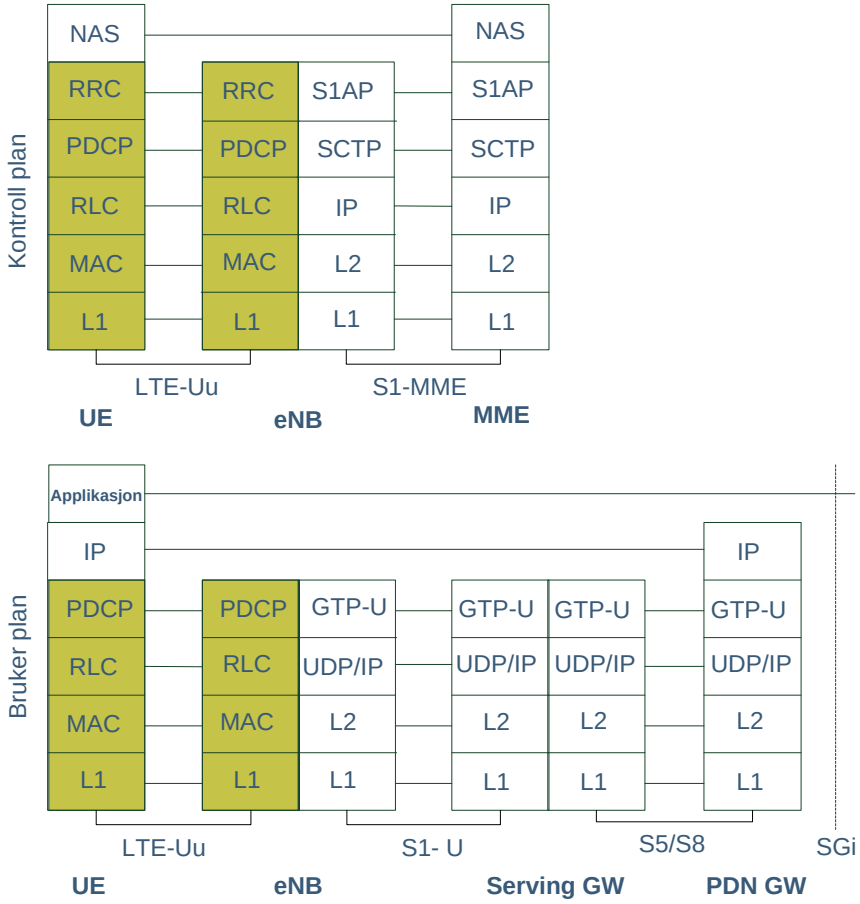


Figur 4.4 Mobilinitiert oppkobling av Defaultbærer (forenklet) [2]

En bruker kan ha en eller flere EPS-bærere tilgjengelig, hvor hver EPS-bærer har en bestemt QoS. Et eksempel kan være multiple applikasjoner, med forskjellige QoS-krav, som kjører samtidig i UE. Da er det behov for like mange EPS-bærere som antall QoS-krav [3].

5 LTE/EPC protokollstruktur

Protokollstrukturen for LTE/EPC er delt opp i bruker- og kontrollplan, se Figur 5.1. I kapittelet fokuseres det mest på ”Access Stratum” protokollene (markert grønt i figur), som går mellom UE og eNB, både for kontroll- og brukerplan. I tillegg tar kapittelet for seg ”Non Access Stratum” protokollen som går mellom UE og MME, og som er en ren kontrollplanprotokoll. Innholdet i dette kapittelet er i hovedsak hentet fra [5], [4], [3] og [9].



Figur 5.1 Protokollstakk; kontrollplan og brukerplan [3]

5.1 Non Access Stratum (NAS)

Det er definert to EPS NAS-protokoller; ”EPS Mobility Management” (EMM) og ”EPS Session Management” (ESM). Funksjoner relatert til forvaltning av EPS-bærer inkluderer etablering, opprettholdelse og frigjøring av EPS-bærer, og er håndtert av ESM NAS-protokollen. EMM-protokollen er ansvarlig for registrering av UE i nettverket, som vil si autentisering, enighet om NAS-nøkler og forhandling om algoritmer og parametere som er nødvendig for kryptering- og integritetsbeskyttelse av NAS-signalering og data. Se kapittel 8 for mer informasjon om sikkerhet. I tillegg tar EMM-protokollen seg av utvelgelse av ”Public Land Mobile Network” (PLMN), ”Tracking Area” (TA) oppdatering og ”paging” av UE i idle tilstand. For mer

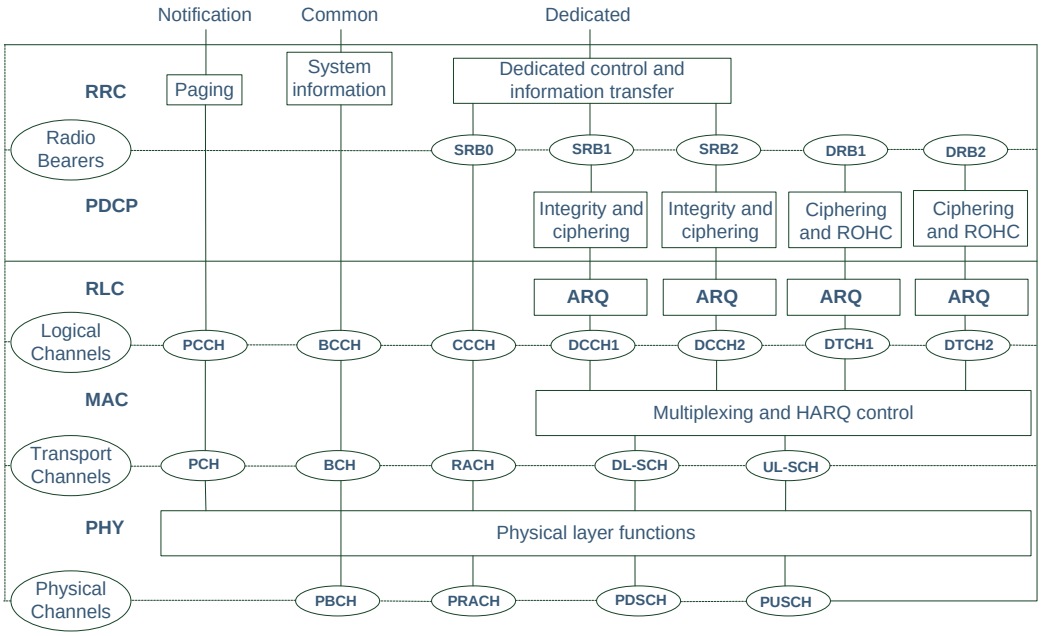
informasjon om TA og ”paging” se kapittel 6.2. Vi skiller mellom dedikert og felles NAS-informasjon, hvor dedikert NAS-informasjon går til en enkelt bruker og felles NAS-informasjon går til alle brukere. NAS-signalering mellom UE og MME vil transparent passere eNB, og ikke være tilgjengelig for basestasjonen. Over radiogrensesnittet er NAS-signalering innkapslet i RRC-signalering, som er kontrollsignalering mellom eNB og UE, se kapittel 5.3.1 [3;10]. I denne rapporten opereres det også med ”EPS Connection Management” (ECM), fordi det blir brukt istedenfor EMM i deler av litteraturen [11].

5.2 Access Stratum (AS) protokollstakk for brukerplan – Lag 2

Lag 2 i AS-protokollstakken for brukerplan består av tre sublag; ”Packet Data Convergence Protocol” (PDCP), ”Radio Link Control” (RLC) og ”Medium Access Control” (MAC), se Figur 5.1. Lag 2 i protokollstakken muliggjør effektiv bruk av Fysisk lag (Lag 1) for pakkedatatrafikk.

5.2.1 Packet Data Convergence Protocol (PDCP)

PDCP-laget prosesserer RRC-meldinger i kontrollplanet og ”Internet Protocol” (IP) pakker i brukerplanet, se Figur 5.1 og Figur 5.2. En av hovedfunksjonene til PDCP-laget i brukerplanet er ”header” kompresjon av ”Data Radio Bearer” (DRB) ved bruk av ”RObust Header Compression (ROHC) protokollen, se Figur 5.2. ”Header” kompresjon er viktig i LTE, fordi LTE ikke har noe linjesvitsjet domene for overføring av tale. For å kunne tilby taletjenester i pakkesvitsjet domene er det nødvendig å komprimere ”headerne” til IP/UDP/RTP, som er typisk for ”Voice over IP” tjenester. En annen viktig funksjon er sikkerhet i form av krypteringsbeskyttelse av DRB, se Figur 5.2. Det er en PDCP per radiobærer [3].



Figur 5.2 Radioarkitektur [3]

5.2.2 Radio Link Control (RLC)

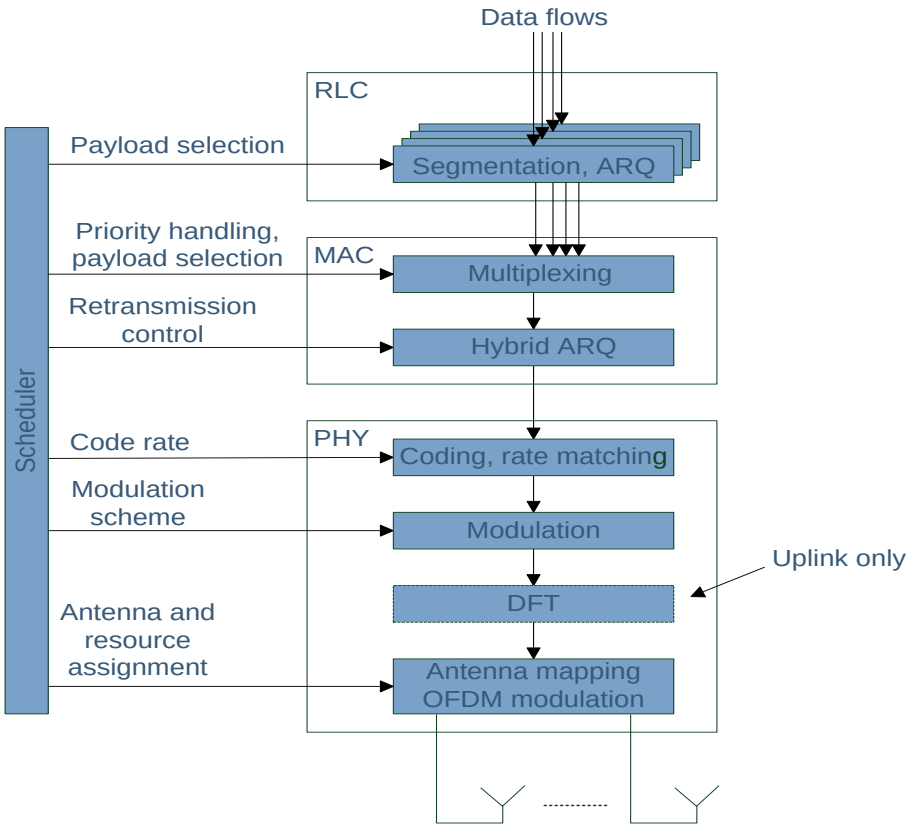
Hovedfunksjonen til RLC-laget er segmentering og sammensetting av pakker fra øvre lag, for å tilpasse dem til en størrelse som det er mulig å sende over radiogrensesnittet. For radiobærere som trenger feilfri transmisjon, vil RLC sende pakker på nytt for å gjenopprette tap av pakker. I tillegg utfører RLC ”in-sequence” levering av data som er blitt mottatt ”out-of-sequence” på grunn av ”Hybrid Automatic Repeat Request” (HARQ) operasjon i MAC-laget under [4]. Det er en RLC enhet for hver radiobærer [3].

5.2.3 Medium Access Control (MAC)

MAC-laget er det laveste sublaget i lag 2 arkitekturen til AS-protokollstakken. Koblingen til det fysiske laget (L1) under er gjennom fysiske transportkanaler, og koblingen til RLC-laget over er gjennom logiske kanaler, se Figur 5.2. MAC-laget utfører derfor multipleksing og demultipleksing mellom logiske- og transportkanaler [3].

MAC-laget er ansvarlig for ”scheduling” av brukerdata i henhold til prioriteringer og multiplekser dataene til L1-transportblokker. MAC-laget multiplekser data fra forskjellige radiobærere, og det er derfor bare en MAC-enhet per UE. MAC-laget har til hensikt å oppnå den avtalte QoS for hver radiobærer ved å bestemme mengden av IP-pakker som kan bli overført fra hver radiobærer og gi beskjed til RLC-laget hvor mange IP-pakker den skal skaffe til veie. Ved opplink inkluderer denne prosessen å rapportere størrelsen på bufrede IP-pakker klar for transmisjon til eNB [3;4].

For å håndtere bitfeil har LTE et retransmisjonssystem over to protokollag, som består av en rask ”Hybrid Automatic Repeat Request” (HARQ) protokoll med lav overhead, supplert med en høyt pålitelig selektivt repeterende ARQ-protokoll med høyere overhead. HARQ-protokollen ligger i MAC-laget, mens ARQ ligger i RLC-laget, se Figur 5.2 og Figur 5.3. Fordelen ved å ha ARQ-håndtering over to lag er oppnåelse av lav forsinkelse og lav overhead uten å ofre påliteligheten. Flest feil er fanget opp og rettet av den enklere HARQ-protokollen på MAC-laget, som sender feedback til sender for hvert sendte subframe. Mens det er sjeldnere behov for å bruke ARQ-protokollen på RLC-laget, som koster mer i form av forsinkelse og overhead. Den tette koblingen mellom de to retransmisjonslagene er mulig fordi begge mekanismene er terminert i basestasjonen [5]. For mer detaljert informasjon om HARQ se [3].



Figur 5.3 LTE-protokollstruktur (forenklet) [5]

5.3 Access Stratum (AS) protokollstakk for kontrollplan - Lag 2 og 3

AS-kontrollplan omhandler radiospesifikk funksjonalitet. Lag 2 i AS-protokollstakken for kontrollplan består, som i brukerplanet, av PDCP-, RLC- og MAC-laget. De utfører samme funksjoner som for brukerplan, med unntak av at det ikke er ”header” kompresjon i kontrollplan. I kontrollplan vil PDCP kun utføre integritets- og krypteringsbeskyttelse av ”Signalling Radio Bearer” (SRB), se Figur 5.2, som overfører RRC-dedikerte meldinger. RRC-protokollen er kjent som lag 3 i AS-kontrollplan protokollstakken, se Figur 5.1.

RRC-protokollen er hovedkontrollfunksjonen i AS og er blant annet ansvarlig for etablering av radiobærere over radiogrensesnittet, ”Signalling Radio Bearer” (SRB) og ”Data Radio Bearer” (DRB) se Figur 5.2. RRC-protokollen dekker en rekke funksjonelle områder, som kringkasting av systeminformasjon, RRC- tilkoblingskontroll, nettverkskontrollert inter-RAT mobilitet, målekonfigurasjon og rapportering. RRC-tilkoblingskontroll dekker alle prosedyrer relatert til etablering, modifisering og frigivelse av en RRC-signalering- og dataforbindelse. Dette inkluderer ”paging”, initial sikkerhetsaktivering, etablering av SRBer og DRBer og handover i LTE. Inter-RAT mobilitet inkluderer blant annet mobilitetsprosedyrer og sikkerhetsaktivering [3].

6 Mobilitet

Mobilitetsbegrepet omfatter UEs mobilitet mellom celler i LTE (E-UTRAN), og til andre systemer som GSM/EDGE, UMTS, WiMAX og CDMA2000.

Mobilitetsprosedyrene i LTE avhenger av om UE er i aktiv eller idle tilstand. Mobilitet i idle tilstand er basert på at UE selv velger hvilken celle den skal knytte seg opp mot (”cell selection”), mens mobilitet i aktiv tilstand baserer seg på hard handover styrt av eNB. Overgangen mellom idle og aktiv tilstand er kontrollert av nettverket avhengig av UE sin aktivitet [4].

6.1 Overgang idle til aktiv tilstand

Når mobilterminalen ønsker å registrere seg i nettverket (UE blir slått på), sende en TA-oppdatering (se 6.2), eller sende eller motta data, sender den henholdsvis NAS-meldingene; ”Attach Request”, ”TAU Request” og ”Service Request” til MME. UE må etablere en logisk NAS-signaleringsforbindelse med MME, som igjen betyr at en RRC- og S1-AP-signaleringsforbindelse må etableres. UE utfører en ”Random Access” prosedyre mot eNB slik at eNB setter opp en RRC-forbindelse (SRB0) over radiogrensesnittet. NAS-meldingene sendes innkapslet i RRC-signaleringen fra UE til eNB og trigger etablering av S1-AP-forbindelsen mellom eNB og MME. Når både RRC- og NAS-signaleringsforbindelse eksisterer er UE i aktiv tilstand og får tildelt radioressurser. MME oppretter UE relatert informasjon i eNB og EPS-bærere etableres. UE vil gå tilbake til idle tilstand når den er blitt registrert i nettverket, har gjort TA-oppdatering eller har sluttet å sende eller motta data. UE i idle tilstand har ikke radioressurser eller signaleringsforbindelse med eNB eller MME. All UE relatert informasjon i aksessnettverket blir slettet når UE går til idle tilstand. Dette gjøres for å redusere overhead i E-UTRAN og prosessering i UE ved lange perioder med datainaktivitet. MME beholder UE-konteksten og informasjon om de etablerte EPS-bærerne når UE er i idle tilstand, for å unngå å sende UE-konteksten så ofte over radiogrensesnittet [3;8;9].

6.2 Mobilitet i idle tilstand

Det er to hovedgrunner for at UE selvstendig styrer mobiliteten i idle tilstand. UEs bruk av transmisjonsressurser minimaliseres ved at signalering over luften bare er nødvendig ved behov for TA-oppdateringer. I tillegg sparer UE batterikapasitet. ”Cell selection” går ut på at UE etter prioritet søker etter den sterkeste cella på alle tillatte frekvenser på alle støttede ”Radio Access Technologies” (RATs), til den finner en egnet celle. UE skanner først over alle radiofrekvensene i E-UTRA-båndet og hvis den finner en egnet celle, blir den valgt. Hvis UE ikke finner en egnet celle innenfor E-UTRA-båndet, vil den søke videre etter prioritet på andre ”Radio Access Technologies” (RATs). [4].

MME vil kjenne UE sin lokasjon enten til nærmeste eNB, hvis UE er tilkoblet, eller til nærmeste ”Tracking Area” (TA) gruppe hvis UE er i idle tilstand. ”Tracking Area” er en pool av eNBer og en eller flere TAer kan være tilknyttet en MME. UE vil i idle tilstand rapportere sin lokasjon enten periodisk, eller når den beveger seg ut av TA-gruppen som den har fått tildelt av MME.

Ved innkommende data til UE fra eksternt nettverk, vil MME be eNBer i den aktuelle TA-gruppen om å søke etter UE, slik at en forbindelse kan bli satt opp for å overføre data [3;4].

6.3 Mobilitet i aktiv tilstand

Nettverket vil alltid forsøke å opprettholde tjenesten til UE på en prioritert ”Radio Access Technology” (RAT), gitt visse preferanser som for eksempel ”Quality of Service” (QoS), kostnad eller nettverksoperatør. Ved mobilitet i prioritert RAT vil UE ta handover til sterkeste celle, og hvis det ikke finnes god nok celle innenfor prioritert RAT vil UE ta handover til en celle i en annen RAT. Da vil UE alltid prøve å ta handover tilbake til en celle i prioritert RAT. Inter-RAT handover er kontrollert av ”source” aksessystemet, som starter målinger og iverksetter handover. Ved inter-RAT handover blir ressurser reservert i ”target” systemet før handoverkommando er sendt til UE. Da GSM/EDGE-systemet ikke støtter ”Packet Switched Handover” (PS HO), vil ikke ressurser bli reservert i GSM/EDGE før HO.

7 Tjenesteegenskaper

Dette kapittelet ser på de grunnleggende tjenestene operatøren leverer og hvordan de flyter i nettet. Tjenesten LTE-nettet leverer er IP-trafikk som funksjon av ”Quality of Service” (QoS).

7.1 ”Quality of Service” (QoS)

For applikasjonslaget vil QoS referere til brukeropplevd kvalitet, som igjen er avhengig av typen applikasjon. Det er ofte vanskelig å oversette brukeropplevd kvalitet til tekniske parametre. Aktuelle parametre er for eksempel tap av data, ”call setup time” og ”call drop rate”. På nettverkslaget vil QoS referere til ende-til-ende transportevne som er tilgjengelig for en tjeneste. Dette inkluderer parametre som datahastighet (bit/s), forsinkelse og tap av data. På det fysiske laget og på linken blir QoS målt i ”bit error rate” og kapasiteten til radioforbindelsen.

7.2 Teoretisk og opplevd hastighet

Teoretisk hastighet på 100 Mbit/s i nedlink og 50 Mbit/s i opplink er den hastigheten systemet kan oppnå ved ideelle forhold som god dekning og lav interferens, og en bruker i cella.

Opplevd hastighet vil si den hastigheten som folk flest får når de bruker LTE-nettet. Trafikklast, dekning, fart og interferens er faktorer som innvirker på den opplevde hastigheten. Dataraten blir lavere når trafikklasten øker, når dekningen blir dårligere som ved randen av cella og når kjøretøyhastighet øker. Interferens fra andre celler påvirker også dataraten negativt. Netcom har et LTE-nett med 20 MHz båndbredde i Oslo og lover opplevd nedlastingshastighet på 10-20 Mbit/s og opplevd opplastingshastighet på 5-10 Mbit/s. Til sammenligning er opplevd nedlastingshastighet med UMTS/HSPA 1-2 Mbit/s.

De høye bitratene som er nevnt for E-UTRA er først og fremst mulig på grunn av større systembåndbredde (20 MHz), høyere ordens modulasjon (64QAM) og bruk av MIMO-teknikken

med opp til fire antenner. Et LTE-system med 5 MHz båndbredde er ikke spesielt mer spektraleffektivt enn et HSPA+ (UMTS 3GPP Release 8) system med 5 MHz båndbredde. Begge systemene har mye til felles, som forenklet arkitektur, 64QAM-modulasjon og MIMO.

7.3 Kontrollplankapasitet

Kapasiteten til LTE-systemet er også påvirket av hvor mange brukere kontrollsignaleringen i systemet kan håndtere samtidig i cella. LTE-systemet skal støtte minst 200 aktive brukere per celle for båndbredder opp til 5 MHz, og minst 400 brukere per celle for større båndbredder. Bare et mindre antall av disse brukerne vil aktivt motta eller overføre data ved et gitt tidspunkt, avhengig for eksempel av tilgjengeligheten av data for sending og av radiokanalens tilstand. Et enda større nummer av ikke aktive brukere vil også være tilgjengelig i hver celle, som kan nås ved ”paging” eller som selv kan starte å sende data med lav oppkoblingsforsinkelse [3].

7.4 Brukerplanforsinkelse

Brukerplanforsinkelse er relevant for ytelsen til mange applikasjoner, som for eksempel VoIP-trafikk og interaktive tjenester som online-spill etc. Brukerplanforsinkelse er definert som gjennomsnittstiden fra den første transmisjon av en datapakke og til mottakelsen av en ”Acknowledgement” (ACK) på det fysiske laget. Forsinkelsen kan måles ved tiden det tar å sende en liten IP-pakke fra terminalen gjennom nettverket til internettserveren og tilbake, ”round trip time”. Kravet til ”round trip time” fra mobilterminal til basestasjon er på 10 ms, og ende-til-ende på 25 ms. Disse ”round trip time” verdiene er lave nok for applikasjoner med strenge krav til brukerplanforsinkelse [3;4].

LTE-kravet på 25 ms “Round – trip time” er en svært lav ende til ende forsinkelse og kan være vanskelig å få til i praksis. Den reelle forsinkelsen vil være avhengig av hvordan overføringskanalen påvirker signalet og av trafikkmengden [3]. Ofte kan ende til ende ”round trip time” bli dominert av forsinkelser som ikke har noe med radiokanalen å gjøre, som avstand og andre elementer i internett [4].

7.5 Kontrollplanforsinkelse

Kontrollplanforsinkelse vil si tiden det tar for en mobilterminal å gå fra idle til aktiv tilstand. For å gi mange brukere opplevelsen av å være ”alltid på” er LTE/EPC designet med lav kontrollplanforsinkelse. Det er satt krav til at kontrollplanforsinkelsen i LTE/EPC skal være mindre enn 100 ms, da er det ikke tatt med ”paging” forsinkelse og NAS-signaleringsforsinkelse.

7.6 Makshastighet kan bli begrenset av TCP bufferstørrelse

Innholdet i dette kapittelet er hovedsakelig hentet fra Wikipedia. Ved kontakt mot internett vil ”Transmission Control Protocol” (TCP) protokollen bli brukt utenfor mobilnettet. En typisk anvendelse av TCP er webapplikasjoner og overføring av datafiler. Tale og videoforbindelser som er følsomme for forsinkelse benytter ikke TCP, men UDP som ikke krever bekreftelse på mottatt pakke og er derfor ikke berørt av denne diskusjonen. Ved bruk av TCP er det behov for buffere

både på sender- og mottakersiden, slik at dataene er lagret i sendermaskinen ved behov for retransmisjon, hvis ikke går dataene tapt. Datamaskiner har ved bruk av TCP en bufferbegrensning på 65535 bytes (TCP Window Size), hvor noen datamaskiner også kan ha mindre buffer enn det maksimalt mulige. Sannsynligvis vil denne bufferen være enda mindre i en mobil. Bufferstørrelsen kan bli en begrensning ved enten høye datahastigheter eller store forsinkelser som for eksempel i satellitt linker. I et mobilt system har vi relativt store forsinkelser som er et produkt av forsinkelsene i de forskjellige komponentene i systemet, blant annet interleaveren. Den maksimale bithastigheten for en enkelt TCP-forbindelse er gitt av bufferstørrelsen i sender og mottaker og ende til ende forsinkelsen i mobilsystemet:

Max Throughput = TCP Window Size/Round – trip time

Over en enkelt TCP-forbindelse, mellom en datamaskin som er koblet opp mot internett via et LTE-modem, vil vi få maks bithastighet:

Maks bithastighet = 65535 bytes/0,025s = 2621400 bytes/s = 20,97 Mbit/s.

Brukeren vil få maks 20 Mbit/s selv om det er mer tilgjengelig kapasitet på LTE-cella.

TCP-bufferen kan være i terminalen, i USB-dongelen som benyttes for dataoverføring, eller i en ruter alt avhengig av system. Hvis datamaskinen, USB-dongelen eller mobilterminalen, som er koblet opp mot internett via LTE, har lavere bufferkapasitet enn maksimal bufferstørrelse vil også makshastighet bli lavere. Det stilles krav til bufferstørrelse hos den som leverer data. Siden dette vanligvis er en større webserver, som man forventer har stor nok bufferstørrelse, går dette bra. Med forskjellige bufferstørrelser hos sender og mottaker vil det kunne oppstå en ustabil situasjon, som vil kunne føre til sterk reduksjon av hastigheten. Med mange brukere i en LTE-celle vil sannsynligvis ikke TCP-problematikken være den begrensende faktor, da hastigheten til hver bruker vil bli begrenset av antall brukere i cella.
Det er blitt utviklet en ”TCP window scale option”, som gjør det mulig å øke ”TCP receive window size” fra maksverdi på 65535 bytes til 1 gigabyte. ”TCP Window Scaling” er implementert som default i Windows siden Windows 2000. Det er usikkert om ”TCP Window Scaling” er implementert i andre operativsystemer som Android, Symbian OS, Blackberry, iPhone OS. I fremtiden med nok minne overalt vil dette problemet forsvinne.

8 Sikkerhet i Evolved Packet System (EPS)

Dette kapittelet omhandler hvordan EPS sikrer konfidensialitet, integritet og tilgjengelighet. Konfidensialitetsbeskyttelse sikrer bruker-, kontroll- og managementplantrafikk mot informasjonslekkasjer. Integritetsbeskyttelse gjør det mulig for mottaker å oppdage om bruker-, kontroll- og managementdata er korrekte og uendret, det vil si oppdage om pakker er blitt lagt til, erstattet eller endret av uautoriserte [3;12]. Tilgjengelighet går ut på å sikre autorisert sluttbrukers tilgang til tjenester og informasjon. ”3GPP Specification group of Security” (SA3) har bestemt at

sikkerhetsløsningene i LTE skal bli utviklet som en verktøykasse uavhengig av sikkerhetstjenester i applikasjonslaget [10]. Informasjon om sikkerhet for tale over LTE se [8].

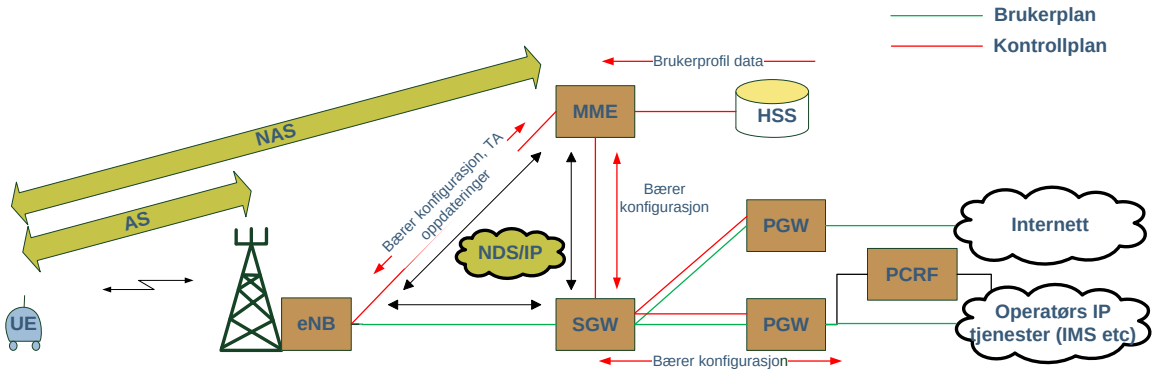
Kapittelet tar for seg beskyttelse av brukerdata og signalering over radiogrensesnitt, backhaul og X2-grensesnitt mellom basestasjoner, se Tabell 8.1. Det ser på hvordan beskyttelsen er realisert ved å gå inn på sikkerhetsarkitektur, algoritmer, autentisering og nøkkelutledning. I tillegg ser kapittelet på sårbarheter i EPS, og sikkerhet i samvirking med andre aksessnettverk.

	eNB	MME	S-GW
UE	**Signalering:** Integritsbeskyttelse Konfidensialitetsbeskyttelse anbefalt **Brukerdata:** Konfidensialitetsbeskyttelse anbefalt	**Signalering:** Integritetsbeskyttelse Konfidensialitetsbeskyttelse anbefalt	
eNB	**Signalering og brukerdata:** Integritetsbeskyttelse og konfidensialitetsbeskyttelse Operatørvalg: kryptografisk eller fysisk beskyttelse	**Signalering:** Integritetsbeskyttelse og konfidensialitetsbeskyttelse Operatørvalg: kryptografisk eller fysisk beskyttelse	**Brukerdata:** Integritetsbeskyttelse og konfidensialitetsbeskyttelse Operatørvalg: kryptografisk eller fysisk beskyttelse

Tabell 8.1 Beskyttelse på radiogrensesnitt, backhaul og X2-grensesnitt

8.1 Sikkerhetslag i Evolved Packet System (EPS)

I EPS er sikkerhetshåndteringen delt opp i tre lag, ”Access Stratum” (AS) sikkerhet, ”Non Access Stratum” (NAS) sikkerhet og ”Network Domain” sikkerhet over IP-grensesnitt (NDS/IP) med ”Internet Protocol Security” (IPsec). ”Access Stratum” sikkerhet håndterer sikkerhet mellom nettverksbruker (UE) og basestasjonen (eNB) i E-UTRAN, se figur 8.1, og sikrer ”Radio Resource Control” (RRC) signalering og brukerdata som går over radiogrensesnittet. NAS-sikkerhet gir ende-til-ende sikkerhet mellom bruker (UE) og ”Mobility Management Entity” (MME) i kjernenettverket (EPC). NAS-sikkerhet sikrer NAS-kontrollsignalering for blant annet autentisering, registrering av UE i nettverket og periodisk re-registrering av UE. NAS-sikkerhetslaget er etablert så lenge UE er registrert i nettverket, mens AS-sikkerhetslaget blir etablert bare når brukerdata og dermed også RRC-signalering trenger å bli utvekslet. NDS/IP-sikkerhet håndterer sikkerheten på IP-grensesnittene i EPS; på backhaul mellom eNB og S-GW, eNB og MME og mellom eNBer, og på grensesnitt mellom forskjellige nettverk, se figur 8.1. Det er separat beskyttelse av signalering og brukerdata, som forsterker sikkerheten i EPS-systemet.



Figur 8.1 AS, NAS og NDS/IP sikkerhet(forenklet) i EPS

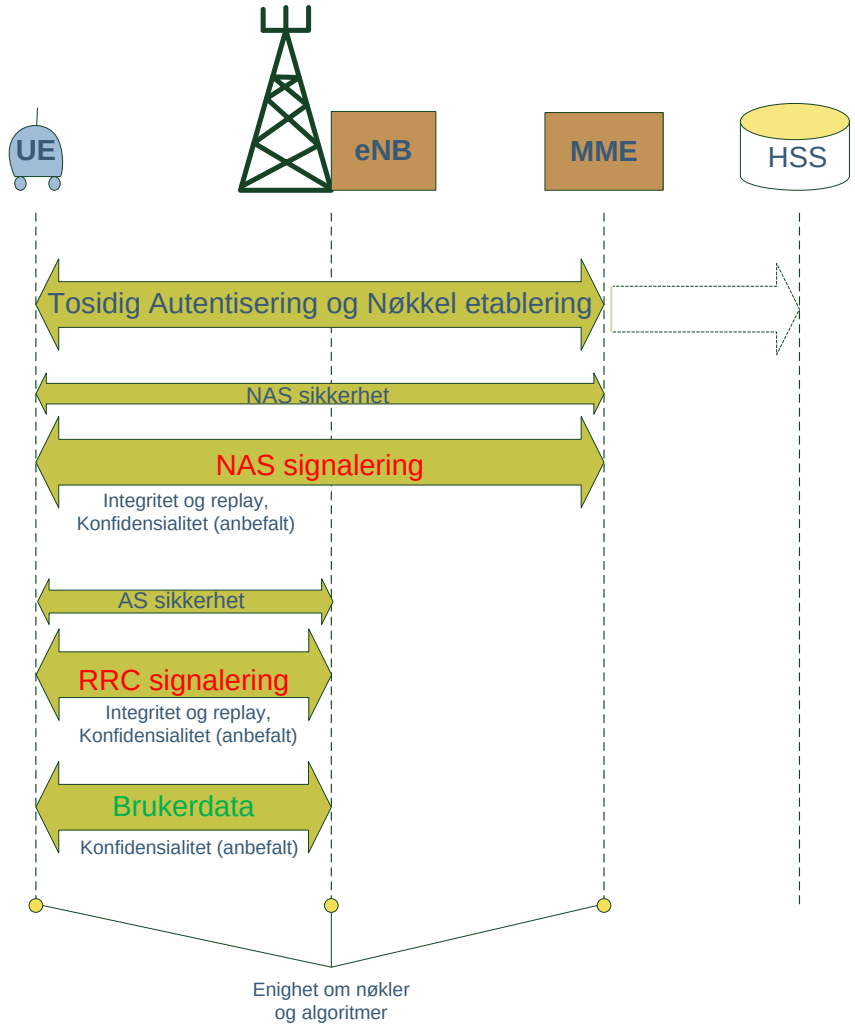
Hensikten med lagdelingen av sikkerheten i LTE/EPC er å minimalisere effekten på NAS-sikkerhetslaget hvis AS-sikkerhetslaget blir kompromittert. Dette prinsippet forbedrer den totale systemsikkerheten og gjør det mulig å plassere eNB i mer utsatte posisjoner uten høy risiko for operatøren. Hvis en angriper klarer å kompromittere det første sikkerhetslaget, så vil det andre sikkerhetslaget fortsatt være uberørt og intakt. Et viktig tema for evaluering er hvordan en eventuell kompromittering av det første sikkerhetslaget vil påvirke den totale LTE/EPC-systemsikkerheten. Målet er å gjøre denne effekten lav og lokal, slik at skadene som følger et kompromittert AS-sikkerhetslag blir begrenset [10].

8.2 Beskyttelse av radiogrensesnittet og NAS-signalering

Dette kapittelet omhandler AS- og NAS-sikkerhetslag og hvorvidt de forskjellige lagene er sikret med hensyn til integritets-, replay- og konfidensialitetsbeskyttelse. Kapittelet kommer også inn på forskjellige varianter av EPS-sikkerhetskontekst, som er parametre som utgjør sikkerheten på sikkerhetslagene. I tillegg ser det på realisering av integritets-, replay- og konfidensialitetsbeskyttelse og sikkerhetsalgoritmer for beskyttelse av NAS, RRC og brukerdata.

8.2.1 Integritetsbeskyttelse

RRC-signalering (SRB1, SRB2) over radiogrensesnittet og NAS-signalering mellom UE og MME skal være integritets- og replaybeskyttet, se figur 8.2 og Tabell 8.1. Replaybeskyttelse er en del av integritetsbeskyttelsen. Brukerdata over radiogrensesnittet skal ikke være integritetsbeskyttet. Dette valget er nok tatt først og fremst på grunn av hensyn til ytelse, da integritetsbeskyttelsen tilføyer en betraktelig større overhead for korte pakker, som for eksempel for VoIP-trafikk [11]. Integritets- og replaybeskyttelse gjør det mulig for mottaker å oppdage om pakker er blitt lagt til, fjernet eller endret, slik at disse pakkene kan avvises hos mottaker [3;12]. På den måten blir integriteten til signaleringen intakt, slik at mottaker og nettverket kan stole på at de mottatte signaleringsdataene er uendret.



Figur 8.2 Access Stratum (AS) og Non Access Stratum (NAS) sikkerhet[2]

8.2.2 Konfidensialitetsbeskyttelse

Konfidensialitetsbeskyttelse er et operatørvalg. 3GPP anbefaler konfidensialitetsbeskyttelse av RRC- og NAS-kontrollsignalering, og av brukerdata over radiogrensesnittet, slik at det ikke skal være mulig å få tilgang til kontrollmeldinger eller brukerdata, se figur 8.2 [11].

8.2.3 EPS-sikkerhetskontekst

En EPS-sikkerhetskontekst er et sett av sikkerhetsparametre (nøkler, algoritmer etc.) som må være etablert mellom UE og nettverket for at de skal kunne kommunisere sikkert seg imellom. EPS-sikkerhetskontekst består både av EPS NAS- og AS-sikkerhetskontekst når UE er i aktiv tilstand. NAS-sikkerhetslaget med EPS NAS-sikkerhetskontekst er etablert så lenge UE er registrert i nettverket. AS-sikkerhetslaget med EPS AS-sikkerhetskontekst blir etablert bare når brukerdata og dermed også RRC-signalering trenger å bli utvekslet, og blir slettet når UE går tilbake til idle tilstand. NAS-signalering kan dermed bli sikret før AS-sikkerhet er etablert mellom eNB og UE når UE går fra idle til aktiv tilstand. En EPS NAS-sikkerhetskontekst etableres enten ved å reetablere en lagret sikkerhetskontekst, utføre en EPS-AKA-prosedyre, se kapittel 8.4, eller mappe sikkerhetskonteksten fra en UMTS-sikkerhetskontekst, se kapittel 8.8 [8;11].

8.2.4 Realisering av integritets-, replay- og konfidensialitetsbeskyttelse

Integritetsbeskyttelse blir realisert ved å legge til en kontrollsum. Replaybeskyttelse, som er en del av integritetsbeskyttelsen, blir ivaretatt av et opptellingssystem. Konfidensialitetsbeskyttelse blir realisert ved hjelp av kryptering. For mer detaljert informasjon se [8;11]. Kryptering og dekryptering av brukerdata og RRC-signalering som går over radiogrensesnittet blir utført i en fysisk sikret del av basestasjonen, hvor også sensitive data som sikkerhetsnøkler, sikkerhetsalgoritmer og vitale konfigurasjonsdata blir lagret [8;13].

Integritetsbeskyttelse av RRC (SRB1 og SRB2) og konfidensialitetsbeskyttelse av RRC og brukerdata (DRB1 og DRB2), blir utført på ”Packet Data Convergence Protocol” (PDCP) laget. Ingen lag under PDCP er dermed beskyttet. Konfidensialitets- og integritetsbeskyttelse av NAS-signalering blir utført som en del av NAS-protokollen. For en oversikt over protokollstakken for kontroll- og brukerplan, se figur 5.1. MAC-laget er ikke integritets- eller konfidensialitetsbeskyttet, da angrep på MAC-laget kun forårsaker dårligere QoS, som oppnås enklere med radiojammeangrep. Da det ikke er mulig å beskytte LTE-systemet mot radiojammeangrep, er det heller ikke blitt brukt ressurser på å beskytte MAC-laget [11].

8.2.5 Algoritmer for beskyttelse av NAS, RRC og UP

I design av EPS-sikkerhet er det lagt til rette for at systemet skal være fleksibelt med hensyn på innføring og fjerning av algoritmer. Det er forventet at EPS vil få nye algoritmer i fremtiden [8].

Krypterings- og integritetsalgoritmene som brukes i EPS for beskyttelse av NAS, RRC og brukerdata er henholdsvis ”128-EPS Encryption Algorithm” 1 og 2 (128-EEA1 og 128-EEA2) og ”128-EPS Integrity Algorithm” 1 og 2 (128-EIA1 og 128-EIA2), se Tabell 8.2. 128-EEA1 er basert på SNOW3G og er tilnærmet identisk med UMTS-krypteringsalgoritme UEA2, som ble introdusert i 3GPP-release 7. 128-EIA1 er også basert på SNOW3G og er tilnærmet identisk med UMTS-integritetsalgoritmen UIA2. 128-EEA2 og 128-EIA2 er begge algoritmer basert på ”Advanced Encryption Standard” (AES). 128-EEA2 er basert på AES i ”Counter” modus og 128-EIA2 er basert på AES i ”Cipher-based MAC” (CMAC) modus.

	SNOW 3G	AES i Counter modus	AES i CMAC modus
Krypteringsalgoritmer	128-EEA1	128-EEA2	
Integritetsalgoritmer	128-EIA1		128-EIA2

Tabell 8.2 Krypterings- og integritetsalgoritmer for NAS, RRC og brukerdata

Valg av AS og NAS 128-EEA/128-EIA algoritmer er uavhengig av hverandre og trenger ikke å være de samme. Alle krypterings- og integritetsalgoritmer har som navnet tilsier en 128-bit inputnøkkel, med mulighet for oppgradering til 256-bit nøkkel i fremtiden[11]. AES-teknologien er dagens standard og går for å være veldig sikker.

8.3 Identifisering av bruker og terminal

GSM, 3G og EPS bruker alle den permanente ”International Mobile Subscriber Identity” (IMSI) for unik identifisering av nettverksbruker. IMSI består av tre deler; ”Mobile Country Code” (MCC), ”Mobile Network Code” (MNC) og ”Mobile Subscriber Identification Number” (MSIN). MCC identifiserer nettverksbrukers hjemland, MNC identifiserer hjemmenettverket til nettverksbruker og MSIN identifiserer nettverksbruker i hjemmenettverket.

En rekke temporære identiteter er assosiert med IMSI i EPS:

- ”Globally Unique Temporary UE Identity” (GUTI)
- ”SAE-Temporary Mobile Subscriber Identity” (S-TMSI) – forkortet versjon av GUTI
- “Cell Radio Network Temporary Identifier” (C-RNTI)

GUTI er den temporære brukeridentiteten som blir brukt i EPS og blir allokert av MME, ved bruk av NAS-protokollen EMM, for å konfidensialitetsbeskytte brukeridentiteten IMSI. C-RNTI blir brukt til å identifisere en brukerterminal når en RRC-forbindelse eksisterer og gir en unik UE-identifisering på cellenivå. GUTI består av ”Globally Unique MME Identifier” (GUMMEI) og M-TMSI. GUMMEI vil globalt identifisere MME som allokerte GUTI, og M-TMSI vil unikt identifisere UE innenfor MME som allokerte GUTI. GUMMEI er konstruert fra MCC, MNC og ”MME Identifier” (MMEI). For visse prosedyrer som paging og ”Service Request” brukes ”SAE-Temporary Mobile Subscriber Identity” (S-TMSI), som er en forkortet versjon av GUTI. S-TMSI brukes for å oppnå mer effektive radiosignaleringsprosedyrer. S-TMSI består av M-TMSI og en del av MMEI. MME kan tildele GUTI til UE i en ”Attach Accept” melding eller i en ”Tracking Area Update Accept” melding. MME kan også tildele GUTI i en separat ”GUTI Reallocation” prosedyre. I hvert tilfelle skal MME sende GUTI først etter at beskyttelse av NAS-signalering er aktivert. Når UE skifter MME, må den få tildelt ny GUTI. C-RNTI er preallokert i target eNB og sendt til UE i handoverkommando eller i forbindelse med tildeling av radioressurser [8;10].

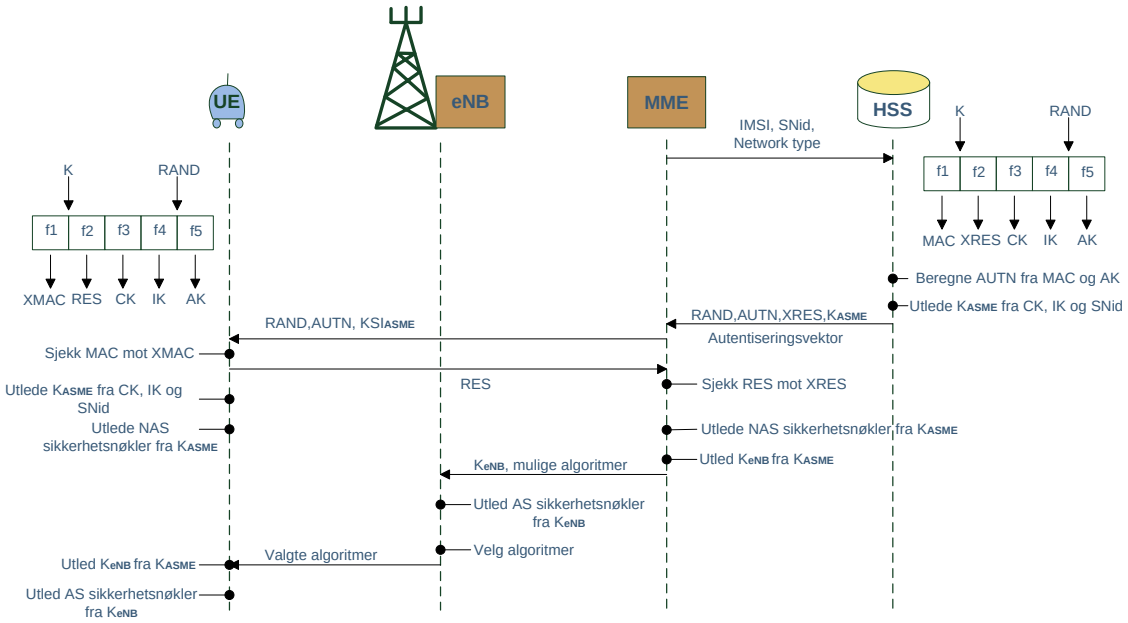
GSM, 3G og EPS bruker alle den permanente terminalidentiteten ”International Mobile Equipment Identity” (IMEI). I GSM og 3G kan nettverket be om å få oversendt IMEI fra UE før signaleringssikkerhet er etablert, slik at IMEI blir sendt i klartekst over radiogrensesnittet. Da nettverksbruker gjerne har en mobilterminal for en lengre periode, vil IMEI også kunne gi sterke indikasjoner angående brukeridentiteten. I EPS skal UE ikke sende IMEI til nettverket før NAS-sikkerhet er aktivert, terminalidentiteten IMEI er derfor bedre beskyttet i EPS forutsatt at NAS-signaleringen er konfidensialitetsbeskyttet [8].

8.4 EPS-AKA (Authentication and Key Agreement protocol)

”Authentication and Key Agreement” (EPS-AKA) er autentiseringsprotokollen som blir brukt i EPS for gjensidig autentisering av UE og nettverket, og produksjon av en basisnøkkel K_{ASME}. K_{ASME} blir brukt direkte og indirekte i utledning av sikkerhetsnøklene i EPS. EPS-AKA er gjenbruk av UMTS-AKA med noen små endringer. EPS-AKA blir utført mellom USIM/UE og MME. Gjenbruk av UMTS-AKA ble valgt for blant annet å gjøre handover (HO) mellom UMTS

og LTE enklere. Med gjensidig autentisering er en sikker på at basestasjon og mobilterminal er den de gir seg ut for. Det er alltid MME som initierer EPS-AKA-prosedyren. Prosedyren må kjøres når UE og MME ønsker å kommunisere og de ikke deler en EPS-sikkerhetskontekst. Det vil blant annet si når UE for første gang registrerer seg i nettverket eller hvis UE av forskjellige årsaker har blitt avvist av nettverket og alle autentiseringsdata i UE og MME er blitt slettet. MME bestemmer når det er behov for en ny AKA-gjennomkjøring, som for eksempel ved ønske om å fornye en EPS-sikkerhetskontekst. EPS-AKA-prosedyren blir initiert av nettverket så ofte operatøren ønsker [3;8;10;11].

Autentiseringsprosessen og videre utledning av sikkerhetsnøkler er vist i Figur 8.3. EPS-AKA initieres av at MME sender en forespørsel om autentiseringsvektor til "Home Subscriber Server" (HSS), hvis den ikke har en ubrukt autentiseringsvektor lagret. Forespørselen inneholder IMSI, "Serving Network Identity" (SNid) og nettverkstypen (E-UTRAN). IMSI er koblet til den permanente hemmelige nøkkelen *K*, som er unik for hver bruker. K er lagret bare i USIM i mobilterminalen og i "Authentication Center" (AUC), som er en del av HSS, og forlater aldri USIM eller AUC.



Figur 8.3 EPS AKA (Authentication and Key Agreement) og utledning av sikkerhetsnøkler [2]

Autentiseringsvektoren som HSS sender til MME består av parametrene RAND, AUTN, *XRES* og K_{ASME}, se Figur 8.3. RAND er et tilfeldig tall som brukes sammen med *K* i AUC som input til et sett algoritmer for kalkulering av *MAC*, *XRES*, *CK*, *IK* og *AK*. AUTN blir utledet fra "Message Authentication Code" (*MAC*), "Anonymity Key" (*AK*) og et "Sequence Number" (*SQN*) i HSS. AUTN er et autentiseringsbevis som USIM bruker for å autentisere nettverket. *XRES* står for "expected RES" og blir brukt av MME til å autentisere bruker. Basisnøkkelen K_{ASME} blir utledet fra "Ciphering Key" (*CK*), "Integrity Key" (*IK*), *SNid* og (*SQN* xor *AK*) i HSS. Hver autentiseringsvektor kan brukes til bare én gjennomkjøring av EPS-AKA-prosedyren. *CK* og *IK* generert ved EPS-AKA skal aldri forlate HSS [2;8;11].

Autentisering av nettverket skjer i USIM i mobilterminalen. Den hemmelige nøkkelen *K* er sammen med RAND input til en rekke algoritmer som regner ut *XMAC*, *RES*, *CK*, *IK* og *AK* i USIM. *XMAC* står for ”expected MAC” og blir brukt av USIM til å autentisere nettet. I USIM vil *MAC*, som er overført gjennom AUTN, bli sjekket opp mot *XMAC*, og nettverket er autentisert hvis disse er like. Når USIM har gjort en vellykket verifisering av AUTN skal den ikke akseptere en annen AUTN med samme *SQN*. RAND og AUTN kommer fra autentiseringsvektoren og er oversendt fra MME, se Figur 8.3.

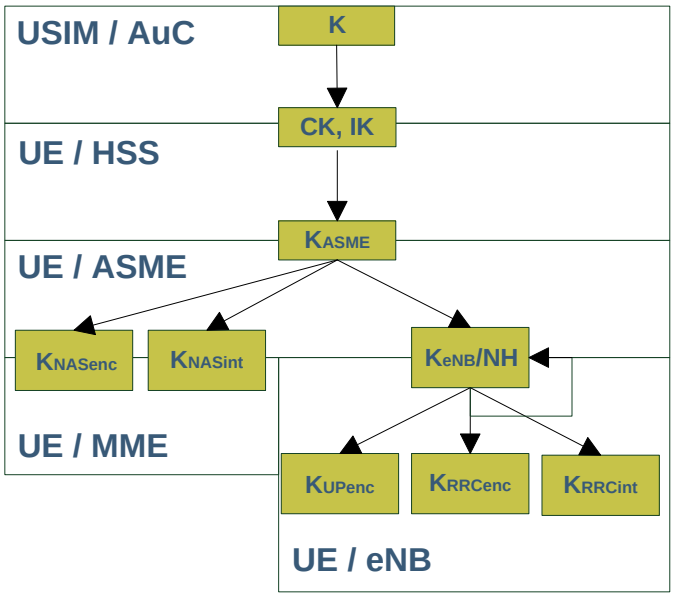
Autentisering av mobilterminalen skjer i MME. Når nettverket er autentisert vil UE sende parameteren *RES* i en autentiseringsrespons til MME, hvor den sjekkes opp mot *XRES*. UE er autentisert av nettverket hvis *RES* er lik *XRES*.

Basisnøkkelen K_{ASME} blir deretter utledet i UE fra *CK*, *IK*, *SNid* og (*SQN* xor *AK*). For å sikre at UE og MME blir synkronisert med lik K_{ASME}, brukes nøkkelidentifikatoren KSI_{ASME}. Både nettverk og bruker er nå autentisert og K_{ASME} er tilgjengelig for videre utledning av sikkerhetsnøkler som UE kan bruke i kommuniakasjon med nettverket.

8.5 Nøkkelutledning i EPS

Prosessen for etablering av EPS NAS-sikkerhetskontekst med K_{ASME} og NAS-sikkerhetsnøkler, avhenger av om UE registrerer seg i nettverket, om UE går fra idle til aktiv tilstand eller om UE beveger seg mellom forskjellige aksessnettverk. Når UE registrerer seg i nettverket vil den enten reaktivere en lagret EPS NAS-sikkerhetskontekst, eller kjøre en EPS-AKA-prosedyre. UE som går fra idle til aktiv tilstand vil bruke eksisterende EPS NAS-sikkerhetskontekst. For mobilitet mellom LTE og andre aksessnettverk se kapittel 8.7, 8.8 og 8.9. Når EPS NAS-sikkerhetskontekst er etablert vil den bli brukt til å etablere EPS AS-sikkerhetskontekst med AS-sikkerhetsnøkler.

EPS opererer med symmetriske nøkler. Den hemmelige nøkkelen *K*, som blir brukt til å utlede nøklene *CK* og *IK* i USIM og HSS, er den øverste nøkkelen i nøkkelhierarkiet i EPS, se Figur 8.3, Figur 8.4 og Figur 8.5. Nøklene *CK*, *IK* blir igjen brukt i utledning av basisnøkkelen K_{ASME} i UE og MME. NAS-sikkerhetsnøkler og K_{eNB} utledes fra K_{ASME} i UE og MME og AS-sikkerhetsnøkler utledes fra K_{eNB} i UE og eNB.



Figur 8.4 Nøkkelhierarki i Evolved Packet System (EPS) [11]

Nøkkel	Hensikt	Lengde	Utled fra	Beskrivelse
K	Hovednøkkel for GSM, UMTS, EPS	128	-	Hemmelig nøkkel lagret permanent i USIM og AuC eller HSS
CK,IK	Kryptering, Integritets nøkler	128	K	Nøkler laget i AuC eller HSS og USIM ved AKA prosess.
K_{ASME}	MME (ASME) Basis / mellom nøkkel	256	CK, IK	Nøkkel laget i HSS og UE fra CK,IK ved AKA. MME tar på seg rollen til ASME i EPS.
K_{eNB}	eNB basis nøkkel	256	K_{ASME} K_{eNB}*	Mellomnøkkel laget i MME og UE fra K_{ASME} når UE går over i ECM – CONNECTED tilstand eller laget i UE og Target eNB fra K_{eNB}* ved HO.
K_{eNB}*	eNB overgangsnøkkel ved HO	256	K_{eNB} (H) NH (V)	Mellomnøkkel laget ved HO i Source eNB og UE enten med horisontal (K_{eNB}) eller vertikal (NH) nøkkel derivasjon. Brukes av Target eNB til å utlede K_{eNB}.
NH	Next Hop	256	K_{eNB}	Mellomnøkkel laget i MME og UE brukt for forward security, og sendt til eNB via S1-MME
K_{NASint}	Integritetsnøkkel for NAS signalering	256 (128 LSB)	K_{ASME}	Integritetsnøkkel laget i MME og UE for beskyttelse av NAS data
K_{NASenc}	Krypteringsnøkkel for NAS signalering	256 (128 LSB)	K_{ASME}	Krypteringsnøkkel laget i MME og UE for beskyttelse av NAS data
K_{UPenc}	Krypteringsnøkkel for brukerplanet (Data Radio Bearer - DRB)	256 (128 LSB)	K_{eNB}	Krypteringsnøkkel laget i eNB og UE for beskyttelse av brukerplan data
K_{RRCint}	Integritetsnøkkel RRC signalering (Signaling Radio Bearer - SRB)	256 (128 LSB)	K_{eNB}	Integritetsnøkkel laget i eNB og UE for beskyttelse av RRC data
K_{RRCenc}	Krypteringsnøkkel for RRC signalering (SRB)	256 (128 LSB)	K_{eNB}	Krypteringsnøkkel laget i eNB og UE for beskyttelse av RRC data

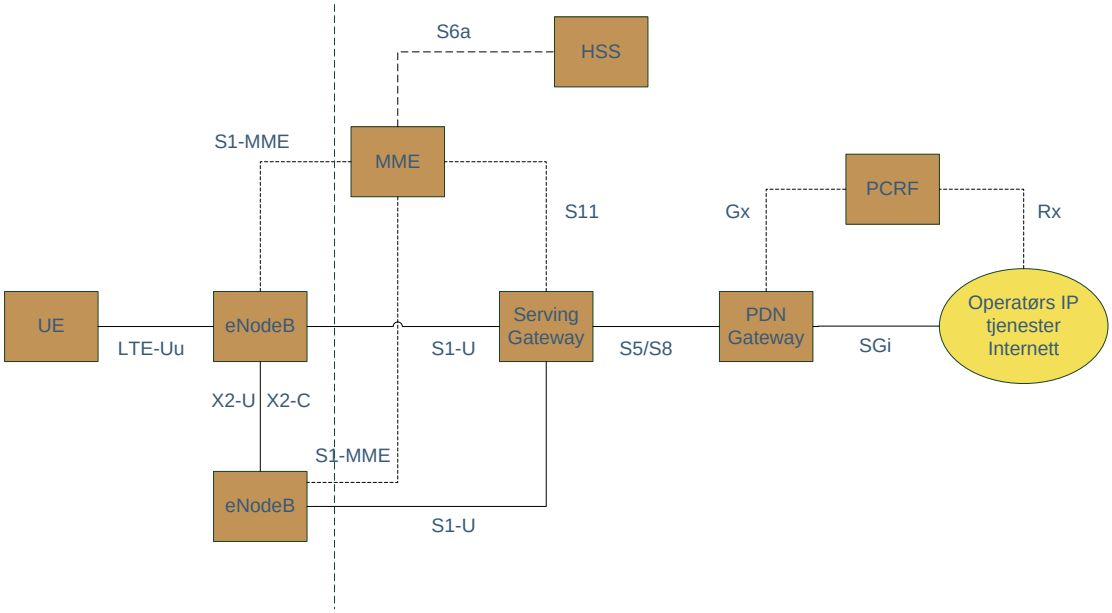
Figur 8.5 Sikkerhetsnøkler i EPS, noe forenklet [14]

Ingen nøkler blir sendt over radiogrensesnittet. Nøkkelidentifikatoren KSI_{ASME} blir sendt over radiogrensesnittet for identifisering av basisnøkkel K_{ASME}. K_{ASME} skal aldri forlate EPC og den sendes ikke over "backhaul" eller radiogrensesnittet. Nøkkelen K_{eNB} sendes over "backhaul" og X2. K_{eNB} er unik innen hver basestasjonscelle og endres ved handover, som igjen fornyer AS-sikkerhetsnøklene. Fornyelse av AS-sikkerhetsnøkler uten ny EPS-AKA-prosedyre er en

forbedring i forhold til UMTS. I nøkkelgenerering ved handover vil basestasjonen bruke enten en "Next Hop" (NH) parameter eller K_{eNB} for å utlede ny K_{eNB^*} for bruk i ny basestasjonscelle. For nærmere beskrivelse se [8;11]. "Access Security Management Entity" (ASME) er en instans som mottar toppnivånøkler i aksessnettverk fra HSS. MME tar rollen som ASME. K_{ASME} er 256 bit med nøkkelentropi på 128 bit. Alle nøkler kan bli forlenget til 256 bit ved behov [2;3;8;11].

8.6 Beskyttelse av backhaul, X2-grensesnittet og andre IP-grensesnitt

"Network Domain Security over IP layers" (NDS/IP) med "Internet Protocol Security" (IPsec) blir brukt for å beskytte IP-baserte grensesnitt i EPS, det vil si på backhaul mellom eNB og S-GW, eNB og MME og mellom eNBer, i tillegg til grensesnitt mellom forskjellige nettverk, se figur 8.1 og 8.6 [8;11;14].



Figur 8.6 Grensesnitt i Evolved Packet Service (EPS) [3]

8.6.1 Integritetsbeskyttelse og Konfidensialitetsbeskyttelse

Kontrollsignalering over grensesnittene S1-MME og X2-C og brukerdata over grensesnittene S1-U og X2-U skal være integritets-, replay- og konfidensialitetsbeskyttet. Managementplantrafikk over S1-grensesnittet, som blant annet er oppsett- og konfigurasjonstrafikk av eNB, skal også være integritets-, replay- og konfidensialitetsbeskyttet. Det er opp til operatør hvordan dette gjøres, om grensesnittene beskyttes fysisk eller ved bruk av NDS IPsec [8;11].

8.6.2 Realisering av NDS/IP sikkerhet

Sikkerhetsbeskyttelsen er etablert på nettverkslaget og implementert i basestasjonen. NDS/IP bruker IPsec med sikkerhetsprotokollen "Encapsulating Security Payload" (ESP) i tunnelmodus. IPsec-funksjonalitet som må være støttet i NDS/IP, er krypteringsalgoritmene 3DES-CBC, AES-CBC og autentiseringsalgoritmen ESP-HMAC-SHA-1. Implementering av "Internet Key Exchange" (IKEv2) med sertifikatbasert autentisering er obligatorisk. IKEv2 blir brukt i NDS/IP

nettverk for å forhandle, etablere og opprettholde en sikker ESP-tunnel mellom ”Security Gateways” (SEGs) [8;11;14].

”Network Domain” sikkerhetsfunksjoner bruker hashfunksjoner for å lage digitale signaturer, spesielt i sertifikater. Hashfunksjoner brukes også for å lage ”Message Authentication Code” (MAC) for NDS/IP sikkerhet. Den mest brukte algoritmen for begge tilfellene over er SHA-1. Da SHA-1 ikke lenger er kollisjonssikker, må andre hashfunksjoner, som SHA-256 (256-bit hash), bli brukt i de tilfeller hvor hashfunksjonen avhenger av at algoritmen er kollisjonssikker. Dette gjelder blant annet for utregning av digitale signaturer. Kollisjonssikkerhet er ikke kritisk når hashfunksjonen blir brukt for å lage ”Message Authentication Code” eller ved nøkkelderivasjon. SHA-1 kan derfor fortsatt bli ansett som tilstrekkelig for utregning av MAC og nøkkelderivasjon i LTE/EPC [8]. ”The National Institute of Standards and Technology” (NIST) leder i dag en internasjonal konkurranse for å utvikle en ny standard hashfunksjon, kalt SHA-3.

Tunnelmodus vil si at den opprinnelige IP-pakken blir pakket inn i en ny IP-pakke. ESP vil i tunnelmodus beskytte hele den opprinnelige IP-pakken inkludert dens IP-header. Den nye IP-header vil inneholde IP-adressen til IPsec ”Security Gateways” (SEGs). I praksis vil det settes opp en IPsec-tunnel i eNB, som termineres i en SEG på kjernenettverksiden [8;11;14].

8.7 Sikkerhet i samvirking med andre EPS-nettverk

Mobilitet mellom to E-UTRAN-aksessnettverk baserer seg på overføring av EPS NAS-sikkerhetskontekst fra ”source” til ”target” nettverk, og da også bruk av denne sikkerhetskonteksten mellom UE og den nye MME, gitt at begge operatørers sikkerhetspolicy tillater det. K_{ASME} forlater ikke EPC, selv om den blir overført fra gammel MME til ny MME i nytt E-UTRAN-nettverk. EPS-autentiseringsvektorer blir ikke overført fordi de ikke kan brukes i ”target” nettverk. Overføring av sikkerhetskontekst i handover mellom to EPS-nettverk øker effektiviteten, da det ikke er nødvendig å kontakte HSS og utføre en ny EPS-AKA-prosedyre. Dette er spesielt viktig i områder hvor topologien kan forårsake mange handover frem og tilbake mellom MMEer i forskjellige EPS-nettverk, som for eksempel på grensen mellom to land.

Overføring av sikkerhetskontekst og bruk av ”source” nettverkets sikkerhetskontekst i ”target” nettverk strider imot LTE sitt opprinnelige mål om ikke å bruke nøkler bundet til et nettverk, i et annet nettverk. Dette er en avveiing 3GPP har gjort mellom effektivitet og sikkerhetsrisiko i handoversituasjonen. Argumenter som er brukt for å forsvare denne avgjørelsen er blant annet at EPS-sikkerhetskonteksten bare blir overført til MMEer som den gamle MMEen har tillit til og at det nye nettverket vil bli autentisert ved en senere EPS-AKA-kjøring [8].

8.8 Sikkerhet i samvirking med GERAN/UTRAN

I mobilitet mellom systemene E-UTRAN og GERAN/UTRAN brukes en prosedyre som heter mapping av sikkerhetskontekst. Samvirking med GERAN/UTRAN forutsetter at UE har USIM. Mapping av sikkerhetskontekst brukes alltid i handover av hensyn til effektivitet, selv om det er lagret en sikkerhetskontekst i ”target system”. Mapping av sikkerhetskontekst unngår behovet for

å kontakte HSS og en ny runde med autentisering i ”target” nettverk og øker dermed ytelsen. Dette er spesielt viktig i områder med mange handover mellom E-UTRAN og GERAN/UTRAN. Noe som blir svært aktuelt da E-UTRAN i starten vil bli bygget ut som dekningsøyer innenfor dekningsområdet til GERAN/UTRAN. I tillegg vil sannsynligvis operatørene i fremtiden styre trafikken mellom de tre aksessnettverkene etter hva slags tjenester bruker ønsker og de forskjellige aksessnettverkenes dekning og kvalitet. Mobilitet mellom systemene i idle-modus bruker den eksisterende sikkerhetskonteksten i ”target system” hvis den er tilgjengelig, ellers vil den også bruke mappet sikkerhetskontekst. En mappet EPS-sikkerhetskontekst blir beholdt i overgang fra aktiv til idle tilstand og kan bli brukt til å sikre den første NAS-meldingen når UE går tilbake til aktiv tilstand. En mappet EPS-sikkerhetskontekst blir slettet når UE deregistreres, som for eksempel når UE slås av [8;15].

Mappingen går ut på at en UMTS-sikkerhetskontekst blir brukt til å utlede en EPS-sikkerhetskontekst og omvendt. Ved handover fra E-UTRAN til UMTS vil UE og EPC bruke basisnøkkelen K_{ASME} til å utlede sikkerhetsnøkler for bruk i UMTS, som blir sendt til UMTS over kjernenettverket. Ved handover fra UMTS til E-UTRAN vil UMTS sende sine sikkerhetsnøkler til EPC som bruker dem til å utlede egen basisnøkkel for bruk i EPS. UE utleder også basisnøkkel fra sikkerhetsnøklene den har tilgjengelig i UMTS nettet. Basisnøkkelen blir så brukt til å utlede resten av nøkkelhierarkiet i EPS.

Sikkerhetskontekstmapping tilfredsstiller kravet om ”backward security”, men ikke ”forward security”. Det vil si at ”target system” ikke kan utlede nøklene til ”source system”, mens ”source system” kjenner til de mappede nøklene som blir brukt i ”target system”. Det er derfor tilrådelig å etablere en ny sikkerhetskontekst i EPS så raskt som mulig etter handover, for å minimalisere denne usikkerheten rundt tillit til ”source system”. Selv når begge nettene tilhører samme operatør er det ikke anbefalt å bruke en mappet kontekst i E-UTRAN, da EPS-sikkerheten er sterkere enn UMTS-sikkerheten. Det er derfor sterke anbefalinger for å kjøre en EPS-AKA-prosedyre så raskt som mulig etter handover til E-UTRAN, eller reaktivere en eventuelt lagret EPS-sikkerhetskontekst. Det er ingen motforestillinger mot å bruke en EPS-sikkerhetskontekst mappet over på UTRAN eller GERAN, når nettene tilhører samme operatør. For nærmere beskrivelse av nøkkelhåndtering ved mapping av sikkerhetskontekst se [8;15].

8.9 Sikkerhet i samvirking med non-3GPP-aksessnettverk

I mobilitet mellom E-UTRAN og non-3GPP-aksessnettverk er det verken mulig å overføre sikkerhetskontekst eller mappe sikkerhetskontekst, fordi sikkerhetsarkitekturen i 3GPP- og non-3GPP-nettverkene er for forskjellige. Generelt er det ikke mye som kan gjøres, sett fra et sikkerhetssynspunkt, for å forbedre ytelsen.

3GPP definerer allikevel to forskjellige prosedyrer for handover mellom E-UTRAN og non-3GPP-aksessnettverk:

- handover med optimalisering mellom E-UTRAN og en cdma2000 HRPD aksess
- handover uten optimalisering mellom E-UTRAN og en generell non-3GPP-aksess

For handover uten optimalisering vil det ikke være noen nyutvikling med hensyn til sikkerhet. UE vil knytte seg til ”target” aksessnettverk og utføre sikkerhetsprosedyrene definert for ”target” aksessnettverk. Hvis for eksempel UE beveger seg fra et non-3GPP-aksessnettverk til E-UTRAN, vil UE knytte seg til E-UTRAN, utføre EPS-AKA og etablere konfidensialitets- og integritetsbeskyttelse.

Ved handover med optimalisering mellom E-UTRAN og cdma2000 HRPD blir preregistrering brukt for å forbedre ytelsen. Preregistrering inkluderer preautentisering. UE registrerer seg i ”target” nettverk og bruker prosedyrer som er spesifikke for ”target” nettverk mens UE fortsatt er knyttet til ”source” nettverk. Handoverfasen starter når preregistreringen er fullført. Preregistrering effektiviserer handover betydelig [8].

8.10 Sårbarheter i EPS

Kapittelet tar for seg sårbarheter i forbindelse med manglende integritets- og konfidensialitetsbeskyttelse i EPS. Det at MAC-laget ikke er beskyttet vil kunne føre til dårligere QoS, som kan gå utover tilgjengeligheten til nettverksbruker. Hvis kryptering blir innført for NAS-signalering, og brukerdata og RRC-signalering over radiogrensesnittet etter anbefaling fra 3GPP, vil sårbarhetene i punktene 8.10.2, 8.10.3 og 8.10.5 bli ivaretatt.

8.10.1 Injeksjon og modifikasjon av brukerplanpakker på radiogrensesnittet

Manglende integritetsbeskyttelse av IP-pakker over radiogrensesnittet, vil blant annet åpne for angrep i form av injeksjon og modifikasjon av IP-pakker uten at det blir oppdaget. Hvis IP-pakkene er konfidensialitetsbeskyttet, vil injeksjon eller modifikasjon av IP-pakkene bare resultere i ugjenkjennelig data ved dekryptering på mottagersiden. Dette vil resultere i dårligere kvalitet for UE eller DoS (”Denial of Service”) angrep, som vil påvirke tilgjengeligheten for nettverksbruker. Hvis IP-pakkene ikke er kryptert, vil det også være mulig å modifisere brukerdataene, som igjen vil svekke integriteten til dataene slik at de ikke vil være til å stole på. Bare integritetsbeskyttelse kan oppdage injeksjon og modifikasjon av IP-pakker, slik at pakkene kan forkastes [10].

8.10.2 Konfidensialitetsangrep gjennom avlytting av brukerplanpakker

Hvis operatør ikke krypterer brukerdata på radiogrensesnittet, vil angriper kunne tilegne seg fortrolig innhold fra nettverksbruker, identitets- og routinginformasjon og kommunikasjonsmønster. Dette vil igjen gjøre det mulig å tracke bruker. Da konfidensialitetsbeskyttelsen i LTE blir etablert på PDCP-laget, som ligger under IP-laget, blir IP-adresser og routinginformasjon beskyttet ved kryptering. Protokollagene under PDCP-laget

blir ikke beskyttet, se figur 5.1 for oversikt over protokollstakken [3;4;10;11]. GSM og UMTS har konfidensialitetsbeskyttelse av brukerdata over radiogrensesnittet, og det er stor sannsynlighet for at dette videreføres i LTE.

8.10.3 Konfidensialitetsangrep gjennom avlytting av RRC- og NAS-signalering

Avlytting av "mobility management" trafikk, som kan bli sendt som RRC- og NAS-signalering, kan frembringe sensitiv informasjon relatert til brukere og nettverksoperatører. Analyse av slik informasjon kan føre til brudd på konfidensialitet og lede til for eksempel lokalisering av nettverksbruker. Mottiltak vil være kryptering av RRC- og NAS-signalering, avhengig av sårbarhet. Hvis for eksempel RRC-signaleringen ikke blir kryptert, vil det være mulig å målfølge UE basert på feltstyrkemålinger på cellenivå og kartlegging av HO [3;10].

8.10.4 Konfidensialitetsangrep på grensesnittene S1-MME, S1-U, X2-C og X2-U

Hvis operatør satser på fyskisk beskyttelse av grensesnittene S1-MME, S1-U, X2-C og X2-U kan det åpne for konfidensialitetsangrep avhengig av angripers ressurser. Angriper vil da kunne tilegne seg fortrolig innhold fra brukerdata som går over backhaul og mellom basestasjoner. Og det vil være mulig å få tak i basestasjonsnøkkelen K_{eNB} fra signalering på backhaul og X2-C.

8.10.5 IMSI, GUTI, S-TMSI og C-RNTI blir sendt i klartekst over radiogrensesnittet

I avsnittene under følger en rekke eksempler på sårbarheter som oppstår ved at UE sin statiske identitet IMSI og temporære identiteter GUTI, S-TMSI og C-RNTI, blir sendt i klartekst over radiogrensesnittet. Dette muliggjør blant annet sporing av og redusert tilgjengelighet for nettverksbruker. Et tiltak mot denne trusselen er å reallokere GUTI eller S-TMSI etter at NAS-kryptering er aktivert og reallokere C-RNTI etter at RRC-kryptering er aktivert [10].

Når UE registrerer seg i nettverket for første gang eksisterer det ingen EPS NAS-sikkerhetskontekst og IMSI vil bli sendt i klartekst i "Attach Request" melding til MME, for at MME kan bruke IMSI i EPS-AKA. Da MME tildeler GUTI i en "Attach Accept" melding med NAS-sikkerhet etablert, vil UE ved senere registreringer sende GUTI i klartekst i "Attach Request" til MME.

Hvis UE har en EPS NAS-sikkerhetskontekst lagret, vil GUTI bli integritetsbeskyttet men ikke kryptert. GUTI kan ikke krypteres i tilfelle MME ikke har samme EPS NAS-sikkerhetskontekst som UE lagret, slik at MME ikke kan dekryptere meldingen. MME vil da bruke GUTI til å finne UE sin forrige MME, som vil sende IMSI, sikkerhetskapabiliteten til UE og EPS NAS-sikkerhetskontekst til ny MME. "Tracking Area Update Request" melding, med GUTI og KSI_{ASME}, fra UE til MME ved en TA-oppdatering vil av samme grunn bare integritetsbeskyttes.

Da det ikke eksisterer noen AS-sikkerhtskontekst når UE sender "Attach Request" eller "Tracking Area Update Request" til MME, vil GUTI bli sendt i klartekst over radiogrensesnittet. Dette kan i begge tilfeller kompenseres for ved at MME kan sende en ny GUTI til UE etter at NAS-sikkerhet er etablert. Når UE skal sende eller motta data, det vil si gå fra idle til aktiv tilstand, vil den sende S-TMSI integritetsbeskyttet i "Service Request" melding til MME. Da AS-

sikkerhet ikke er etablert når ”Service Request” meldingen sendes, vil S-TMSI også sendes i klartekst over radiogrensesnittet fra UE til MME. Hvis NAS-signalering er kryptert på linken fra MME til UE, vil en angriper ikke kunne tilegne seg ny GUTI eller ny S-TMSI. Angriper kan da ikke assosiere ny GUTI eller ny S-TMSI med IMSI eller en tidligere sendt GUTI eller S-TMSI i en melding fra UE til MME, som beskytter konfidensialiteten til brukeridentiteten. Det vil hindre at bruker blir tracket ved å observere temporære identiteter tildelt bruker etter hverandre [8].

En passiv angriper (som bare lytter) kan, etter en uventet IMSI-S-TMSI avsløring i nettet, sette brukers adferd og bevegelser mellom forskjellige aktive sesjoner i sammenheng når S-TMSI er uendret. Angriper kan dermed tracke nettverksbruker. En aktiv angriper trenger ikke en IMSI-S-TMSI avsløring, men kan fortsette sitt angrep gjennom hver idle periode når S-TMSI er kjent og uendret. Et tiltak mot denne trusselen er å reallokere S-TMSI, og sende den beskyttet av NAS-kryptering til UE ved hver overgang til aktiv tilstand [3;10]. En passiv angriper avlytter kommunikasjonen og prøver å bryte konfidensialiteten. En aktiv angriper prøver også å bryte andre sikkerhetsfunksjoner i tillegg til konfidensialitet, som for eksempel å legge til, fjerne og modifisere meldinger [8].

Reallokering av S-TMSI med NAS-kryptering ved hver overgang til aktiv tilstand, er også viktig for å forhindre tracking av bruker mellom forskjellige aktiv og idle sesjoner slik at gjeldende C-RNTI, som kan være allokert uten beskyttelse i aktiv tilstand, ikke blir koblet til den fremtidige S-TMSI etter overgang til idle tilstand [10].

Hvis ikke allokeringen av C-RNTI er konfidensialitetsbeskyttet, kan en passiv angriper linke gammel og ny C-RNTI og derav tracke nettverksbruker fra celle til celle i aktiv tilstand. På grunn av at angriper allerede kan bruke idle tilstand til sine angrep kan det bli akseptert at den innledende C-RNTI blir transportert og allokert uten konfidensialitetsbeskyttelse. Det eksisterer flere sikre C-RNTI reallokeringsløsninger, med forskjellig kompleksitet. Det er antatt at tildelingen av initial C-RNTI blir utført av eNB før det er mulig å konfidensialitetsbeskytte overføringen av C-RNTI til UE. Reallokering av C-RNTI ved bruk av RRC-kryptering er en mulighet, der C-RNTI blir transportert med konfidensialitetsbeskyttelse til UE etter aktivering av RRC-sikkerhet på radiogrensesnittet [10].

8.10.6 Trafikkanalyse

Trafikkanalyse vil si å analysere trafikksituasjonen enten mellom avsender og mottager eller bare for avsender, for å se hvor ofte det går trafikk og mengden trafikk som sendes. Endring av trafikk både i forhold til volum og intensitet kan si noe om aktiviteten mellom to endepunkter eller bare aktiviteten til avsender. Videre beskrives muligheter for trafikkanalyse på radiogrensesnittet og backhaul i EPS.

Hvis brukerdataene blir kryptert over radiogrensesnittet, vil det ikke være mulig å gjøre trafikkanalyse på radiogrensesnittet med utgangspunkt i informasjon om identiteten til avsender og mottager, da IP-adresser og routinginformasjon vil være kryptert. Selv om brukerdata er kryptert vil det kunne være en mulighet for at avsender kan bli kjent via avlytting av ”mobility

management" trafikk, dersom RRC- og NAS-signalering ikke er kryptert. Dette vil åpne for trafikkanalyse kun av avsender, hvor en ser på intensiteten til trafikken som avsender genererer. Hvis operatør krypterer RRC- og NAS-signalering, vil det allikevel være mulig å registrere aktiviteten til avsender hvis vi har en IMSI-S-TMSI avsløring i nettet og S-TMSI eller C-RNTI blir sendt i klartekst over radiogrensesnittet før kryptering av RRC-signalering er aktivert. Hvis operatør velger å ikke bruke NDS IPsec og satser på fysisk beskyttelse av backhaul og grensesnittet mellom basestasjoner vil det åpne for trafikkanalyse av avsender og mottager på disse grensesnittene avhengig av angripers ressurser.

8.10.7 Handover til dårligere beskyttet "Radio Access Technologies" (RAT)

Dette kapittelet tar blant annet for seg en sikkerhetsproblemstilling som oppstår ved en tett interaksjon mellom forskjellige RATs. Det vil bli mer vanlig i fremtiden at en mobilterminal tar handover mellom forskjellige RATs alt ettersom hvilket nett som har best dekning og kvalitet. Nettverket med dårligst sikkerhet vil utgjøre en sikkerhetstrussel for mobilterminaler som vanligvis er koblet opp mot nettverk med høyere sikkerhet. En potensiell angriper kan utnytte dette til å ramme UE når den er tilkoblet et dårligere beskyttet nettverk.

En angriper kan tvinge en LTE mobil, som også støtter andre RATs, til å ta handover til en RAT med dårligere sikkerhet for å utnytte dette. Hvis angriper har full kontroll over et system, på grunn av dårligere sikkerhet i systemet, så kan han utføre mer seriøse sikkerhetsangrep ved å få mobilterminaler som henger på andre system til å ta handover til nettverket han har kontroll over. På denne måten kan angriper utvide sitt angrep til også å gjelde UE på ellers sikre systemer. Dette betyr at et dårlig beskyttet nettverk (enhver RAT som er knyttet opp mot E-UTRAN) blir en sårbarhet ikke bare for seg selv, men også for alle andre nettverk i området [10].

8.11 Oppsummering av sårbarheter i EPS

Sårbarheten ved at MAC-laget ikke er beskyttet vil kunne føre til dårligere QoS, som kan gå utover tilgjengeligheten til nettverksbruker. De resterende sårbarhetene i LTE/EPC er avhengig av hva hver enkelt operatør velger å innføre av sikkerhetstiltak. GSM og UMTS krypterer brukerdata over radiogrensesnittet i dag og det er stor sannsynlighet for at det videreføres for LTE. Videre i oppsummeringen antas det at brukerdata er kryptert.

Manglende integritets- og replaybeskyttelse av brukerplanpakker mellom UE og eNB åpner for angrep i form av injeksjon og modifikasjon av IP-pakker uten at det blir oppdaget. Når brukerdata er kryptert vil injeksjon og modifikasjon av IP-pakker kun føre til dårligere kvalitet eller DOS angrep, som vil påvirke tilgjengeligheten til nettverksbruker.

Avlytting av "mobility management" trafikk, som kan bli sendt som RRC- og NAS-signalering, kan frembringe sensitive data relatert til brukere og nettverksoperatører. Analyse av slike data kan føre til brudd på konfidensialitet og lede til for eksempel lokalisering av nettverksbruker. Mottiltak vil være kryptering av RRC- og NAS-signalering, avhengig av sårbarhet. Hvis ikke

RRC-signaleringen blir kryptert vil det være mulig å målfølge UE basert på feltstyrkemålinger på cellenivå og kartlegging av HO.

Mobilterminalen er sårbar for ”tracking” når IMSI, GUTI, S-TMSI og C-RNTI blir sendt i klartekst over radiogrensesnittet. Tiltak mot denne sårbarheten er å reallokere de temporære UE-identitetene ved bruk av NAS- eller RRC-kryptering.

8.12 Oppsummering og konklusjon av sikkerhet i EPS

Integritetsbeskyttelse av signalering og brukerdata i EPS er obligatorisk, unntatt for brukerdata over radiogrensesnittet. Konfidensialitetsbeskyttelse av signalering og brukerdata over backhaul og X2-grensesnittet mellom basestasjoner er obligatorisk. Konfidensialitetsbeskyttelse av signalering og data over radiogrensesnittet og av signalering mellom mobilterminal og EPC er valgfritt, men anbefalt av 3GPP. Managementtrafikk over ”backhaul” er både integritets- og konfidensialitetsbeskyttet. Det er opp til operatør hvordan integritets- og konfidensialitetsbeskyttelse på backhaul og mellom basestasjoner skal realiseres, om det blir med fysisk beskyttelse av grensesnittene eller med NDS IPsec. Det er stor sannsynlighet for at kryptering av brukerdata blir innført for LTE over radiogrensesnittet, da det eksisterer i GSM og UMTS i dag. Det at konfidensialitetsbeskyttelse av signalering og brukerdata over radiogrensesnittet er valgfritt for operatør vil kunne føre til at forskjellige operatører velger forskjellige sikkerhetsløsninger.

Ny sikkerhetsarkitektur med separat beskyttelse av bruker- og kontrollplan, innføring av AS- og NAS-sikkerhet over hvert sitt grensesnitt, hyppig utregning av sikkerhetsnøkler, beskyttelse av managementtrafikk, signalering og data på backhaul og X2-grensesnittet, gjør EPS-systemet til et robust og sikkert system. Det er allikevel noe usikkerhet rundt valgfriheten av konfidensialitetsbeskyttelse for brukerdata og signalering over radiogrensesnittet, i tillegg til hvordan operatør velger å beskytte backhaul og grensesnittet mellom basestasjoner.

9 LTE-tjenester

Nøkkelelementene for at ny teknologi skal bli en suksess er nettverket, mobilterminalene og applikasjonene. LTE-nettet vil tilby høyere datahastigheter og mindre forsinkelse for brukeren, som er viktig for blant annet multimediatjenester og onlinespill. I tillegg vil eksisterende tjenester fungere bedre og raskere med LTE. Smarttelefoner og mini-PCer vil være drivere for avanserte tjenester i LTE-nettet.

I en internasjonal undersøkelse som Nokia Siemens Networks har gjennomført, referert til i Inside Telecom, kommer det frem at sosiale nettverkstjenester (Facebook, Twitter, Linkedin etc.), app stores, mobil-TV og mobil IP-telefoni er blant tjenestene som driver den eksplosive veksten i mobildata i UMTS-nettet. Eksempler på andre tjenester som er på vei inn i mobilverdenen med smarttelefonene som viktigste redskap:

- chat, blogg, dele innhold, dele medier, sende gruppemeldinger, underholdning, værvarsling, knytte seg til hjemmet, lokasjonsbaserte tjenester

LTE-mobilterminaler kommer, ifølge Inside Telecom, sannsynligvis først på markedet i 2011-2012. Før vi har LTE-mobilterminaler er det lite sannsynlig at LTE-markedet vil ta av med nye spennende tjenester. LTE vil med høy overføringshastighet og/eller lav forsinkelse være gunstig for tjenester som:

- multimediatjenester, internett radiostasjoner, nedlastning av musikk, nedlastning av tunge applikasjoner, grafikkintensivefiler
- onlinespill, ”video on demand”, mobil-TV, internett video, HD-video, videodeling, ”se hva jeg ser”, videosamtale, videokonferanse

En videosamtale bruker i dag 64kbit/s og med 100kbit/s får du en videooverføring på en liten skjerm med god kvalitet. Det betyr at med hastighetene som tilbys i UMTS-nettet i dag (1-2Mbit/s), vil både video, lokasjonsbaserte tjenester og mobil-TV fungere godt. Noen mener derfor at LTE-nettet bare vil bli et kapasitetsavlastningsnett for UMTS-nettet og ikke selv bidra til nye revolusjonerende tjenester, da ingen tenkelige tjenester trenger så store hastigheter som LTE-nettet vil tilby. Andre igjen mener at det finnes ingen grenser for hva vi kan få til av tjenester bare hastighetene blir høye nok. Sannsynligvis vil LTE-nettet både fungere som et kapasitetsavlastningsnett og bidra med nye spennende tjenester.

Alcatel-Lucent har gjennomført en markedsundersøkelse i Europa, Japan og Nord-Amerika, som startet november 2008 [16]. I markedsundersøkelsen kom det frem at brukerne ønsker raskere internettsurfing, forbedret videooppløsning og muligheten til å kjøre flere applikasjoner samtidig uten å kompromisse (multimedia tjenester). Forbrukerne regner med at det som går treigt og klossete i 3G vil gå raskere og mer smidig med LTE. Det kom frem at forbedret brukeropplevelse er en hovedmotivasjon for å velge LTE. I Europa og Japan vil brukerne også være interessert i tjenester som gir dem skreddersydd geografisk lokasjonsspesifikk informasjon på deres mobilterminaler, såkalte lokasjonsbaserte tjenester. I en undersøkelse utført av Nokia Siemens Networks i 2010, referert til i Inside Telecom, sier over halvparten av 1500 respondenter i Tyskland, Frankrike, Spania og Storbritannia at de er interessert i mobilt bredbånd med stor fart, og 30 prosent er villig til å betale for det. I utviklingsland, hvor internett ikke er utbredt og hvor en stor del av befolkningen ikke har tilgang til PC, vil mobilt bredbånd være den eneste tilgangen de får til internett.

Erfaringer viser at kundene bare ønsker høyere og høyere datahastighet fordi dette gjør brukergrensesnittet enklere for en rekke krevende applikasjoner. Utfordringen til operatørene er om de klarer å tilby dette tilstrekkelig billig.

10 Utbygging og utvikling av LTE

Dette kapittelet ser på problematikken rundt tilgang på frekvensressurser, tar for seg dekning og utbyggingsstrategier og ser på LTE-utbygging.

10.1 Frekvensressurser

Den største utfordringen fremover for å få utnyttet LTE og LTE-Advanced teknologien er tilgang på frekvenser, da store deler av frekvensbåndet er tatt i bruk. Sannsynlig må det gjøres en omprioritering av frekvenser. For at LTE og LTE-Advanced skal bli global som GSM og UMTS er det ønskelig å kunne avsette de samme frekvensene til LTE og LTE-Advanced i respektive land, eventuelt vil multiband mobilterminaler kunne brukes for roaming der koordinering av frekvensbånd ikke har lykkes. Multiband mobilterminaler er også nødvendig for at en mobilterminal kan ta handover mellom LTE og UMTS/GSM. I Norge og flere land i Europa blir den digitale dividende 790-862 MHz satt av til mobilt bredbånd. Den digitale dividende er frekvensene som ble frigitt etter digitaliseringen av TV-kanaler.

I fremtiden ser en for seg at frekvensproblematikken løses ved å koordinere frekvensene på en mer dynamisk måte, ved bruk av ”Software Defined Radio” (SDR) teknologi og konseptet ”Dynamic Frequency Broker” (DFB). Det foregår forskning på DFB på FFI i dag.

10.1.1 Frekvensbesparende teknologi og refarming

Utviklingen fra GSM, via HSCSD, GPRS, EDGE, UMTS, HSPA, HSPA+ og til LTE har gått ut på å få høyest mulig datahastighet ut av den tildelte frekvensressursen. Forskjellige teknikker kan brukes for å få til dette. Smarte antenner, adaptiv modulasjon, MIMO-teknikker og dual carrier vil bidra til høyere overføringshastigheter for UMTS/HSPA+ og LTE. HSCSD, GPRS, EDGE er utvikling av GSM-systemet, mens HSPA og HSPA+ er utvikling av UMTS-systemet.

Nokia Siemens Networks har kommet med en ny teknologi; ”Orthogonal Sub Channel” (OSC), som dobler talekanalkapasiteten i GSM/EDGE-nettet. OSC frigjør kapasitet for refarming av GSM-nettet. OSC-teknikken bruker QPSK-modulasjon i nedlink og ”orthogonal subchannels”, også kalt multi-user MIMO, i opplink. 50 % av dagens mobilterminaler støtter OSC og andelen antas å stige fremover. OSC krever bare en softwareoppgradering i radionettverket. Refarming er et begrep som brukes når en skifter teknologi i et frekvensbånd. Hvis en for eksempel bruker deler av GSM-båndet på 900 MHz til UMTS- eller LTE-teknologi kalles det refarming. Februar 2010 ble 900 MHz båndet i Norge teknologinøytralt, som åpner for muligheten for refarming. Det vil sannsynligvis bli mer vanlig med teknologinøytrale bånd, slik at operatørene selv kan bestemme hvilket system de ønsker å ha i de forskjellige frekvensbåndene.

10.2 Dekning og utbyggingsstrategier

LTE bygges først ut i 2.6 GHz båndet i byene. For å få dekning utover byene vil det være nødvendig å bruke lavere frekvenser som rekker lenger, som for eksempel digital dividende eller GSM-båndet. I første omgang vil LTE bygges ut i digital dividende, da GSM-båndet høyst sannsynlig vil brukes til å avlaste eksisterende mobilt bredbånd; UMTS. LTE vil få lavere kapasitet i distriktene, da digital dividende utgjør 1,5 LTE-kanal som igjen deles på flere operatører. På lang sikt vil GSM- og UMTS-nettene fases ut og LTE og LTE-Advanced vil ta over frekvensene.

LTE vil i starten bygges ut som små dekningsøyer innenfor dekningsområdet til UMTS/GSM-nettene. En LTE-mobilterminal vil derfor være dual eller trippelband for å kunne brukes i UMTS/GSM-nettene. Operatørene vil styre trafikk mellom GSM, UMTS og LTE avhengig av dekning, kapasitet og tjenester. Cellestørrelsen i LTE vil variere avhengig av kapasitetsbehovet i området som skal dekkes. I byer vil celleradien kunne være rundt 500m og enda lavere ved svært høyt trafikkpåtrykk. Celleradien vil øke til 5, 10 og 30km ettersom vi beveger oss til områder med mindre trafikkpåtrykk. 100 km celleradius vil mest sannsynlig bare bli brukt i spesielle tilfeller, for eksempel utover sjøen og i fjellet, hvor det er viktig å rekke langt og hvor det er færre brukere.

Sannsynlig vil flere operatører velge å samarbeide om utbygging av LTE i tiden fremover, da inntektene fra mobilt bredbånd ennå ikke dekker utgiftene med utbygging. Det kan enten skje ved at mobiloperatører danner nye selskaper sammen eller samarbeid rundt nettverksdeling.

10.3 Backhaul

Den største flaskehalsen og de største kostnadene med hensyn til utbygging av LTE og mobilt bredbånd er ”backhaul”, det vil si transmisjon fra basestasjonen og inn i nettet. Med samlet hastighet på over 100 Mbit/s i cella og med flere celler på en site vil bare fiber kunne fungere som” backhaul”. Det er dyrt og tar tid og føre frem fiber til en mobilsite. Radiolinjeforbindelse med høy kapasitet vil også kunne være aktuell som ”backhaul” noen steder.

10.4 Femtoceller

Femtocelle er en liten celle med en liten basestasjon (HeNB) som kan monteres hjemme, i hot spots i kafé, restaurant, shoppingsentre, flyplasser eller i et bedriftslokale. Det finnes to typer femtoceller; ”home femto cell” som tar 4 samtidige samtaler og ”business femto cell” som tar 16 samtidige samtaler. Privatpersoner kan kjøpe en femtocelle for å få bedre dekning og høyere kapasitet hjemme hos seg selv, og de bruker da egen bredbåndsforbindelse som ”backhaul”. Femtocella vil være koblet opp mot et av mobilnettene, slik at operatøren tar ansvaret for kvaliteten på cella og det vil være mulig å ta handover fra femtocella og inn i det eksisterende mobilnettet. I byer hvor inntrengningstapet er betydelig vil det bli behov for femtoceller for å oppnå høye hastigheter innendørs. Femtoceller vil bli en kapasitetsavlastning for operatøren sitt nett. Network Norway lanserte 14. februar 2011, som en av de første i verden, selvkonfigurerende femtoceller for bedriftsmarkedet i UMTS-nettet. Med femtoceller oppstår det et sikkerhetsaspekt da andre enn operatøren har tilgang til basestasjonen. Sikkerheten på ”backhaul” vil også bli en

utfordring, da bredbåndslinken fra bruker til EPC vil gå over internett og ses dermed på som en upålitelig forbindelse, for mer info om sikkerhet for HeNB se [8]. Hvis operatør velger å bruke NDS IPsec på ”backhaul”, vil det beskytte brukerdata og signalering på ”backhaul” til HeNB.

10.5 LTE-utbygging

Det er stor satsning på LTE per dags dato i Europa, Nord-Amerika og Asia. Satsningen på LTE begrunnes, ifølge Inside Telecom, først og fremst med at standarden skal gjøre det billigere per megabyte for mobiloperatørene å produsere mobilt bredbånd, i tillegg til at den skal levere lavere forsinkelse og høyere båndbredder til kundene. Netcom i Oslo og TeliaSonera i Stockholm, som bygger ut i 2,6 GHz båndet, var de første i verden til å lansere LTE i 2009. Mange operatører velger LTE på grunn av sømløs mobilitet mellom GSM, 3G/HSPA og LTE. God samvirkning er en stor fordel fordi LTE bygges i første omgang ut i små dekningsøyer innenfor GSM/UMTS-nettene. Da vil en effektiv overgang mellom nettene være svært viktig når vi beveger oss inn og ut av LTE-dekning. ”The Global mobile Suppliers Association” (GSA) informerer om at 17 LTE-nett ble satt i drift i 2010 og minst 45 er forventet satt i drift i 2012. 180 operatører i 70 land investerer i LTE, hvorav det er gjort forpliktende løfter for utbygging av 128 LTE-nett i 52 land.

11 LTE-Advanced

Det er først med LTE-Advanced og 100 MHz båndbredde at vi virkelig kan begynne å snakke om 4G, ut fra definisjonene på overføringshastigheter, forsinkelse osv som er satt som krav til 4G-teknologien. LTE-Advanced er ikke noe nytt system, men en videreføring og forbedring av LTE, i tillegg til at båndbredden økes betraktelig. LTE-Advanced kan til en viss grad utnytte frekvensressurser som ikke ligger ved siden av hverandre, for å gjøre det mulig å oppnå 100 MHz båndbredde. Ved å utnytte en del teknikker, ny teknologi og 100 MHz båndbredde vil LTE-Advanced kunne gi betydelig høyere overføringshastigheter enn LTE. Teoretiske datahastigheter for LTE-Advanced er 1 Gbit/s i nedlink (100 Mbit/s for høy mobilitet) og 500 Mbit/s i opplink [3;4]. LTE-Advanced vil også redusere investerings- og driftsutgifter betraktelig. 3GPP jobber nå med LTE-Advanced standarden i ”release” 10 og utforsker blant annet ”Carrier Aggregation”, videreutviklede ”Uplink and Downlink Transmission Scheme”, ”Coordinated Multipoint Transmission and Reception” (CoMP), interferenskoordinasjon og repeaterforsterkning [17]. Sannsynligvis vil også høyere ordens modulasjonsmetoder bli vurdert, hvor utfordringen blir enda strengere restriksjoner på RF-komponentene i sendere og mottakere. Utfordringen til LTE-Advanced blir å levere disse forbedringene uten en uakseptabel økning i utstyrskostnad. Innholdet i dette kapittelet er i hovedsak hentet fra [3], [17], [18] og [19].

11.1 Carrier Aggregation

“Carrier aggregation” er veldig viktig for å kunne møte kravene til hastigheter som er satt for LTE-Advanced. “Carrier aggregation” vil si å legge sammen frekvensblokker utover 20MHz, slik at det er mulig å oppnå 100 MHz båndbredde. For å beholde kompatibilitet bakover mot LTE, vil to eller flere bærefrekvensblokker á 20 MHz bli lagt sammen. Det er mulig å legge sammen frekvensblokker som ligger ved siden av hverandre i samme bånd, adskilt i samme bånd eller

adskilt i forskjellige bånd. For å utnytte frekvensspekteret enda mer fleksibelt, ses det også på mulighet for å legge til en bærefrekvensblokk som er mindre enn 20 MHz, men det må alltid være minst en bærefrekvensblokk á 20 MHz for å beholde kompatibiliteten bakover mot LTE.

11.2 Uplink Transmission Scheme

For å oppnå ønsket spektraleffektivitet i opplink for LTE-Advanced, må MIMO innføres på opplink. Det vil sannsynlig bli minst to senderantenner i mobilterminalene og for ”Singel User Uplink MIMO” (SU-UL-MIMO) vil også romlig multipleksing (SM) med 4 lag bli vurdert. Det at SC-FDMA, med lav PAPR, blir brukt i opplink kan føre til at gevinsten ved bruk av romlig multipleksing blir redusert. Derfor forskes det også på MIMO-teknikker som går bedre sammen med lav PAPR. MIMO-transmisjon kan bli delt inn i teknikker som baserer seg på prinsippet ”channel reciprocity” eller ”channel non-reciprocity”. Blant teknikkene som baserer seg på ”channel reciprocity” er ”Beamforming” (BF) og ”Multi-user MIMO” (MU-MIMO). Basestasjonen bruker da et lydreferansesignal fra UE til å bestemme radiokanalen og antar at radiokanalen er lik for både eNB og UE (”channel reciprocity”). Basestasjonen former antennelober etter informasjon om radiokanalen, slik at radiosignalene fra UE får best mulig mottak.

”Channel non-reciprocity” teknikker kan deles inn i ”open-loop” MIMO (OL-MIMO), ”closed-loop” MIMO (CL-MIMO) og MU-MIMO. OL-MIMO blir brukt når senderen ikke har noen informasjon om kanalen; ”Channel-State Information” (CSI). Siden UE ikke har noen informasjon om CSI fra eNB vil OL-MIMO-teknikkene ikke kunne bli optimalisert for UE sin radiokanal sett fra eNB-mottakeren, men de er robuste for kanalendringer. Disse teknikkene egner seg derfor veldig godt for mobilterminaler med høy hastighet. I tilfeller hvor eNB sender CSI til UE vil CL-MIMO kunne bli brukt for å øke spektraleffektiviteten betraktelig. CL-MIMO bruker CSI-feedback fra eNB til å optimalisere overføringen over en spesifikk UE radiokanal. Siden CL-MIMO er avhengig av CSI-feedback, blir den sårbar for kanalvariasjoner. Generelt kan vi si at CL-MIMO gir bedre ytelse enn OL-MIMO for UEer som beveger seg med lav hastighet, men har dårligere ytelse enn OL-MIMO for UEer som beveger seg med høy hastighet. Videre vil bruk av MU-MIMO kunne øke spektraleffektiviteten ytterligere [17].

11.3 Downlink Transmission Scheme

For høyere ytelse på nedlinken i LTE-Advanced studeres nå romlig multipleksing (SM) med 8 lag og en forbedring av MU-MIMO. Hvis CA blir brukt vil en kunne bruke SM med 8 lag per ”carrier component”. For nedlink MU-MIMO kan de nye teknikkene som studeres klassifiseres i to kategorier; faste antennelober og brukerspesifikke antennelober. For MU-MIMO med faste antennelober vil basestasjonen bli konfigurert til å sende multiple faste lober, mens fordeleren allokerer en bestemt bruker til en passende antennelobe for å oppnå best mulig ytelse. Denne teknikken er godt egnet for UEer med høy mobilitet. For brukerspesifikke antennelober vil lobene bli produsert for hver bruker adaptivt etter brukerens individuelle CSI. Teknikken med brukerspesifikke antennelober vil gi bedre ytelse enn faste antennelober på grunn av bedre ”Signal-to-Interference plus Noise Ratio ” (SINR), som er et resultat av bedre lobestyring og

interferensundertrykkelse. Den er imidlertid avhengig av at UE gir CSI til eNB, og at radiokanalen endrer seg minimalt mellom CSI-måling og dataoverføring. Derfor vil teknikken med brukerspesifikke antennelober egne seg best for UEer med lav til moderat hastighet [17].

11.4 Coordinated Multi-Point transmission/reception (CoMP)

Bruk av CoMP vil forbedre dekning og ytelse i celleranden. Når UE er i celleranden, vil den sannsynligvis kunne motta signaler fra flere basestasjoner og UE sine signaler vil kunne bli mottatt av flere basestasjoner. Hvis signalene som UE mottar fra de forskjellige basestasjonene blir koordinert, vil det kunne forbedre ytelsen på nedlink betydelig. Denne koordineringen kan være enkel ved bruk av teknikker som fokuserer på å unngå interferens, eller mer kompleks hvor like data blir sendt fra flere basestasjoner. I det siste tilfelle blir det en form for makro-nedlinkdiversitet. Hvis de forskjellige basestasjonene koordinerer ressursfordelingen (scheduling) til UE i opplink, vil systemet kunne dra nytte av multippel mottaking for å øke ytelsen på radioforbindelsen betraktelig. Det er en form for makro-opplinkdiversitet.

En enklere form av CoMP baserer seg på at basestasjonene koordinerer ressurshåndtering seg imellom for å kontrollere interferens mellom cellene. Dette er en effektiv måte å øke spektraleffektiviteten i celleranden på. Utvikling av metoder for ”Inter-Cell Interference Coordination” (ICIC) i LTE-Advanced kan bli delt inn i ”Dynamic Interference Coordination” (D-ICIC) og ”Static Interference Coordination” (S-ICIC). Frekvensressurser, romlige ressurser (“beam pattern”) og effektressurser blir delt dynamisk mellom basestasjonene i D-ICIC. For S-ICIC vil statisk og semistatisk romlig ressurskoordinering mellom basestasjoner bli vurdert [17].

11.5 Relay Node

Konseptet med en ”Relay Node” (RN) er blitt introdusert i LTE-Advanced for å muliggjøre videresending av trafikk og signalering mellom eNB og UE til områder med dårligere dekning. En RN vil bedre dekningen i området og med bedre S/N vil vi få høyere overføringshastigheter. Sannsynligvis vil det være mest aktuelt å bruke RN for å forbedre innendørsdekning. RN kan også benyttes for å bedre dekning og ytelse i randsonen av cella, områder som ligger i radioskygge og for å utvide celledekningen.

RN-noden er knyttet opp mot en moderbasestasjon og kan enten fungere som en basestasjon eller som en repeater som bare forsterker signalet. Hvis RN-noden fungerer som en basestasjon, bruker den radioaksessen til moderbasestasjonen som ”backhaul”. Den kan da enten bruke aksessfrekvensene til moderbasestasjonen, eller den kan bruke egne frekvenser satt av for dette formålet. En ulempe med RN er nettopp at den bruker frekvensressurser til ”backhaul”, slik at det kan gå mindre trafikk på moderbasestasjonen. Når trafikken på moderbasestasjonen øker slik at den trenger alle frekvensressursene til aksess, vil det være mulig å anvende andre backhaul-alternativer for RN. Da vil RN-noden ikke lenger være knyttet opp mot moderbasestasjonen og sannsynligvis vil det i slike tilfeller heller lønne seg med små basestasjoner i utgangspunktet.

GSM og UMTS bruker repeater for å forbedre dekning i tunnel og skyggeområder. Operatører har hatt vanskeligheter med å inkludere repeaterkonseptet i radioplanleggingsverktøyet sitt, noe som gjør det praktisk vanskelig å bruke i stor skala. I litteraturen blir RN-noder sett på som et viktig virkemiddel for å nå kravene til 4G. Det er allikevel usikkert hvor mye det vil bli brukt tatt i betraktning ulempene med frekvensbruk og radioplanlegging. Femtoceller vil sannsynligvis konkurrere med RN-noder for bedring av innendørsdekning.

11.6 Sikkerhetsutfordringer

Det er først med LTE-Advanced at vi får en 4G-arkitektur. Det vil ikke være store forskjeller på aksessikkerhetsarkitekturen til LTE og LTE-Advanced [12]. Innføring av ”Relay Node” (RN) i LTE-Advanced arkitekturen vil ha en innvirkning på LTE-sikkerhet.

RN vil enten fungere i rollen som en basestasjon eller som en repeater, begge deler vil kunne påvirke sikkerheten i LTE-systemet. Når RN fungerer som en basestasjon vil S1-signaltrafikk gå i DRBer mellom donorbasestasjonen og RN. S1-signaltrafikken må integritetsbeskyttes, og da trafikk som går i DRBer over radiogrensesnittet vanligvis ikke er integritetsbeskyttet, vil dette skape sikkerhetsutfordringer som må løses. En løsning er å tillate integritetsbeskyttelse på noen DRBer over radiogrensesnittet mellom donorbasestasjon og RN, men det vil igjen gå imot ønsket om mest mulig likhet på de to radiogrensesnittene. En annen løsning er å bruke IPsec til å beskytte IP-trafikken over grensesnittet mellom donorbasestasjon og RN. I så fall må det bli bestemt hvordan IP-lagssikkerhet skal fungere sammen med PDCP-lagssikkerhet.

Når RN-noden fungerer som en repeater vil forbindelsen mot moderbasestasjonen bli satt opp på en liknende måte som med en UE. I oppstart kommuniserer RN med en MME (som kan være forskjellig fra MME til UE) og i dette tilfellet vil S1-signaleringstrafikken gå mellom moderbasestasjonen og MME som server RN-noden. Vi får derfor ikke samme sikkerhetsutfordring som over. Imidlertid vil det bli en sikkerhetsutfordring at RN-noden vil måtte inneholde en USIM eller lignende funksjonalitet. En USIM i en RN er lettere tilgjengelig enn en USIM i en UE som er kontrollert av menneskelige brukere. USIM i RN-noden vil kunne bli fjernet av en angriper og plassert i en annen RN-node eller i en UE. Det er nødvendig å studere potensielle trusler og mottiltak i dette tilfellet [8].

12 Oppsummering

LTE er et nytt mobilt bredbåndsystem som bygges ut som et eget nett etter UMTS-nettet. LTE/EPC vil gi høyere datahastigheter, forbedret spektraleffektivitet og redusert forsinkelse. LTE lover teoretisk hastighet på 100 Mbit/s på nedlink og 50 Mbit/s på opplink med 20 MHz båndbredde, mens det i praksis er mer realistisk med 10-20 Mbit/s på nedlink og 5-10 Mbit/s på opplink. Det er først med LTE-Advanced at vi får et reelt 4G-system med teoretiske hastigheter på opptil 1000 Mbit/s på nedlink og 500 Mbit/s på opplink uten mobilitet (100 MHz båndbredde).

LTE benytter en helt ny radioaksessteknologi, OFDM. OFDM-teknologien ble valgt blant annet fordi den er robust mot ”Intersymbol Interference” (ISI). OFDM-teknologien vil dessuten sammen med bruk av MIMO føre til en mer effektiv spektrumsutnyttelse sammenlignet med HSPA. EPC er et rent pakkesvitsjet IP-basert kjernenettverk, hvor det er lagt vekt på en enkel og flat IP-struktur som bidrar til redusert forsinkelse.

Integritetsbeskyttelse av signalering og brukerdata i EPS er obligatorisk, unntatt for brukerdata over radiogrensesnittet. Konfidensialitetsbeskyttelse av signalering og brukerdata over backhaul og X2-grensesnittet mellom basestasjoner er obligatorisk. Konfidensialitetsbeskyttelse av signalering og data over radiogrensesnittet og av signalering mellom mobilterminal og EPC er valgfritt, men anbefalt av 3GPP. Managementtrafikk over ”backhaul” er både integritets- og konfidensialitetsbeskyttet. Det er opp til operatør hvordan integritets- og konfidensialitetsbeskyttelse på backhaul og mellom basestasjoner skal realiseres, om det blir med fysisk beskyttelse av grensesnittene eller med NDS IPsec. Det er stor sannsynlighet for at kryptering av brukerdata blir innført for LTE over radiogrensesnittet, da det eksisterer i GSM og UMTS i dag. Det at konfidensialitetsbeskyttelse av signalering og brukerdata over radiogrensesnittet er valgfritt for operatør vil kunne føre til at forskjellige operatører velger forskjellige sikkerhetsløsninger.

Ny sikkerhetsarkitektur med separat beskyttelse av bruker- og kontrollplan, innføring av AS- og NAS-sikkerhet over hvert sitt grensesnitt, hyppig utregning av sikkerhetsnøkler, beskyttelse av managementtrafikk, signalering og data på backhaul og X2-grensesnittet, gjør EPS-systemet til et robust og sikkert system. Det er allikevel noe usikkerhet rundt valgfriheten av konfidensialitetsbeskyttelse for brukerdata og signalering over radiogrensesnittet, i tillegg til hvordan operatør velger å beskytte backhaul og grensesnittet mellom basestasjoner.

LTE-Advanced er en videreutvikling av LTE, hvor mer båndbredde og bruk av forskjellige teknikker og ny teknologi gir betydelig høyere hastigheter. Det vil sannsynligvis ikke være store forskjeller på aksessikkerhetsarkitekturen til LTE og LTE-Advanced, selv om innføring av RN-node vil tilføre nye sikkerhetsutfordringer som må løses.

Den største utfordringen for LTE og LTE-Advanced er tilgang på frekvenser. LTE vil med noen unntak først bli bygget ut på 2,6 GHz i byer, og senere vil ”digital dividende” og GSM-båndet

benyttes for å dekke mer grisgrendte strøk. ”Backhaul” er den største flaskehalsen og gir de største kostnadene ved utbygging av LTE. Bare fiber vil fungere som ”backhaul”. Det er kostbart og tar tid å føre fiber frem til basestasjonene.

Det er stor interesse for å bygge ut LTE over store deler av verden, hvor den største satsningen per dags dato er i Europa, Nord-Amerika og Asia. ”The Global mobile Suppliers Association” (GSA) informerer om at 17 LTE-nett ble satt i kommersiell drift i 2010 og minst 45 er forventet satt i drift i 2012. Det er gjort forpliktende løfter for utbygging av 128 LTE-nett i 52 land.

LTE vil fungere godt for tjenester som krever høy overføringshastighet og/eller lav forsinkelse, som blant annet multimediatjenester og online spill. Erfaringer viser at kundene ønsker høyere og høyere datahastighet fordi dette gjør brukergrensesnittet enklere for en rekke krevende applikasjoner. Den største utfordringen for operatørene er å klare å tilby dette tilstrekkelig billig.

Referanser

[1] B. H. Farsund, "WIMAX - teknologi, funksjonelle egenskaper og sikkerhet," FFI-rapport 01347: 2010.

[2] "LTE / SAE System Overview," apis kurs: 2009.

[3] S. Sesia, I. Toufik, and M. Baker, "LTE - The UMTS Long Term Evolution," WILEY: 2009.

[4] H. Holma and A. Toskala, "LTE for UMTS - OFDMA and SC-FDMA Based Radio Access," WILEY: 2009.

[5] D. Astély, E. Dahlman, A. Furuskär, Y. Jading, M. Lindström, and S. Parkvall, "The Evolution of Mobile Broadband," IEEE Communications Magazine: 2009.

[6] A. Simonsson and A. Furuskär, "Uplink Power Control in LTE - Overview and Performance,". Ericsson Research, Ed. IEEE: 2008.

[7] A. M. Rao, "Reverse Link Power Control for Managing Inter-cell Interference in Orthogonal Multiple Access Systems,". Alcatel-Lucent, Ed. IEEE: 2007.

[8] D. Forsberg, G. Horn, W.-D. Moeller, and V. Niemi, "LTE Security," Wiley, 2010.

[9] 3GPP, "3GPP Technical Specification 23.401 v10; GPRS enhancements for E-UTRAN access (Release 10)," www.3gpp.com: 2010.

[10] 3GPP, "3GPP Technical Report 33.821 V9 - Rationale and track of security decisions in LTE/SAE," 2009.

[11] 3GPP, "3GPP Technical Specification 33.401 V9.2.0 - SAE Security architecture," 2009.

[12] G. M. Køien, "Access Security in 3GPP-based Mobile Broadband Systems," Telektronikk 1, 2010.

[13] R. Blom, K. Norrman, M. Naslund, S. Rommer, and B. Sahlin, "Security in the Evolved Packet System," Ericsson Whitepaper, 2010.

[14] Agilent Technologies, "LTE and the Evolution to 4G Wireless - Design and Measurement Challenges," www.agilent.com: 2009.

[15] G. M. Køien, "Entity Authentication and Personal Privacy in Future Cellular Systems," River Publishers, 2009.

[16] J. Power and D. Callagher-Carpenter, "Developed and Emerging Markets Readying for LTE,". Alcatel-Lucent, Ed. enriching communications, 2009.

[17] "3GPP Mobile Broadband Innovation Path to 4G: Release 9, Release 10 and beyond - HSPA+, LTE/SAE and LTE-Advanced,". 3G americas, Ed. 2010.

[18] "The Mobile Broadband Evolution - HSPA+, SAE/LTE and LTE-Advanced,". 3G americas, Ed. 2009.

[19] "Transition to 4G - 3GPP Broadband Evolution to IMT-Advanced,". 3G americas, Ed.

Forkortelser

3GPP – 3rd Generation Partnership Project
ACK – Acknowledgement
AES – Advanced Encryption Standard
AK – Anonymity Key
AKA – Authentication and Key Agreement
ARQ – Automatic Repeat Request
AS – Access Stratum
ASME – Access Security Management Entity
AUC – Authentication Center
BCCH – Broadcast Control Channel
CA – Carrier Aggregation
CBC – Cipher Block Chaining
CCCH – Common Control Channel
CDM – Code Division Multiplexing
CDMA – Code Division Multiple Access
CK – Ciphering Key
CL-MIMO – Closed-loop MIMO
CoMP – Coordinated Multipoint Transmission and Reception
CP – Control Plane
CP – Cyclic Prefix
CQI – Channel Quality Indicatior
C-RNTI – Cell Radio Network Temporary Identifier
CSI – Channel State Information
DCCH – Dedicated Control Channel
DFB – Dynamic Frequency Broker
DFT – Discrete Fourier Transform
D-ICIC – Dynamic Interference Coordination
DL-SCH – Downlink Shared Channel
DoS – Denial of Service
DRB – Data Radio Bearer
DSP – Digital Signal Processor
DTCH – Dedicated Traffic Channel
ECM – EPS Connection Management
EDGE – Enhanced Data Rates for GSM Evolution
EEA – EPS Encryption Algorithm
EIA – EPS Integrity Algorithm
EKOM – Elektronisk Kommunikasjon
EMM – The EPS Mobility Management protocol
eNB – Evolved NodeB (basestasjon i LTE)
EPC – Evolved Packet Core
EPS – Evolved Packet System
EPS-AKA – EPS Authentication and Key Agreement

ESM – The EPS Session Management protocol
ESP – Encapsulating Security Payload
E-UTRA – Evolved UTRA
E-UTRAN – Evolved UTRAN
FDD – Frequency Division Duplexing
FDM – Frequency Division Multiplexing
FFT – Fast Forier Transform
FTP – File Transfer Protocol
GBR – Guaranteed Bit Rate
GERAN – GSM EDGE Radio Access Network
GPRS – General Packet Radio Service
GSA – The Global mobile Suppliers Association
GSM – Global System for Mobile Communication
GTP – GPRS Tunneling Protocol
GUMMEI – Globally Unique MME Identifier
GUTI – Global Unique Temporary UE identity
HARQ – Hybrid Automatic Repeat Request
HeNB – E-UTRAN basestasjon i en femtocelle
HII – High-Interference Indicator
HO – Handover
HSCSD – High-Speed Circuit-Switched Data
HSDPA – High-Speed Downlink Packet Access
HSPA – High-Speed Packet Access
HSPA+ – Evolved High-Speed Packet Access
HSS – Home Subscriber Server
ICI – Inter-Carrier Interference
ICIC – Inter-Cell Interference Coordination
IFFT – Invers Fast Forier Transform
IK – Integrity Key
IKE – Internet Key Exchange
IMS – IP Multimedia Subsystem
IMSI – International Mobile Subscriber Identity
IP – Internet Protocol
IPsec – Internet Protocol Security
ISI – Intersymbol Interference
K – hemmelig nøkkel
K_{ASME} – Access Security Management Entity Key
K_{eNB} – eNB basis nøkkel
K_{eNB*} - eNB Handover Transition Key
K_{NASenc} – NAS encryption Key
K_{NASint} – NAS integrity Key
K_{RRCenc} – Encryption Key for RRC Signaling
K_{RRCint} – Integrity Key for RRC Signaling

KSI – Key Set Identifier
KSI$_{ASME}$ – nøkkelidentifikator som identifiserer K$_{ASME}$ og nøkler utledet fra den
K$_{UPenc}$ – Encryption Key for User Plane
LTE – Long Term Evolution
LTE-Advanced – 4G nettet som kommer etter LTE
MAC – Medium Access Control
MAC – Message Authentication Code
MBR – Maximum Bit Rate
MCC – Mobile Country Code
MIMO – Multiple Input Multiple Output
MISO – Multiple Input Single Output
MME – Mobility Management Entity
MNC – Mobile Network Code
MRC – Maximum Ratio Combining
M-TMSI – M-Temporary Mobile Subscriber Identity
MU-MIMO – Multi User MIMO
NAS – Non Access Stratum
NDS/IP – Network Domain Security over IP layers
NH – Next Hop
NodeB – basestasjon i UMTS
OFDM – Orthogonal Frequency Division Multiplexing
OFDMA – Orthogonal Frequency Division Multiple Access
OI – Overload Indicator
OL-MIMO – Open-loop MIMO
PAPR – Peak to Average Power Ratio
PCCH – Paging Control Channel
PCEF – Policy Control Enforcement Function
PCRF – Policy and Charging Rules Function
PDCP – Packet Date Convergence Protocol
PDCSH – Physical Downlink Shared Channel
PDN – Packet Data Network
P-GW – Packet Data Network Gateway
PLMN – Public Land Mobile Network
PRB – Physical Resource Block
PS HO – Packet Switched Handover
PUSCH – Physical Uplink Shared Channel
QAM – Quadrature amplitude modulation
QoS – Quality of Service
QPSK – Quadrature phase-shift Keying
RAT – Radio Access Technology
RES – Response
RLC – Radio Link Control
RN – Relay Node

RNC – Radio Network Controller
RNTP – Relative Narrowband Transmit Power
ROHC – Robust Header Compression
RRC – Radio Resource Control
RTP – Reliable Transport Protocol
S1AP – S1 Application Protocol
S/N – Signal to Noise ratio
SA3 – 3GPP Specification group of Security
SAE – System Architecture Evolutio
SC-FDMA – Single Carrier Frequency Division Multiple Access
SDR – Software Defined Radio
SEG – Security Gateway
S-GW – Serving Gateway
S-ICIC – Static Interference Coordination
SIMO – Single Input Multiple Output
SINR – Signal-to-Interference plus Noise Ratio
SISO – Single Input Single Output
SM – Spatial Multiplexing
SNid – Serving Network identity
SQN – Sequence Number
SRB – Signalling Radio Bearer
STC – Space-Time Coding
S-TMSI – System Architecture Evolution-Temporary Mobile Subscriber Identity
SU-MIMO – Single User MIMO
SU-UL-MIMO – Singel User Uplink MIMO
TA – Tracking Area
TCP – Transmission Control Protocol
TDD – Time Division Duplexing
UDP – User Datagram Protocol
UE – User Equipment
UICC – Universal Integrated Circuit Card
UL-SCH – Uplink Shared Channel
UMTS – Universal Mobile Telecommunication System
UP – User Plane
USB – Universal Serial Bus
USIM – Universal Subscriber Identity Module
UTRAN – Universal Terrestrial Radio Access Network
VoIP – Voice over IP
WCDMA – Wideband Code Division Multiple Access
WiMAX – Worldwide Interoperability for Microwave Access
XRES – expected Response