NTNU
Det skapende universitet

Posisjonsinnhenting og geografisk ruting

Demonstrator av nødmeldetjeneste for "Trådløse Trondheim"

Hallstein Brøtan
Stian Landsnes

Master i kommunikasjonsteknologi
Oppgaven levert: Juni 2007
Hovedveileder: Steinar Andresen, ITEM

Norges teknisk-naturvitenskapelige universitet
Institutt for telematikk

Oppgavetekst

Bruk av VoIP øker stadig, og utviklingen går mot økt transport av tale over IP-nettverk. Slik IP-nettet fungerer i dag, behøver det ikke være noen sammenheng mellom IP-adresse og lokasjon til klienten. Denne begrensningen vanskeliggjør bruk av lokasjonsbaserte tjenester.

Nødmeldetjenester er avhengig av lokasjonen til klienten. Det er derfor nødvendig å finne metoder for å kunne avdekke denne lokasjonen. Ved å bruke Trådløse Trondheim som nettverksplattform skal vi studere foreslått arkitektur, og eventuelt foreslå forbedringer.

I tillegg skal vi utarbeide et utkast for en fleksibel løsning for en modifisert SIP-klient i terminalen til brukeren, der posisjondata sendes med anropet. En slik løsning vil også kunne anvendes for sivile formål basert på lokasjon, for eksempel bestilling av drosje og pizza, samt navigering og finne nærmeste tilbyder av en tjeneste eller et produkt.

Oppgaven gitt: 17. januar 2007
Hovedveileder: Steinar Andresen, ITEM

Forord

Denne diplomoppgaven er skrevet i løpet av vårsemesteret 2007, som avsluttende del av masterutdanningen ved Norges Teknisk-Naturvitenskapelige Universitet - NTNU. Hele arbeidet er utført ved Institutt for telematikk, Fakultetet for informasjonsteknologi, matematikk og elektronikk. Oppgaven ble foreslått av professor Steinar H. Andresen, som også har medvirket som faglærer og veileder.

Bakgrunnen for at vi valgte oppgaven var at vi begge hadde lyst til å gjøre noe praktisk arbeid, i tillegg til det teoretiske. I løpet av de tjue ukene vi har arbeidet med oppgaven har vi utviklet en demonstrator for et nødmeldesystem i Trådløse Trondheim. Det har vært inspirerende å jobbe med noe som har stor nytteverdi for samfunnet. I dette arbeidet har vi tatt i bruk diverse teknologier og innretninger som også har vært spennende å jobbe med. Spesielt interessant har det vært å få nærmere innblikk i, og bedre forståelse av, hvordan Trådløse Trondheim fungerer.

Vi vil gjerne benytte anledningen til å takke professor Steinar H. Andresen ved Institutt for telematikk for engasjement og veiledning. Han har gjennom hele prosessen kommet med mange innspill og gode ideer. I tillegg vil vi takke Ruter-Tore for utlån av kaffetrakter.

Hallstein Brøtan

Stian Landsnes

Innhold

Figurer

Tabeller

Kodeeksempler

Forkortelser

3GPP	3rd Generation Partnership Project
A-GPS	Assisted GPS
AMK	Akutt Medisinsk Kommunikasjonssentral
ATA	Analog Telephone Adapter
ATIS	Alliance for Telecommunications Industry Solutions
CLA	Cisco Location Applicance
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
E-CSCF	Emergency Call Session Control Function
E911	Enhanced 911 (emergency)
ECRIT	Emergency Context Resolution with Internet Technologies
ECRS	Emergency Call Routing Support
EMTEL	Emergency Telecommunications
ERC	Emergency Response Center
ERDB	Emergency Reference Database
ESINet	Emergency Service IP Network
ETSI	European Telecommunications Standards Institute
FCC	Federal Communications Commission
FMK	Fast Mobil Konvergens
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
GSM	Global System for Mobile Communications
HELD	HTTP Enabled Location Delivery
IETF	Internet Engineering Task Force
IMS	IP Multimedia Core Network Subsystem
IP	Internet Protocol
IP-CAN	IP Connectivity Access Network
ISP	Internet Service Provider
ITU	International Telecommunication Union
LCP	Location Configuration Protocol
LIS	Location Information Server
LLDP-MED	Link Layer Discovery Protocol for Media Endpoint Devices
LoST	Location to Service Translation
LRF	Location Retrieval Function
MAC	Media Access Control
MMoIP	Multi-Media Over Internet Protocol
NAP	Network Access Point

NENA	National Emergency Number Association
NG9-1-1	Next Generation 9-1-1
NGN	Next Generation Network(s)
NRDB	Nasjonal Referansedatabase
P-CSCF	Proxy Call Session Control Function
PIDF	Presence Information Data Format
POTS	Plain Old Telephone Service/System
PSAP	Public Safety Answering Point
PSTN	Public Switched Telephone Network
RTP	Real-Time Transport Protocol
S-CSCF	Serving Call Session Control Function
SDP	Session Description Protocol
SIP	Session Initiation Protocol
UDP	User Datagram Protocol
UE	User Equipment (terminal)
UMTS	Universal Mobile Telecommunications System
URI	Uniform Resource Identifier
URL	Universal Resource Locator
URN	Uniform Resource Name
UTM	Universal Transverse Mercator
VoIP	Voice over IP
WGS84	World Geodetic System 1984
WiFi	Wireless Fidelity (IEEE 802.11b wireless networking)
WLAN	Wireless Local Area Network

Definisjoner

AMK-sentralen	Medisinsk nødsentral ansvarlig for å behandle nødanrop.
Arkitektur	Systemets oppbygning, samhandling og funksjonalitet.
Bruker	Person som anvender en tjeneste.
Brukerklient	Programvare på terminal benyttet av brukeren
Brukerterminal	(se terminal)
Klient	Komponent i en klient-server arkitektur som sender forespørsler. Brukes ofte for brukerklient, bruker og terminal.
Lokasjon	(se posisjon)
Lokasjonsdata	(se lokasjonsinformasjon)
Lokasjonsdatabase	Referanseliste med lokasjon tilknyttet en nettverksadresse
Lokasjonsinformasjon	En samling lokasjonsparametre
Lokasjonskilde	Komponent i arkitekturen som anskaffer lokasjon.
Lokasjonsmegler	Komponent i arkitekturen som behandler lokasjonsforespørsler på vegne av klienten. Lokasjonsmegleren finner lokasjonen ved å forespørre en lokasjonskilde. Lokasjonsinformasjon returneres tilbake til klienten.
Lokasjonsparameter	En attributt som beskriver en type lokasjonsinformasjon (for eksempel koordinater)
Lokasjonsregister	(se lokasjonsdatabase)
Lokasjonstjeneste	Komponent i arkitekturen som tilbyr klienten lokasjonsinformasjon. Brukes både for lokasjonskilde og lokasjonsmegler
NAP MAC	Nettverksaksesspunktets MAC-adresse (uavhengig av nettverk).
Nødanrop	Forespørsel til en nødsentral fra en bruker i en nødsituasjon.
Nødmeldesystem	Overordnet struktur for behandling av nødanrop.
Nødmeldetjeneste	Den delen av nødmeldesystemet sett fra klientsiden.
Posisjon	Angir hvor en bruker/terminal befinner seg (synonymt med lokasjon).
PSAP	Nødsentral som mottar nødanrop. (For eksempel AMK-sentralen).
SOS-agent	Mellomliggende programvare som behandler nødanrop på klientsiden
Terminal	Den elektroniske innretningen brukeren benytter til kommunikasjon.

Sammendrag

Nødtelefoni er en allmenn tjeneste for tilkalling av hjelp fra sentraliserte nødsentraler i nødsituasjoner. En nødsentral er avhengig av brukerens lokasjon for å kunne tilby hjelp på en mest mulig effektiv måte. Nødsentralene har ett felles nummer, så brukerlokasjonen er nødvendig for å viderekoble anropet til riktig nødsentral. Utviklingen viser økt bruk av IP-basert telefoni (VoIP), og et moderne nødmeldesystem må være i stand til å håndtere IP-baserte nødanrop på lik linje med PSTN-baserte anrop. I tillegg vil et IP-basert nødmeldesystem muliggjøre et mangfold av nødmeldetjenester som ikke finnes per dags dato. Hovedproblemet med en overgang til IP-infrastruktur er at det ikke finnes et fast forhold mellom IP-adresser og lokasjon. Dette gjør lokalisering av brukere og geografisk ruting vanskelig.

Forskning og arbeid rundt integrering av nødtjenester i IP-nettverket blir blant annet utført av aktører som ECRIT og EMTEL, i form av standardiseringer av rammeverk for et fullstendig ende-til-ende IP-basert nødmeldesystem. Med grunnlag i dette arbeidet har vi definert en rekke krav og utfordringer, og beskrevet arkitektoniske løsningsmodeller. Vi har vurdert forskjellige metoder for posisjonsinnhenting, og foreslått en arkitektur for et nødmeldesystem i Trådløse Trondheim der klienten selv sørger for å innhente sin lokasjon. I tillegg har vi utviklet en demonstrator for en IP-basert terminal, som viser hvordan et nødanrop kan foregå. Her er anskaffelse, transport og presentasjon av lokasjonsinformasjon implementert, samt funksjonalitet for en nødsentral med en integrert kartapplikasjon som viser fra hvor anropet originerer. Demonstratoren er testet med hensyn på relevante lokasjonstjenester, og med Trådløse Trondheim som nettverksplattform.

Testene våre viser at de forskjellige lokasjonstjenestene oppfyller kravene for et nødmeldesystem i ulik grad. For posisjonsinnhenting har vi valgt en hybrid løsning der brukerklienten benytter GPS og lokasjonsmegleren GeoPos tilknyttet lokasjonskilden Cisco Location Appliance. Vår foreslåtte arkitektur baserer seg hovedsaklig på IMS-arkitekturen, og er en "tykk klient"-løsning med SIP som signaleringsprotokoll. Arkitekturen oppfyller de definerte kravene for et nødmeldesystem.

Kapittel 1

Introduksjon

1.1 Motivasjon

Mobile terminaler er ikke assosiert med en fast lokasjon eller adresse. En bruker av en mobil terminal kan dermed befinne seg hvor som helst. For mobiltelefoner kan nærliggende basestasjoner brukes for å gi en generell indikasjon på hvor brukeren befinner seg, men dette er ikke eksakt nok for enkelte formål.

For nødmeldinger er eksakte posisjonsdata er svært viktig, slik at hjelpemannskaper kan komme innringeren til unnsetning raskest mulig. I Trådløse Trondheim bør det være mulig for innringere å bruke en VoIP tjeneste ved nødanrop. Et problem er å finne ut fra hvor dette pakkebaserte anropet originerer. For å løse dette problemet kan innringeren sende med lokasjonsdata i anropet, men dette er avhengig av at innringerens terminal er i stand til å finne sin eksakte lokasjon på egen hånd. Dette kan gjøres ved at innringerens terminal er utstyrt med en GPS-mottager. Problemet er at innringeren sannsynligvis er innendørs, der GPS-signalet er enten svakt eller fraværende. I slike tilfeller trengs andre metoder for å innhente posisjonsdata.

Utviklingen viser en økning av antall mobile brukere i forhold til fasttelefon, og i tillegg tror mange at VoIP etterhvert vil ta over for telefoni over offentlig svitsjet fastnett. I USA har antall nødanrop til deres nødnummer 911 blitt fordoblet fra 1995 til 2006, til over 50 millioner per år. Det er estimert at 30% av disse er fra mobiltelefoner, og at denne prosenten øker kraftig [FCC06]. AMK-sentralen ved St. Olavs Hospital i Trondheim har verken støtte for VoIP eller en teknisk løsning for å stadfeste lokasjon hvis en innringer benytter mobiltelefon [Appendiks A].

Ergo finnes det et stort behov for å kunne fastsette lokasjonen til en innringer som benytter en mobil terminal. I tillegg til den åpenbare nytten dette vil ha for nødmeldetjenester vil det også muliggjøre lokasjonsbaserte tjenester, som vil være av kommersiell interesse for tjenesteleverandører.

1.2 Problemstilling

Bruk av VoIP øker stadig, og utviklingen går mot økt transport av tale over IP-nettverk. Slik IP-nettet fungerer i dag, behøver det ikke være noen sammenheng mellom IP-adresse og lokasjon til klienten. Denne begrensningen vanskeliggjør bruk av lokasjonsbaserte tjenester.

Nødmeldetjenester er avhengig av lokasjonen til klienten. Det er derfor nødvendig å finne metoder for å kunne avdekke denne lokasjonen. Ved å bruke Trådløse Trondheim som nettverksplattform skal vi studere foreslått arkitektur, og eventuelt foreslå forbedringer.

I tillegg skal vi utarbeide et utkast for en fleksibel løsning for en modifisert SIP-klient i terminalen til brukeren, der posisjondata sendes med anropet. En slik løsning vil også kunne anvendes for sivile formål basert på lokasjon, for eksempel bestilling av drosje og pizza, samt navigering og finne nærmeste tilbyder av en tjeneste eller et produkt.

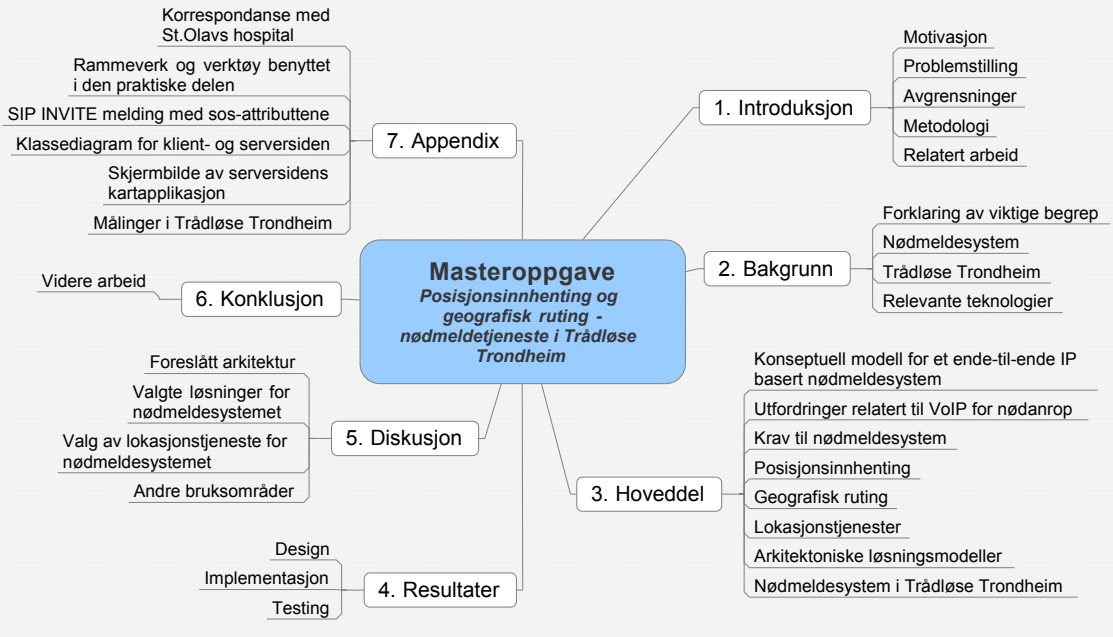
1.3 Avgrensninger

Emner som er utenfor oppgavens omgang:

- Etiske problemstillinger rundt personvern og konsekvenser for distribusjon av lokasjonsinformasjon over nettverk. Konsekvenser for arkitektur er inkludert ved et eksempel 3.7.6.
- Serversidefunksjonalitet. Oppgaven tar utgangspunkt i at klienten skal finne sin lokasjon. Vi har dermed utelatt diskusjon rundt dette emnet. I demonstratoren vår har vi imidlertid implementert en kartapplikasjon for anropsmottager 4.2.6.
- Mobiltelefoni og nødmeldesystem basert på mobilnettet. Vår oppgave omhandler telefoni over IP-baserte nettverk (VoIP).
- Vi skal bare se på SIP som signaleringsprotokoll (ikke H.323, eller MEGACO eller andre).
- Vi ser ikke på IP-adresse for posisjonsinnhenting, men forklarer konseptet.
- Vi ser bare på de tre lokasjonstjenestene; GPS, GeoPos og lokasjonsdatabase basert på MAC.
- Grensesnitt mellom lokasjonsmegler, NRDB, ERDB og underliggende
- Vi ser bare på et ende-til-ende IP-basert nødmeldesystem, ikke en hybrid løsning med IP og PSTN.
- Forskjeller på PSTN/POTS og tale over IP.
- Sikkerhet (bare kortfattet).
- Juridiske og økonomiske aspekter.

1.4 Metodologi

1.4.1 Oppbygning av rapporten



Figuren viser hvordan rapporten er bygd opp. Bakgrunnen fokuserer på nødvendig teorikunnskap for å kunne forstå innholdet i rapporten. Hoveddelen spesifiserer krav og utfordringer tilknyttet et nødmeldesystem, og beskriver hvordan lokasjonsinformasjon kan behandles. I tillegg vurderes forskjellige lokasjonstjenester aktuelle i et nødmeldesystem. Arkitektoniske løsningsmodeller blir beskrevet ut fra hva som er foreslått av relatert arbeid. Til slutt beskriver vi et nødmeldesystem i Trådløse Trondheim, som er vår foreslåtte løsning med tanke på arkitektur og funksjonalitet.

Resultater tar for seg det praktiske arbeidet utført. Design beskriver nødmeldesystemet og funksjonalitet på klientsiden i form av en plug-in løsning. Implementasjon er en teknisk beskrivelse av implementeringen utført for å utvikle en demonstrator for nødmeldetjenesten. Testing viser hvordan vi testet demonstratoren, spesielt med tanke på lokasjonstjenestene benyttet. Herunder finnes også resultater og analyse av resultatene.

Diskusjonen vurderer de arkitektoniske valgene vi har gjort, og begrunner strukturelle løsninger. I tillegg begrunnes valg av løsninger i nødmeldesystemet, samt valg av en primærløsning for posisjonsinnhenting. Til slutt diskuteres bruk av systemet i form av hensyn som må tas, og andre bruksområder.

Appendiksene gir en grundigere beskrivelse av enkelte emner i rapporten, samt testresultater.

1.4.1.1 Referanser

Referanser er merket [WSC08] og refererer til bibliografien bakerst i rapporten. Kryssreferanser er merket [kap. 3.2.1] og refererer til et spesielt kapittel i rapporten.

1.4.2 Framgangsmåte

Oppgaven består av en teoretisk del og en praktisk del. Den teoretiske delen består av å vurdere arkitekturer, samt krav og utfordringer knyttet til disse, som et litteraturstudie. Vi har studert forskjellige forslag fra relaterte arbeidsgrupper (for ekempel 3GPP og IETF), og gjengitt disse med fokus på særpreg som kan være aktuelle for den praktiske delen. Den praktiske delen består av å foreslå en arkitektur for et nødmeldesystem i Trådløse Trondheim, i tillegg til utvikling av en demonstrator av nødmeldesystemet. Her har vi valgt en prosedyremessig framgangsmåte, ved å først designe systemet, og så implementere det i henhold til design og krav. Testdelen viser hvordan systemet fungerte i praksis.

1.4.3 Hvordan vi har samarbeidet

I den teoretiske delen har vi valgt å fordele arbeidet, noe som har resultert i inkonsekvent bruk av terminologien i enkelte tilfeller. Vi har derfor definert viktige begreper i kapittelet *Definisjoner*.

Det praktiske arbeidet ble delt i to deler. En del sto for kommunikasjon mellom SOS-agenten og terminalens VoIP-applikasjon samt serverens SIP-proxy. Den andre delen tok for seg kommunikasjon mellom SOS-agenten og lokasjonstjenestene, GPS og GeoPos. I tillegg tok den andre delen seg av parsing og metode for å legge til lokasjonsinformasjon som sos-attributter. Serverfunksjonaliteten besto av en del for å fange opp anropet, og tolke lokasjonsparametrene. Den andre delen koblet lokasjonsparametrene opp mot en kartapplikasjon. Testdelen besto av testing av feilmarginer og forsinkelse for CLA, i tillegg til testing av signalstyrke og antall aksesspunkter.

Enkelte steder har vi samarbeidet med å skrive, for eksempel i konklusjon og sammendrag.

1.5 Relatert arbeid

1.5.1 Organisasjoner

Det dokumenterte arbeidet med nødanrop over IP er hovedsaklig utført av sammensatte organisasjoner eller arbeidsgrupper. Dette delkapittelet presenterer de viktigste gruppene i dette arbeidet:

- **3GPP - The 3rd Generation Partnership Project**
  Samarbeidsorganisasjon som arbeider med å spesifisere et tredjegenerasjons (3G) mobiltelefonisystem.
- **ATIS - Alliance for Telecommunications Industry Solutions**
  Standardiseringsorganisasjon for informasjonsteknologi i telekommunikasjonsindustrien. Fokuserer på IPTV, fast-mobil konvergens (FMK), neste generasjons nett (NGN), VoIP og andre nettverksaspekter.
- **ECRIT - Emergency Context Resolution with Internet Technologies**
  Arbeidsgruppe under IETF. Tar for seg nødanrop fra sivile brukere tilkoblet Internett, og hvilke konsekvenser det får for autentisering og viderekobling.
- **EMTEL - Emergency Communications**
  Undergruppe av ETSI som utarbeider dokumentasjon for telekommunikasjonstjenester i nødsituasjoner.
- **ETSI - European Telecommunications Standards Institute**
  Uavhengig standardiseringsorganisasjon for telekommunikasjonsindustrien. Var blant annet ansvarlig for å standardisere GSM.
- **FCC - Federal Communications Commission**
  Uavhengig amerikansk myndighetsbyrå som regulerer radiospekteret (tv og radio) utenfor myndighetenes bruk. I tillegg regulerer de all telekommunikasjon mellom statene, og internasjonal kommunikasjon som originerer eller terminerer i USA.
- **NENA - National Emergency Number Association**
  Amerikansk organisasjon som har ansvaret for drift og teknologisk utvikling av nødtjenesten 911 i USA.

1.5.2 Next Generation 9-1-1

NENAs i3 arkitektur for Nord-Amerika, også kalt Next Generation 9-1-1 (NG9-1-1), bygger på IETFs arbeid rundt et IP-basert nødmeldesystem [kap. 3.7.3]. i3 er en videreutvikling fra i2 arkitekturen. i2 er en overgangsarkitektur og krever ingen forandringer av nødsentralene. I motsetning til dette ønsker NENA med i3 et fullstendig ende-til-ende IP-basert system. Det vil si at også nødsentralene er IP-baserte. Derfor vil hele kommunikasjonsveien gå over samme protokoll i nettverkslaget og ingen gatewaykonvertering er nødvendig. Nødsentralene vil også kunne håndtere flere typer anrop; video, audio og tekst. Emergency Service IP Network (ESINet) er betegnelsen på den delen av IP-nettverket som tilhører nødmeldesystemet og som sørger for korrekt ruting til nødsentralene.

1.5.3 Arbeid

Arbeidsgruppene presentert i kapittel 1.5.1 har utgitt, eller arbeider med, diverse forslag til spesifikasjoner som omhandler emner relatert til vår oppgave. Dette delkapittelet presenterer de viktigste dokumentene fordelt på ansvarlig arbeidsgruppe:

- 3GPP
  - *IP Multimedia Subsystems (IMS) emergency sessions (Release 7)* [3GP06]
    Dokumentet spesifiserer nødmeldetjenester i IMS-arkitekturen, og nødvendige elementer som kreves for å støtte nødmeldetjenester. Denne artikkelen innfører konseptet om en E-ruter (E-CSCF) og beskriver også hvordan en lokasjonsfunksjon (LRF) skal fungere.
- Atis
  - *Location Acquisition and Location Parameter Conveyance for Internet Access Networks in Support of Emergency Services* [AA07]
    Dokumentet beskriver områder innenfor anskaffelse av lokasjon og hvordan lokasjonsparametre skal transporteres, med fokus på hvordan dette angår arkitektur og protokoller. Dokumentet beskriver også hvordan LIS-funksjonen kan brukes for å kalkulere lokasjon.
- ECRIT
  - *Requirements for Emergency Context Resolution with Internet Technologies* [HS07]
    Dokumentet definerer terminologi og spesifiserer rammebetingelser for sivile nødanrop ved hjelp av VoIP og generelle multimediesystemer som baserer seg på transportprotokoller.
- EMTEL
  - *Emergency calls and VoIP : Possible short and long term solutions and standardisation activities* [EMT06]
    Dokumentet adresserer implementeringsproblemer med nødtelefoni over IP, og de ulike scenarioene og mulighetene for å håndtere nødanrop. I tillegg gis en oversikt over forskjellig standardiseringsarbeid hos andre grupper, og en oppsummering over ulike metoder som VoIP-tilbydere benytter for å tilby nødmeldetjenester.
- IETF
  - *Emergency Services for Internet Telephony Systems* [HS04]
    Dokumentet beskriver hvordan SIP kan benyttes for å tilby avanserte nødmeldetjenester basert på VoIP, der DNS blir benyttet for å koble lokasjon til korrekt PSAP.
  - *Session Initiation Protocol Location Conveyance* [JP07]
    Dokumentet beskriver rammeverk og krav for å transportere lokasjonsinformasjon mellom SIP-entiteter, både for ende-til-ende transport og lokasjonsbasert ruting.

  - *Emergency Services URI for the Session Initiation Protocol*[Sch06]
    Dokumentet definerer universelle SIP URI (for eksempel sip:sos@domain), som muliggjør kontakt med nødsentraler for SIP-agenter. I tillegg defineres konvensjoner for å øke sannsynligheten for å komme fram til korrekt nødsentral.

- Annet (forslag til arkitektur)

  - *A VoIP Emergency Services Architecture and Prototype* [MMH05]
    Dokumentet foreslår en arkitektur for et nødmeldesystem basert på VoIP og SIP, som også kan håndtere anrop fra PSTN. Dokumentet beskriver identifikasjon av nødanrop, innhenting av lokasjon og hvordan anropet blir rutet til korrekt PSAP. Det spesielle med dette dokumentet er at det beskriver en implementering av en prototype, som viser at arkitekturen er mulig og at den er skalerbar.
  - *Providing emergency services in Internet telephony* [HS02]
    Dokumentet beskriver dagens løsning for nødtelefoni, og foreslår en SIP-basert arkitektur for nødtelefoni og varsling med fokus på hastighet, skaleringsevne og økt funksjonalitet.
  - *The IETF Geopriv and Presence Architecture Focusing on Location Privacy*[Tsc06]
    Dokument som beskriver GeoPriv i forhold til tilstedeværelsesarkitektur med fokus på personvern. Innfører en personvernbasert arkitektur med regelmyndighet.

Kapittel 2

Bakgrunn

Dette kapittelet forklarer konsepter for et nødmeldesystem, og hvordan systemet kan realiseres i Trådløse Trondheim. Fokuset ligger på hva posisjonsinnhenting er, hvordan dette har blitt brukt tidligere, hvordan det kan bli utnyttet og tekniske konsepter nødvendig for å realisere dette; SIP, GPS etc.

2.1 Forklaring av viktige begrep

Dette delkapittelet definerer viktige begreper for å forstå hvordan et nødanrop fungerer, og hvorfor posisjonsinnhenting er viktig for et sikkert nødmeldesystem.

2.1.1 Posisjon/Lokasjon

En posisjon eller lokasjon kan enten være sivil eller geodetisk. Sivil lokasjon kan være et land, en by eller et gatenavn, for eksempel "Storsvingen 1, Oslo". Geodetiske data er breddegrad, lengdegrad og høyde over havet (geodetisk eller ellipsoidisk høyde). Disse angir koordinatene til ett punkt på Jorden. Den geodetiske lokasjonen er mest nøyaktig, men ofte er den sivile mer praktisk. Man kan derfor bruke den geodetiske lokasjonen for å finne den sivile.

I denne teksten blir posisjon og lokasjon brukt som synonyme begreper.

2.1.2 Lokasjonsdata for nødmeldetjenester

Dagens nødmeldesystem [kap. 2.2.2] benytter lokasjonsdata som sentral informasjon ved et nødanrop. Et nødanrop viderekobles på grunnlag av klientens lokasjon, til nærmeste PSAP (Public Safety Answering Point)[kap. 2.1.3], som er en nødsentral ansvarlig for å svare på nødanrop [3GP06]. Dette gjelder dog kun for nødanrop over det offentlige svitsjede telenettet, også kjent som PSTN (Public Switched Telephone Network).

Nødmeldetjenester trenger dermed lokasjon for å [JP07]:

- Koble anropet til riktig PSAP.
- Sende hjelpemannskap til riktig sted.

2.1.3 Public Safety Answering Point (PSAP)

PSAP er den amerikanske betegnelsen på en nødsentral som mottar nødanrop. Hver nødsentral har ansvaret for et geografisk område, for eksempel en by eller et fylke. Eksempelvis er det 6500 PSAPer i USA, som deler ansvaret med å betjene deres 911 nødnummer. Dette nødnummeret gjelder for både brann, politi og ambulanse. Norge har til sammenligning forskjellige nødnummer for hver av de tre etatene. De norske PSAPene som har ansvaret for det medisinske nødnummeret 113, kalles akuttmedisinsk kommunikasjonssentral (AMK)[kap. 2.1.4]. I Europa kalles en slik nødsentral Emergency Response Center (ERC) [HS02].

2.1.4 Akuttmedisinsk kommunikasjonssentral (AMK)

Det finnes per dags dato 24 AMK-sentraler i Norge [Hun06]. AMK-sentralen i Trondheim er en del av akuttmottaket ved St. Olavs Hospital, universitetssykehuset i Trondheim. AMK-sentralen mottar alle nødanrop (113) som originerer fra en kommune som sogner til St. Olavs Hospital, ved hjelp av geografisk ruting [kap. 2.1.5]. Disse nødanropene er ment å være hastemeldinger som inkluderer akutt sykdom og skade.

På AMK-sentralen svarer spesialopplærte sykepleiere på anropet, og koordinerer lege, ambulanse og luftambulanse avhengig av alvorlighetsgrad og omfang. En innringer må oppgi følgende opplysninger :

- Adressen for hendelsen.
- Telefonnummeret det ringes fra.
- Hendelsen.

2.1.5 Geografisk ruting

Ruting av anrop baseres på geografisk informasjon i sesjonsoppsettet. Dette kan for eksempel være retningsnummer hos en fasttelefonkunde, landskode, eller tilleggsinformasjon i en datapakke ved IP-basert anrop. Rutingsentralen benytter disse reglene for oppslag og videreruting til nærmeste endebruker. Hovedpoenget med dette er en mer effektiv og raskere behandling av anrop. Hvis en innbygger i Trondheim ringer 113 fra sin hustelefon vil retningsnummeret benyttes for videreruting av anropet til AMK-sentralen i Trondheim.

2.2 Nødmeldesystem

Før mobiltelefonen ble introdusert var hvert nummer ikke-nomadisk, det vil si at hver lokasjon var statisk, og derfor kunne hvert nummer assosieres med en lokasjon. Da mobiltelefonen ble introdusert endret selvsagt dette seg, og lokasjonen til en bruker av mobiltelefon kunne ikke bli bestemt nærmere enn hvilken basestasjon mobiltelefonen var i kontakt med. Man brukte måling av signaler for å bestemme posisjon. Siden har tale over IP (VoIP) blitt introdusert, noe som har satt enda større krav til bestemmelse av lokasjon, da IP-adressen til en klient koblet til et IP-nettverk ikke behøver å ha noen sammenheng med lokasjonen til klienten.

2.2.1 Nødnummerets histore

Det første nødnummeret ble opprettet i London den 30.juni 1937. Nødnummeret var 999, og da noen ringte gikk det en alarm samtidig som det lyste en rød lampe hos telefonoperatøren for å identifisere nødanropet. Årsaken til innføringen av dette systemet var den store pågangen på politistasjonene. Av praktiske årsaker ble nødnummeret valgt til et kort memorerbart nummer. Dette nødmeldesystemet ble først tilgjengelig for alle engelske telefoner på slutten av 1960-tallet [Fir03].

Det første nødmeldesystemet i USA basert på nødnummeret 911 ble opprettet i 1968. Den 29. juli 1991 ble 112 valgt til universielt nødnummer av EU[1] [Com01]. Alle medlemsland av EU og de fleste medlemmer av CEPT[2] har nå implementert 112 som gyldig nødnummer. Det betyr at man ved å ringe 112 i disse landene er sikret å komme fram til en nødsentral. Fellesnummeret 112 er ikke ment å erstatte eksisterende nødnummer som brukes i de forskjellige EU-landene, men skal fungere i parallell med disse.

Global System for Mobile Communication (GSM) standarden bruker 112 som nødnummer, og selv om brukeren befinner seg i et land der 112 ikke er standard nødnummer, vil da anropet bli viderekoblet til det riktige nødnummeret. De fleste GSM telefoner kan ringe nødnummeret 112 selv om telefonen er låst eller mangler SIM[3] kort.

I Norge brukes primært 113 som nødnummer ved medisinske akuttilfeller. Anropet blir viderekoblet til en nødsentral, beskrevet i kapittel 2.1.4.

2.2.2 Nødmeldesystem per dags dato

2.2.2.1 Viktigste komponenter

Et nødmeldesystem inneholder vanligvis fire komponenter [HS02]:

1. *Universelt nummer:* Et enkelt nummer for tilgang til nødmeldetjenester. For eksempel 911 i USA og 112 i Europa. I Norge bruker vi 110 for brannvesen, 112 for politi og 113 for ambulanse.

2. *Anropsruting:* Anropslokasjonen blir benyttet til å viderekoble anropet til nærmeste PSAP/nødsentral.

[1] European Union
[2] European Conference of Postal and Telecommunications Administrations
[3] Subscriber Identity Module

3. *Brukeridentifikasjon:* Brukes til å hindre tulleringing, loggføring etc.

4. *Brukerlokasjon:* Brukes til viderekobling av anropet. Hvis det ringes fra fasttelefon brukes adressen tilknyttet abonnementet, hvis det ringes fra mobiltelefon brukes signalering.

2.2.2.2 Den norske modellen

Nødmeldesystemet i Norge er basert på direkte innvalg [kap. 2.2.2.3], og den medisinske delen består av AMK-sentraler og legevaktsentraler. AMK-sentralene deler det felles nasjonale nødnummeret 113, mens legevaktsentralene har lokale 8-sifrede nummer. Ringer man 113 blir anropet viderekoblet til nærmeste AMK-sentral (basert på tilgjengelig brukerlokasjon).

Den norske modellen tilstreber en distribuert helsetjeneste, der forskjellige aktører ofte samarbeider (gjensidig assistanse) for å bringe helsetjenesten ut til pasienten på en mest mulig effektiv måte. I dette hensyn blir telekommunikasjon benyttet som et hjelpemiddel, slik at akutte situasjoner kan behjelpes ved å:

- Gi best (og raskest) mulig beslutningsstøtte og behandling på stedet.
- Koordinere assistanse ut fra omfang og behov.

Utviklingen innenfor telekommunikasjon har ført til bedre utstyrte mobile enheter, nettverk og tjenester. Utnyttelse av denne teknologien øker evnen til å gjennomføre behandlig utenfor sykehuset. Dette er en ønsket og hensiktsmessig utvikling, fordi det avlaster sykehuset og transportleddet [And07].

2.2.2.3 Direkte innvalg kontra felles nødnummer

I Norge benyttes direkte innvalg, som betyr spesifikke nødnummer til de tre viktigste nødinstansene; brann, politi og lege. Direkte innvalg benyttes av de fleste land i Europa. Alternativet er et felles nummer for alle nødinstansene i samme land. Felles nødnummer brukes for eksempel i USA og Finland.

Med felles nødnummer fungerer nødsentralen som en "formidlingstjeneste", som er spesialist i å motta og videreformidle nødmeldinger til riktig instans. Dette systemet er billigere og mer effektivt i drift, men operatørens ansvar utløper idet nødmeldingen er varslet videre. I tillegg vil det medføre lavere silingsevne enn ved direkte innvalg.

Direkte innvalg har spesialiserte nødsentraler for hver nødinstans. Dette betyr at i mange tilfeller kan operatøren selv besvare nødanropet uten å kontakte videre assistanse. Denne silingsmekanismen avlaster både lokale legesentre og sentrale sykehus. Direkte innvalg fungerer altså mer som en *behandlingstjeneste* [And07].

2.2.2.4 Støtte for VoIP og mobiltelefon

AMK-sentralen har per dags dato ingen støtte for VoIP, og de har heller ingen teknisk løsning for å stadfeste lokasjon hvis anropet kommer fra en mobiltelefon [Appendiks A]. De er derfor avhengig av at innringer oppgir sin lokasjon muntlig, og må så stole på

at de opplysningene er korrekte. Ved å muliggjøre lokasjonsdata vil arbeidet til AMK-sentralen forenkles og gjøres raskere i situasjoner der nøyaktig informasjon kan redde liv. For eksempel kan et anrop med lokasjonsdata aktivere en kartapplikasjon på AMK-sentralen, slik at vaktoperatoren straks vil se hvor anropet kommer fra, og raskeste veg for å nå dit.

2.2.3 Signalering for posisjonsinnhenting

Radiobølger kan passivt brukes for å finne lokasjon, fordi en mobiltelefon sender ut signaler. Basestasjoner kan måle hvordan disse signalene fra en mobiltelefon ankommer, med tanke på vinkel, tiden det tar for et signal å returnere, og signalstyrke.

GSM ble lansert kommersielt i Norge i 1993, og er et digitalt system for mobiltelefoni. GSM kan benytte triangulering for å finne posisjonen til en mobiltelefon/bruker. En type triangulering er multilaterasjon (hyperbolsk posisjonering), en prosess som lokaliserer et objekt nøyaktig ved å regne ut tidsforskjellen til signaler utsendt av tre eller flere basestasjoner. Cell Identification er den mest brukte metoden for å anslå hvor en terminal befinner seg. Dennen metoden fastslår hvilken celle anropet originerer fra, og bruker dette som lokasjon for terminalen. Nøyaktigheten baserer seg på cellens rekkevidde, og feilmarginene kan variere fra et par hundre meter i urbane strøk til opp mot 32 km i suburbane og rurale områder [Wik07e]. Disse feilmarginene er for høye til bruk i nødmeldetjenester.

Metoder for å finne lokasjonen til en mobiltelefon ved bruk av signalering:

- Cell Identification (CI)
- Enhanced Cell Identification (E-CI)
- Angel of arrival (AOA)
- Time difference of arrival (TDOA)
- Location signature
- Enhanced Observed Time Difference (E-OTD)
- Cell Broadcast
- Assisted GPS [kap. 2.4.2.2]

Begrensningen til disse lokasjonsteknikkene basert på signalering er at de er avhengig av mest mulig klar bane slik at signalene ikke svekkes. Dette er praktisk umulig i tettbebygde strøk og i variert terreng [Wik07e].

Assisted-GPS er en såkalt hybrid løsning, som kombinerer teknologier i terminalen og nettverket. Per dags dato begynner GPS å bli innført i mobile terminaler. Mer om GPS og dens begrensninger i kapittel 2.4.2.1.

2.2.4 IP-adresse for posisjonsinnhenting

Ved fasttelefoni (linjesvitsjet) kan telefonnummeret til innringeren benyttes i en viss grad for å finne posisjonen. Og ved anrop fra mobiltelefon kan Cell Identication benyttes for å finne en indikasjon på posisjonen, som er nøyaktig nok til å koble samtalen til riktig PSAP. Men IP-baserte terminaler er identifisert av en IP-adresse, og den er lokasjonsuavhengig.

En IP-adresse var opprinnelig ment som en unik identifkator for nettverksbaserte innretninger. IPv4 er standarden for en IP-adresser per dags dato, selv om IPv6 er i ferd med og innføres. IPv4 er oppbygd av 32bit (4byte) av formen "127.0.0.1". Fordi IP-adresser er representert ved tallkombinasjoner er de i praksis vanskelig å huske på. Av denne grunn ble Domain Name System (DNS) opprettet, et system som mapper navn til IP-adresser. Et slikt navn kan være en URL eller en epostadresse.

En bruker får vanligvis tildelt sin IP-adresse dynamisk av en Internet Service Provider (ISP). Ved å utføre en *WHOIS* spørring mot DNS finnes den fysiske lokasjonen til en ISP, som gir en generell indikasjon på hvor en bruker sannsynligvis befinner seg. Begrensningen med denne metoden er at detaljenivået på indikasjonen oftest begrenser seg til en by eller et tettsted, noe som ikke gir eksakt nok lokasjonsdata til nødmeldetjenester. I tillegg kan ISPen dekke store områder, for eksempel et helt land, og da vil denne informasjonen være verdiløs [Ran05]. På grunnlag av de praktiske problemene knyttet til bruk av IP-adresse for posisjonsinnhenting har vi utelatt videre utdypning av dette som lokasjonstjeneste.

2.2.5 IP-basert PSAP

For å muliggjøre ende-til-ende IP-basert kommunikasjon mellom innringer og PSAP må begge parter være IP-kompatible. Dette betyr at anropet ikke benytter PSTN i hele tatt, og konvertering fra IP til PSTN er unødvending [EMT06].

IP basert ende-til-ende kommunikasjon muliggjør nødmeldetjenester som ikke finnes per dags dato, og disse blir beskrevet i kapittel 2.2.6. En annen fordel med IP-basert PSAP er at den krever en mye enklere infrastruktur enn dagens PSAPer. Infrastrukturen trenger strengt tatt bare å bestå av en datamaskin med tilkobling til det IP-baserte nettverket. Man kan se for seg en distribuert modell der nødoperatørene ikke er avhengig av å fysisk være tilstede på samme sted, så lenge de er tilkoblet det IP-baserte nettverket. Ved å bruke SIP som protokoll kan anropet spaltes i parallelle eller sekvensielle grener, som blir fordelt på nødoperatørene inntil en av dem svarer på anropet. Parallell spalting tillater lastbalanse mellom PSAPene, mens sekvensiell spalting støtter ruteroverflyt, slik at samtaler som har vært lenge på venting blir satt over til en reserve-PSAP [HS02].

2.2.6 Teknologier for nødmeldetjenester

Teknologiene beskrevet i dette kapittelet og bruken av IP-basert nett som transportmedium ved nødanrop muliggjør flere nødmeldetjenester som ikke finnes per dags dato. [EMT06] definerer 12 teknologier som skal kunne anvendes til nødanrop:

1. PSTN/POTS
2. Mobiltelefoni
3. Satelittelefoni
4. VoIP
    - Fast (Klienten har en fast NAP)
    - Nomadisk (Klienten kan forandre NAP)
5. Telefoni over Internett
6. Videosamtale (f.eks 3G-telefon)
7. Dataanrop (f.eks alarm fra en innretning)
8. E-mail
9. Vedlagte filer (f.eks ved e-mail eller MMS)
10. SMS[4]
11. MMS[5]
12. Instant messaging og chat

1-5 er for taletjenester, og 6-12 er for multimedietjenester. Fordelen med de nye taletjenestene (4 og 5) er at de skal kunne benytte lokalisering av anroper uten at anroperen oppgir sin lokasjon. Årsaken til det kan for eksempel være at personen er stum, lider av afasi (mangel på taleevne), tekniske problemer på telefonlinjen etc. Multimedietjenestene (6-12) muliggjør alternative kommunikasjonsmetoder som kan være egnet i spesielle situasjoner.

For eksempel vil videotelefoni tillate nødmannskapet å se situasjonen på video før de ankommer, slik at de kan forberede seg på best mulig måte, eller for å overvåke nødmannskapets innsats på ulykkesstedet. Videotelefoni kan også brukes til å kommunisere med personer som bruker tegnspråk, eller som av andre grunner er ute av stand til å snakke. Et annet eksempel er tekstbasert kommunikasjon, som kan være egnet i en situasjon der batteriet på terminalen ikke strekker til en vanlig samtale. Tekstbasert kommunikasjon er også et alternativ for å kommunisere med døve personer [HS02].

[4] Short Message Service (tekstmeldinger på mobiltelefon)
[5] Multimedia Messaging Service

2.3 Trådløse Trondheim

2.3.1 Om Trådløse Trondheim

Trådløse Trondheim er et forsknings - og utviklingsprosjekt på initiativ fra NTNU. Den offisielle åpningen 26. september 2006 gjorde Trondheim til en av de første trådløse byene i Europa. Formålet med prosjektet er å tilby trådløs Internettilgang til byens innbyggere, i første omgang ved å utnytte Wi-Fi teknologi. Den foreløpige største begrensningen til Trådløse Trondheim er minimal innendørs dekning [Tro07].

Det er rimelig å anta at Trondheims innbyggere vil ha trådløs tilgang til Internett i framtida, både ute og inne. I vår kontekst vil dette bety mulighet for IP-telefoni med lokasjonsdata, noe som vil skape grobunn for et mangfold av tjenester. Eksempler på tjenester muliggjort eller forenklet av lokasjonsdata:

- Mottager vet lokasjon til anroper
  Nødanrop (113), bestilling av drosje, pizza etc.
- Finne nærmeste tilbyder
  Restaurant, frisør, bensinstasjon, matbutikk
- Lokasjonsbestemte tjenester
  Været, trafikk, navigasjon, stedsinformasjon

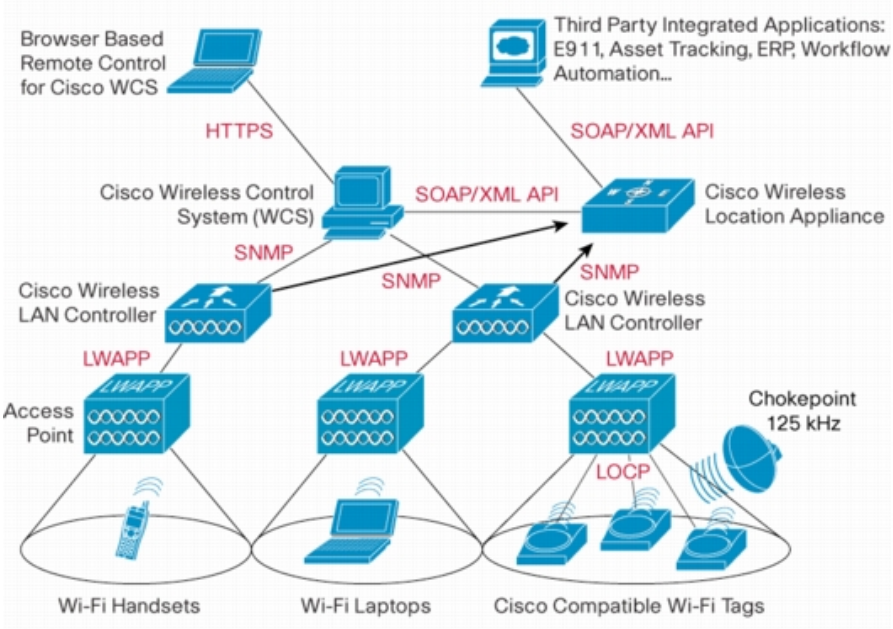
2.3.2 GeoPos

GeoPos er et prosjekt startet opp av professor Steinar Andresen og Institutt for telematikk ved NTNU, høsten 2004. Hovedmålet med prosjektet var å utarbeide en geografisk posisjoneringstjeneste for nettverksklienter ved labbruk. GeoPos fungerer som en lokasjonsmegler, og er avhengig av en eller flere lokasjonskilder. En slik kilde kan for eksempel tilby lokasjonsdata for mobiltelefoner, eller IP-baserte terminaler. Per dags dato benytter GeoPos seg av Cisco Location Appliance som lokasjonskilde. GeoPos Web Service tilbyr et enkelt og sikkert grensesnitt mellom brukeren og Cisco Location Appliance. For autentisering og oppkobling mot GeoPos Web Service må brukeren ha en brukerkonto, samt et eget sertifikat godkjent og signert av GeoPos CA[6].

2.3.3 Cisco Location Appliance (CLA)

Cisco Location Appliance (CLA), også kjent som Cisco Wireless Location Appliance, baserer seg på en WLAN infrastruktur. Denne infrastrukturen kan benyttes for å automatisk spore trådløse enheter som befinner seg i dekningsområdet. Cisco Location Appliance tilbyr også et sentralisert brukergrensesnitt for administrering av systemet.

[6] Certificate Authority



Figur 2.1: Figuren viser arkitekturen til Cisco Wireless Location Appliance [Inc07] med en WLAN basert infrastruktur og en sentralisert administrasjon.

2.4 Relevante teknologier

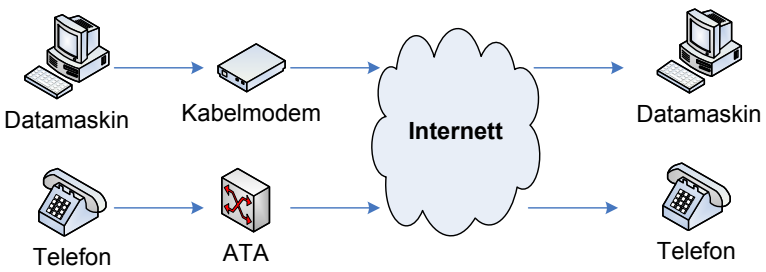
Dette delkapittelet beskriver den teknologien som kreves for å realisere nødmeldetjenester i Trådløse Trondheim.

2.4.1 Voice over IP (VoIP)

Voice over IP kan oversettes til norsk som *tale over IP*. I 1977 ble den første publikasjonen om VoIP utgitt av D. Cohen. Etter dette fulgte en årrekke med forskning, spesielt innefor QoS, før standardiseringen av SIP begynte på midten av nittitallet under ledelse av professor Henning Schulzrinne [JK07].

VoIP er fellesbetegnelsen på tjenester som ruter samtaler via Internett eller via lokale IP-nettverk, derfor tilnavnet *tale over IP*. Analoge audiosignaler blir digitalisert og delt opp i datapakker som kan overføres via IP nettverket ved hjelp av en transportprotokoll (for eksempel UDP). Figur 2.2 illustrerer de tre hovedmåtene for å utføre en VoIP samtale:

- *ATA*
  Analog telefonadapter som konverterer fra analogt signal til digitale data. Hvis en vanlig telefon benyttes kan ATA koble signalet til en datamaskin eller et IP-nettverk.
- *IP telefon*
  Kobles direkte til en ruter, og kan så brukes som en vanlig telefon. En WiFi-telefon kan kobles til en trådløs ruter hvis den er innenfor et område med trådløs dekning.
- *Datamaskin til datamaskin*
  En VoIP-klient muliggjør gratis tale over et IP-nettverk, så lenge man er tilkoblet nettet (for eksempel med et kabelmodem).



Figur 2.2: VoIP betyr tale over IP, og baserer seg på at samtalen blir digitalisert og sendt som pakker over et IP-nettverk. En datamaskin eller en telefon er avhengig av et kabelmodem eller en ATA for å kunne benyttes.

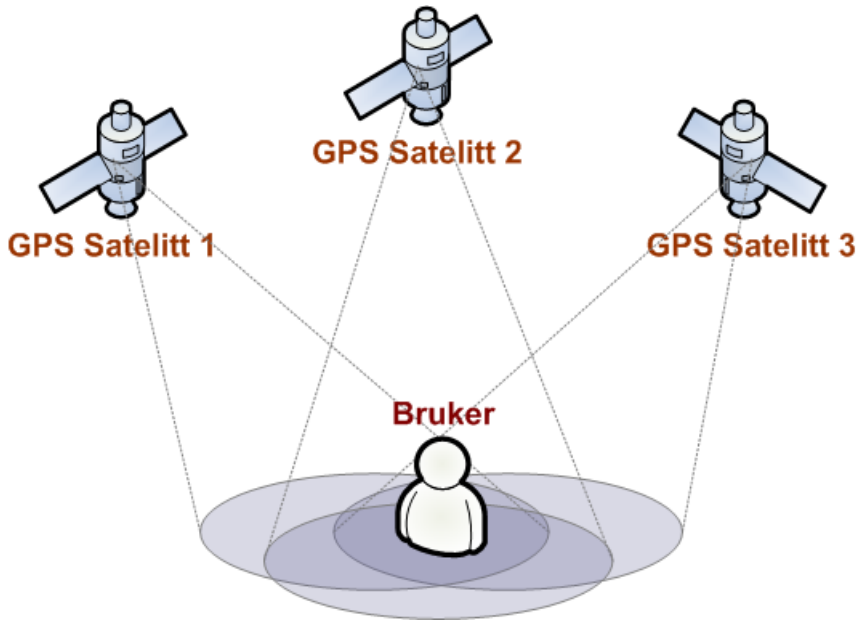
Fordelene med å bruke VoIP er først og fremst at det er en mer effektiv teknologi enn dagens linjesvitsjete fastnett. Man utnytter ressursene på en bedre måte. Dette gjør bruk av VoIP billigere og mer fleksibelt. De største svakhetene gjelder pålitelighet. VoIP kan ikke garantere for tidsforsinkelse, endring av tidsforsinkelse eller pakketap, noe som kan ha en negativ påvirkning på samtalekvaliteten. En annen begrensning er at VoIP er avhengig av strøm, i motsetning til fasttelefoner som får strøm via telefonlinjen. VoIP er derfor

avhengig av en stabil strømkilde, gjerne uavhengig av husholdningens strømkilde.

Det er likevel en felles oppfatning at telefoni over dagens linjesvitsjete nett vil bli erstattet av pakkebaserte nett i nær fremtid [Val07].

2.4.2 Global Navigation Satellite System (GNSS)

Global Navigation Satellite System er en fellesbetegnelse for satellittbaserte navigasjonssystem. Det eksisterer to operasjonelle GNSSer per dags dato; GPS og GLONASS. I tillegg til disse to er navigasjonssystemet Galileo i utviklingsfasen [Wik07c]. Figur 2.3 viser overordnet virkemåte av GNSS.



Figur 2.3: GNSS benytter seg av satellitter som kretser rundt jordkloden for å finne posisjonen til en satellittmottaker.

2.4.2.1 Global Positioning System (GPS)

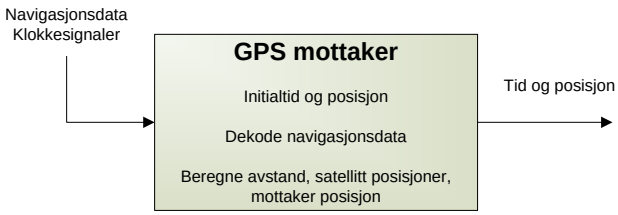
Global Positioning System er et navigasjonssystem bestående av en rekke MEO (Medium Earth Orbit) satellitter som kretser rundt hele jorda. Systemet ble utviklet av USAs forsvarsdepartement og ble først tatt i bruk i 1978. GPS-mottakeren finner sin posisjon ved triangulering. Triangulering skjer ved måling av tidsforskjellen i signaler fra flere GPS-satellitter. Fordi signalhastigheten er konstant, kan avstanden til hver enkelt satellitt, og mottakerens posisjon, kalkuleres. Figur 2.4 viser mottatt data og hvilke beregninger som gjøres av GPS-mottakeren. GPS har en feilrate på bare noen få meter.

Ved å benytte GPS kan en klient finne sin posisjon med stor nøyaktighet. Posisjonsinformasjonen kan legges til ved et VoIP-anrop for geografisk ruting og/eller anvendelse på mottakersiden, enten det er pizzasentralen eller AMK-sentralen. En begresning med

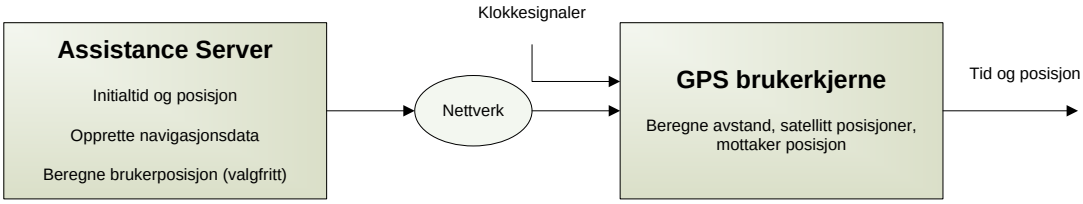
GPS er at det kreves klar synslinje (line-of-sight) for transmisjon, noe som gjør det er vanskelig å posisjonere klienter som befinner seg innendørs.

2.4.2.2 Assisted GPS (A-GPS)

Assisted GPS er en løsning som effektiviserer kommunikasjon mellom GPS-satellitt og klient. Klienten kommuniserer med en bistandsserver (Assistance Server) via et trådløst referansenettverk. Ved dårlige forbindelser kan klienten tilegne seg posisjonsdata fra serveren og nettverket. På denne måten hjelper bistandsserveren GPS-klienten med tunge og energikrevende oppgaver som avstandsmålinger og kalkulasjon av posisjonen (se figur 2.5). A-GPS egner seg godt i områder hvor kommunikasjon svekkes av objekter som dekker synslinjen, for eksempel i urbane miljøer cite.



Figur 2.4: GPS-mottakeren må selv søke etter satellittsignaler og dekode navigasjonsdataen før tid og posisjon kan beregnes. Dette er arbeidsoppgaver som krever sterke signaler og mye prosesseringstid [JL02].



Figur 2.5: Assistance Server tilbyr, i samarbeid med nettverket, en tilnærming av mottakerens posisjon, samt dekodet navigasjonsdata. Med dette kreves ikke like stor signalstyrke og mottakeren kan fortere finne sin posisjon [JL02].

2.4.2.3 Galileo og GLONASS

Galileo og GLONASS[7] er satellittbaserte navigasjonssystem i likhet med NASAs GPS. Galileo er et resultat av et felles initiativ mellom EU og ESA[8]. Formålet med prosjektet er et uavhengig navigasjonssystem for nasjoner i Europa, et system som er tilgjengelig i krigstider eller ved politiske uenigheter. Systemet er planlagt i drift i 2011-2012 [Wik07a]. Utviklingen av GLONASS begynte i Sovjetunionen i 1976 og var opprinnelig for militært bruk. Etter oppløsningen av Sovjetunionen overtok Russland systemet [Wik07d].

[7] Global Navigation Satellite System
[8] European Space Agency

2.4.3 Session Initiation Protocol (SIP)

Session Initiation Protocol er foreslått i RFC 3261 [J.R02] som en applikasjonslagprotokoll for opprettelse, modifisering og terminering av sesjoner mellom en eller flere aktører. Konseptet med en sesjon ble innført i RFC 2327 (Session Description Protocol), og kan for eksempel være en telefonsamtale, en videokonferanse, to brukere som deler data, chatting eller instant messaging (IM).

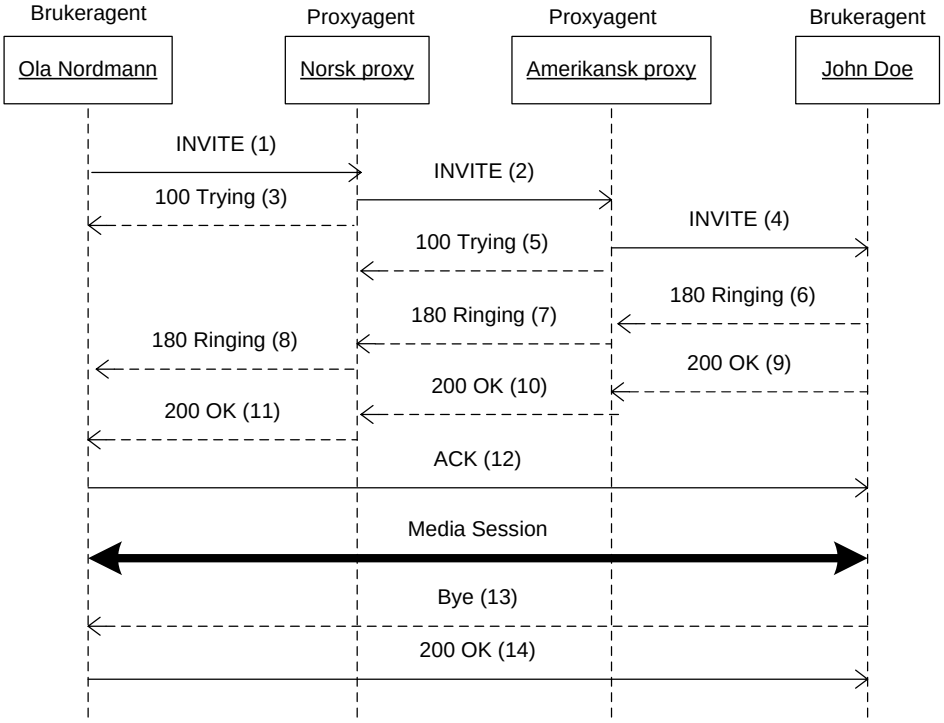
Formålet med SIP var å lage en enkel protokoll, som unngikk klassiske telecom designprinsipper som for eksempel protokollagsisolasjon og fullstendig separasjon mellom funksjonelle blokker. Det ble definert fem egenskaper for SIP [OH05] :

1. Brukerlokasjon. Bestemme tekniske parametre påkrevd for å nå endesystemet (feks. IP-adresse).
2. Brukertilgjengelighet. Bestemme tilgjengeligheten til mottager.
3. Endepunktintelligens. Bestemme medietype, parametre og endefunksjoner som kan bli brukt.
4. Sesjonsoppsett. Starte en sesjon, kontakte endesystemet og opprette sesjonsparametre for anroper og mottager.
5. Sesjonsadministrasjon. Overføring og terminering av sesjoner, forandre sesjonsparametre og benytte tjenester.

SIPs virkemåte baserer seg på å fungere samordnet med eksisterende protokoller for overføring av multimedia, ved å muliggjøre oppdagelse mellom Internettendepunkter (brukeragenter) og for å bestemme egenskaper ved en sesjon mellom disse. SIP muliggjør en infrastruktur av nettverksverter (proxyservere), der brukeragentene kan registrere seg, sende sesjonsinvitasjoner og andre forespørsler [J.R02]. En bruker er identifisert med en SIP URL, av type

sip: ola.nordmann@129.241.208.115

SIP entitetene kommuniserer ved å benytte transaksjoner. Disse er av typen: REGISTER, INVITE, ACK, CANCEL, BYE, OPTIONS. Figur 2.6 viser hvordan en enkel sesjon kan foregå.Styrken i SIP er at det er en relativt enkel protokoll, som samtidig prøver å være abstrakt fra spesifikk bruk. Det betyr at sesjonene fungerer uavhengig av underliggende transportprotokoller, og uavhengig av hvilken type sesjon som blir etablert. SIP brukes bare til opprettelse av sesjonen, og kan dermed transportere objekter den selv ikke forstår.



Figur 2.6: Enkle SIP-transaksjoner mellom to brukeragenter via to proxyer. Nummereringen viser rekkefølgen på transaksjonene. Figuren er modifisert fra [J.R02]

Kapittel 3

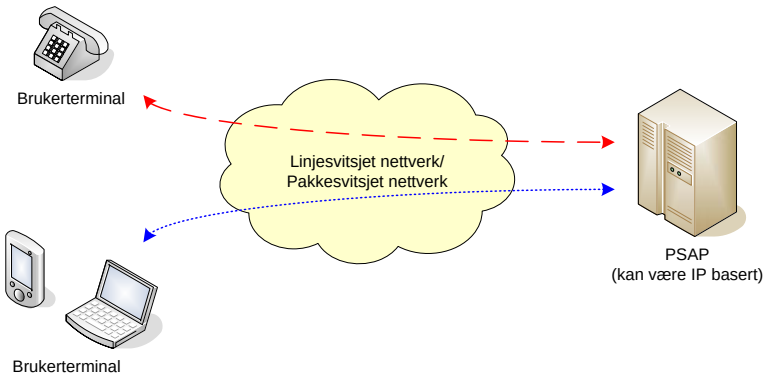
Hoveddel

I denne delen skal vi se på løsninger for et ende-til-ende IP-basert nødmeldesystem. Diverse krav og utfordringer kartlegges først for å få en bedre forståelse av systemet, med fokus på krav til lokalisering av brukerklient og tjenestekvalitet over IP. For posisjonsinnhenting drøftes også ulike forslag for lokasjonstjenester: GPS, tredjeparts lokasjonsmegler, og lokasjonsregister. Videre presenteres allerede etablerte løsningsmodeller og arkitekturer fra blant annet IETF og 3GPP. Basert på disse foreslår vi en arkitektur for et nødmeldesystem i Trådløse Trondheim. Fokuset for denne løsningen er posisjonsinnhenting og geografisk ruting. Til slutt beskrives hvordan ekstra funksjonalitet på klientsiden implementeres i form av en plug-in løsning.

3.1 Konseptuell modell for et ende-til-ende IP-basert nødmeldesystem

Hensikten med et nødmeldesystem er å raskest mulig tilby assistanse ved en nødsituasjon. Det er også essensielt at det er enkelt for allmennheten å benytte seg av systemet. Et ende-til-ende IP-basert nødmeldesystem bygger videre på konseptet fra POTS-systemet hvor brukeren anvender en lett tilgjengelig terminal for å kontakte nødsentralen, som igjen sørger for utrykning til korrekt lokasjon. Hovedforskjellen mellom disse systemene ligger i infrastrukturen mellom bruker og nødsentral, samt i brukermønsteret. POTS er et dedikert linjebasert nettverk for taletrafikk, og brukerterminalene er primært ikke-nomadiske og kan derfor tilegnes en fast lokasjon (dette systemet har etterhvert integrert seg med ulike mobile nettverk, som igjen har skapt nye utfordringer). IP-nettverk er pakkesvitsjet og beregnet for alle typer trafikk, og brukerne er ofte nomadiske. For å få til et effektivt ende-til-ende IP-basert nødmeldesystem kreves derfor tre basisfunksjoner:

- Prioritert ruting til PSAP
- Identifisering av avsender
- Lokalisering av avsender



Figur 3.1: Overordnet modell for nødmeldesystem.

3.2 Utfordringer relatert til VoIP for nødanrop

Ved innføring av VoIP for nødanrop oppstår det en rekke utfordringer som er viktig å identifisere slik at det er mulig å finne en komplett løsning på det vedrørende problemet. Mange av utfordringene skyldes krav til lokasjon. Dette er et krav som ikke er tatt hensyn til ved utbygging av dagens IP-nettverk, og derfor er det vanskelig å implementere dette på en rimelig og effektiv måte. I dette kapittelet skal vi se nærmere på hvilke utfordringer som oppstår og også hva som er årsaken til utfordringene.

3.2.1 Aktører

I VoIP-sesjoner er det som oftest flere parter involvert enn bare anroper og mottaker:

- *Endebruker:* Endebrukeren er personen som benytter seg av VoIP-tjenesten. I et nødmeldesystem vil endebrukeren være den eller de som er i nødsituasjonen og den som håndterer anropet i en nødsentral.
- *Tjenestetilbyder:* Tjenestetilbyderen er instansen som tilbyr den aktuelle tjenesten, i dette tilfellet VoIP. Tjenestetilbyderen kan være, og er ofte, uavhengig av de underliggende aksessnettverkene til brukerne av tjenesten.
- *Internettilbyder:* Internettilbyder sørger for at endebrukeren har tilknytning til Internett. Brukeren betaler da for et abonnement hos Internettilbyderen, som i gjengjeld tilbyr brukeren nettverkskapasitet i forhold til abonnentavtalen.
- *Aksessnettilbyder:* Aksessnettilbyderen er ansvarlig for den fysiske koplingen mellom bruker og resten av Internett. Det finnes flere aksessnetteknologier, men den vanligste i Norge i dag er DSL[1].

Alle disse aktørene er like viktige for å tilby en VoIP-tjeneste, men det er ikke alltid tilfellet at hver aktør er en uavhengig instans. For eksempel kan Internettilbyderen også være eier av aksessnettverket (alternativet er å leie fra en aksessnettilbyder), og på samme måte kan tjenestetilbyder og Internettilbyder være en og samme instans, noe som har blitt mer og mer vanlig. I store universitetsnettverk kan også universitetet som én instans tilby alle disse tjenestene.

I et nødmeldesystem er det essiensielt at nødsentralen lærer seg endebrukerens lokasjon. Dette kan gjøres ved å kartlegge aksessnettverkets infrastrukur i et lokasjonsregister [kap. 3.4.2]. For eksempel kan et aksesspunkt plassert i NTNUs elektrobygg mappes til MAC-adressen 00-0c-cf-32-48-00. Brukerklienter tilkoblet dette aksesspunktet vil da befinne seg i nærheten av aksesspunktets lokasjon. Ergo, mappingen mellom aksesspunkt og brukerlokasjon må foregå i aksessnettverket. Det vil derfor ikke være mulig for en uavhengig tjenestetilbyder å finne brukerens lokasjon uten en direkte relasjon til aksessnettverket.

3.2.2 Mobilitet

Et IP-basert endepunkt kan ha forskjellig bruksmønster avhengig av brukeren og terminaltypen:

[1] Digital Subscriber Line

- *Statiske endepunkter:* Statiske endepunkter har et fast tilknytningspunkt og en fast lokasjon. Dette kan typisk være en hjemme-PC eller en IP-telefon.
- *Nomadiske endepunkter:* Nomadiske endepunkter forandrer ofte lokasjon, men ikke under bruk. Det vil si at endepunktet vil ha samme lokasjon under én sesjon. Dette er typisk for mellomstore brukerterminaler som for eksempel bærbare datamaskiner (laptop/notebook).
- *Mobile endepunkter:* Mobile endepunkter forandrer lokasjon kontinuerlig, også under en sesjon. Dette kan typisk være en Pocket PC eller mobiltelefoner med støtte for WLAN.

I den senere tid har fokuset på mobilitet økt og vi ser en klar trend mot mobile brukerterminaler. Tidligere var de aller fleste IP-baserte brukerterminaler ikke-mobile, eller statiske. Selv om det fortsatt eksisterer en stor andel av disse terminalene (i noen sammenhenger vil disse også være bedre egnet), har vi i dag også en betydelig andel av nomadiske og mobile terminaler. Med dette har også tjenestetilbudet forandret seg. IPv4 har utviklet seg til IPv6, og denne protokollen er bedre egnet for mobilitet. Dette betyr at IP-baserte tjenester, som for eksempel VoIP, også er aktuelle for mobile terminaler.

Et fast eller statisk endepunkt kan finne og konfigurere sin lokasjon ved installasjon. En kontinuerlig oppdatering av lokasjon er derfor ikke nødvendig. I motsetning til dette har mobile endepunkter et mye større behov for lokasjonsoppdatering. Det er viktig at mottaker får avsenders nåværende lokasjon, og ikke lokasjonen brukeren hadde for noen minutter siden. Dette er spesielt viktig i sammenheng med et nødanrop hvor utrykningsmannskapet skal være på åstedet så fort som mulig.

3.2.3 Propagasjonsevne i trådløse teknologier

Fysiske hindre svekker propagasjonsevnen til trådløse teknologier som GPS og WLAN. Det er derfor vanskelig å lokalisere terminaler som befinner seg innendørs ved hjelp av trådløs triangulering. Til tross for at begge teknologiene opererer i samme frekvensbånd (UHF[2]) har WLAN likevel bedre propagasjonsevne enn GPS. Dette skyldes de enorme avstandsforskjellene på signalkildene. Signalet fra GPS-satellitten er betydelig redusert når den kommer frem til mottakeren. Assisted GPS [kap. 2.4.2.2] er ett forslag for å løse denne problemstillingen. For WLAN er det ofte aktuelt å bruke såkalte "hotspots". Dette er trådløse aksesspunkt plassert innendørs på flyplasser, togstasjoner, kjøpesentre, osv.

3.2.4 Protokollstakken

Tjenester som VoIP og MMoIP har strenge krav til tjenestekvalitet (Quality of Service) [kap. 3.3.3]. Forsinkelse og tap av IP-pakker vil skape forstyrrelser og være med på å påvirke sanntidsegenskapene til en pågående sesjon. Det er en nødvendighet at datapakker som originerer fra et nødanrop blir prioritert fremfor andre datapakker. På IP-laget har både IPv4 og IPv6 støtte for ulike tjenesteklasser ved hjelp av et felt for identifisering av tjenesteklassen i pakkens topptekst. DiffServ[3] er en nettverksarkitektur som behandler og prioriterer IP-pakker etter tjenesteklassene.

[2] Ultra High Frequency - 300-3000MHz
[3] Differentiated services

På applikasjonslaget er det også nødvendig med prioritering av signaleringsmeldinger i nettverkskomponentene. For eksempel i en utgående SIP-proxy er det essensielt at nødanropssesjoner blir prioritert fremfor vanlige SIP-sesjoner og at de også får tildelt de nødvendige ressursene. [HS06] foreslår to ekstra felt i SIP-hodet for å gjøre dette; *Resource-Priority* og *Accept-Resource-Priority*.

3.3 Krav til nødmeldesystem

Sluttbruker stiller diverse krav til systemet. Sluttbruker i denne konteksten er AMK-sentralen og personen som foretar nødanropet. Dette kan for eksempel være krav om nøyaktig posisjonering av bruker eller rask utrykningstid. Med dette stilles også strenge krav til den underliggende teknologien. Hvis det skal være mulig for en person å ringe AMK-sentralen, må det være en garanti for aksess og tilgjengelighet i pakkenettverket. Dette kapittelet kartlegger noen av de viktigste kravene tilknyttet en nødtjeneste i Trådløse Trondheim.

3.3.1 Krav til infrastruktur

Nødtjenesten stiller diverse krav til nettverkets infrastruktur. [HS07] gir en grundig beskrivelse av krav til infrastrukturen i et ende-til-ende IP-basert nødnett. Her skal vi kort se på de aller viktigste kravene.

- *Tilgjengelighet til lokasjonstjenestene:* Dersom en bruker skal ha mulighet for å sende med sin posisjon ved et sesjonsoppsett, **må** brukeren også ha tilgang til en lokasjonstjeneste. Det er ikke rimelig å anta at alle brukerterminaler har GPS-funksjon, så derfor må alternative lokasjonstjenester benyttes. Det må være mulig for hvem som helst å benytte seg av GeoPos og/eller lokasjonsregisteret. Det vil si at også fremmedbrukere skal ha øyeblikkelig tilgang ved en nødsituasjon. I konteksten nødtjeneste bør det også være en form for redundans av lokasjonsmeglere. På denne måten reduseres konsekvensene ved systemfeil, og tilgjengeligheten økes.

- *Støtte for flere nødnummerstandarder:* Nødmeldesystemet **bør** ha støtte for flere forskjellige standarder, blant annet 112 som er foreslått av EU. På denne måten kan turister som befinner seg i Trondheim ringe sitt lands nødnummer og likevel nå fram til en nødsentral.

- *Prioritering av nødtjenester:* All datatrafikk som genereres i forbindelse med nødtjenester, både signaleringsmeldinger og VoIP/MMoIP-pakker, **må** prioriteres fremfor annen datatrafikk. På denne måten blir forsinkelsen så liten som mulig. Et scenario kan være et aksessnett med mange brukere som benytter seg av en tjeneste for streaming av film. Dette skaper mye trafikk i nettet, og også forsinkelser og pakketap. Prioritering av nødtjenesten vil være kritisk. Måten dette gjøres på er ved klassifisering av tjenester i nettverket. Pakker som tilhører tidssensitive tjenester blir merket som høyprioritetstrafikk, og får bedre transmisjonsforhold enn klasser med lavere prioritet.

- *Flere kommunikasjonsmodi:* Nødtjenesten **bør** ha støtte for ulike medietyper som audio, video og tekst. Etterhvert som de trådløse aksessnettverkene har fått bedre kapasitet og ytelse, har det vært naturlig å tilføre nye tjenester som Internett, epost, videosamtale og mediestreaming. Nødtjenesten kan utnytte fordelen ved videosamtaler; anroper kan lettere forklare en nødsituasjon ved å filme omstendighetene, eller så kan nødsentralen hjelpe til før utrykning ved å for eksempel vise førstehjelp.

- *Oppetid:* Dersom nødtjeneste over VoIP skal benyttes, **må** en være oppmerksom på de foreliggende tekniske begrensningene. Det nåværende telenettet, POTS, har

utviklet seg igjennom en rekke år, og resultatet av dette er et veldig stabilt og pålitelig system. Fordi dagens pakkebaserte nettverk fortsatt er under utvikling vil det være nødvendig å ta forbehold til disse begrensningene. Kommunikasjon over IP var også opprinnelig tenkt som en "best-effort" løsning.

- *Geografisk ruting:* Ved nødanrop må infrastrukturen sørge for å rute meldingene til nærmeste endepunkt eller nettverkselement i forhold til den geografiske lokasjonsinformasjonen i meldingen. Det vil si at et nødanrop med opprinnelse i Trondheim eller omegn, skal automatisk rutes til AMK-sentralen i Trondheim. På denne måten vil kommunikasjonsstien bli kortest mulig, og i tillegg vil den nærmeste nødsentralen behandle nødanropet og utrykningstiden vil bli vesentlig kortere.

- *Lokasjonsformat:* En lokasjon kan være enten sivil eller geodetisk. Det er et krav til nødmeldesystemet at lokasjonen beskrives på et standardformat. IETF har beskrevet XML-baserte formater for sivil og geodetisk lokasjon i henholdsvis [MT07b] og [MT07a].

3.3.2 Brukerkrav

For "Trådløse Trondheim" er det St. Olavs Hospital som er ansvarlig for nødsentralen som mottar nødanrop fra deres ansvarsregion, og de har egne krav for hvordan et nødanrop skal fungere [Appendiks A]:

- *Feilmargin:* Ca. 20 meter. Feilmarginen skal ikke være større enn at det kan ropes og svares. Med trådløs teknologi i store bygninger kan derfor 20 meter være for mye.

- *Tidsforsinkelse:* Primært ingen, sekundært så liten som mulig. Helst kontinuerlig oppdatering av lokasjon.

Til sammenligning har FCC satt som krav for mobiltelefon at feilmarginen skal kunne fastslås til lavere enn 50m 67% av tiden, og 150m 95% av tiden. FCC har ikke satt krav til høydemåling [HS02].

3.3.3 Krav til tjenestekvalitet for VoIP - Quality of Service

I et pakkesvitsjet nettverk er det vanskeligere å gi tjenestegaranti (QoS) enn i et linjesvitsjet nettverk. Et linjesvitsjet nettverk oppretter en dedikert linje for datatransmisjon, og denne varer helt til sesjonen er over. Slik kan oppnåelig kapasitet kontrolleres. Dette er ikke mulig i pakkesvitsjede nettverk, og derfor kan det oppstå forsinkelser, pakketap og variasjon i forsinkelse, jitter. Dersom VoIP skal være mulig over et pakkesvitsjet nettverk må det settes krav til tjenesten [Cor03]:

- *Forsinkelse:* En forsinkelse på over +-170 ms vil føre til at partene begynner å snakke samtidig eller så vil de avbryte hverandre.

- *Pakketap:* Tap av datapakker vil føre til tap av informasjon. Resultatet vil være en samtale som ikke er kontinuerlig, men hakkete og ujevn. Ved bruk av ITU-T G.711-kodeket vil et pakketap på 1% svekke brukeropplevelsen betydelig.

- *Jitter:* Variasjoner i forsinkelse, også kalt jitter, vil oppstå på grunn av ulik prosesseringstider i rutere og pakkenes ulike transmisjonsstier. VoIP krever en jevn dataflyt og derfor bør forsinkelsen holdes tilnærmet konstant. Ved hjelp av et jitterbuffer kan trafikken formes slik at dette er mulig.

3.3.4 Krav til sikkerhet

Sikkerhet er et nøkkelord for et IP-basert nødmeldesystem, men oppgaven tar ikke dette aspektet i betraktning ved valg av arkitektur da dette er en avgresning. Likevel er det viktig å kartlegge systemtrusler og svakheter, og også diverse mottiltak:

- *Tilgjengelighet:* Et nødmeldesystem skal alltid være tilgjengelig, uansett forhold. Det vil blant annet si at systemet må være robust i forhold til krisesituasjoner (jordskjelv, orkan, osv.). Eventuelle feil i systemet må heller aldri gå ut over endebrukeren. Dersom endebrukeren for eksempel utfører et nødanrop som fører til at systemet på en aller annen måte anser brukeren for mistenkelig sikkerhetsmessig, må anropet likevel håndteres. Den største trusselen for nødmeldesystemet er DoS[4] angrep. Formålet med et DoS angrep er å hindre brukere tilgang til tjenesten.

- *Dataintegritet:* Kryptering og autentisering av bruker er viktig for å sikre integriteten til informasjon som overføres. Dette gjelder spesielt for trådløse teknologier som WLAN og UMTS da disse kringkaster all informasjon til nærliggende omgivelse. TLS[5] er foreslått av IETF for kryptering av data. Hvis endebrukeren ikke klarer å autentisere seg må likevel tjenesten være tilgjengelig (se punktet over). Det er også essensielt å forebygge maskering av nettverkskomponenter og tjenester; det må ikke være mulig for en ondsinnet bruker å maskere seg som lokasjonstjenesten eller nødsentralen.

- *Vern av lokasjonsinformasjon:* Lokasjonsinformasjon må ikke være tilgjengelig for andre enn den som foretar et nødanrop. Dette er meget sensitiv informasjon som lett kan misbrukes. Et lokasjonsregister bør derfor ha strenge restrikasjoner for gyldige brukere og også autentisering av brukere. I tillegg bør lokasjonsinformasjon hemmeligholdes ved transmisjon, for eksempel ved kryptering, eller ved å sende med en peker til lokasjonsverdien i stedet for selve verdien.

[4] Denial-of-Service
[5] Transport Layer Security

3.4 Posisjonsinnhenting

Dette delkapittelet beskriver de valgene som må tas for hvordan posisjonen til en terminal skal innhentes, og hvilke konsekvenser dette får for arkitekturen i et nødmeldesystem.

3.4.1 Utfordringer for IP-baserte terminaler

Et IP-basert nødmeldesystem er avhengig av å kunne lokalisere brukerne. Kapittel 2.2.4 beskriver vanskelighetene ved å lokalisere brukere basert på IP-adresse. I en SIP-basert arkitektur er brukerne identifisert med SIP-adresser, som ikke er tilknyttet en fast lokasjon eller en IP adresse. SIP-signalering traverserer ofte via flere proxy-servere eller NATer[6], og derfor vil ikke en IP-basert PSAP alltid ha tilgang på innringerens IP-adresse. Ergo, lokalisering av en bruker tilknyttet et IP-basert nettverk kan ikke gjøres nøyaktig nok ved bruk av tradisjonelle identifikasjonsmetoder [HS02].

3.4.2 Arkitektoniske valg

Det finnes fire hovedløsninger for hvilke elementer i arkitekturen som er ansvarlig for anskaffelse av lokasjonsinformasjon [BR07]:

- *Brukeren:* Brukeren kan selv konfigurere sin brukerklient med en lokasjon. Dette krever mye ettersyn fra brukeren sin side dersom lokasjonen skal være gyldig, og er derfor et dårlig alternativ. Hvis brukeren for eksempel er ute og reiser, og glemmer å oppdatere lokasjonen, vil meldingen rutes til feil nødsentral. I tillegg krever det at brukeren kjenner til sin lokasjon, og ikke taster feil.

- *Endesystemet/Terminalen:* Ved hjelp av GPS eller A-GPS kan terminalen selv finne sin egen lokasjon. Kapittel 3.6.2 beskriver GPS som lokasjonstjeneste.

- *Aksessnettet:* Lokasjonsregistre inneholder en planskisse av infrastrukturen i aksessnettet samt tilknyttede brukerklienter. Det vil si at hvert nettverkselement kan avbildes til en fast lokasjon. Dette fungerer best i statiske nettverk som for eksempel DSL-nettverk i boligstrøk. På denne måten kan hver residens (det vil si tilknytningspunktet til nettverket) registreres med en fast lokasjon i registeret. Dette tilsvarer på mange måter registrene som finnes for fasttelefoni. Løsningen kan også fungere bra i områder med såkalte WiFi "hotspots" (cafeer, restauranter og lignende). Det største problemet med lokasjonsregistre oppstår når brukerne har veldig stor rekkevidde innenfor et aksesspunkt. Da kan det være vanskelig å finne brukerens eksakte lokasjon ved en nødsituasjon.

- *Tredjepart tilbyr lokasjon:* Trådløs triangulering utføres mellom elementer i nettverksinfrastrukturen for å finne lokasjonen til en brukerklient. GSM og WLAN er eksempler på denne teknologien.

3.4.3 Lokasjonsoppdatering

Som nevnt i avsnittet over er det nødvendig for mobile brukerklienter å utlyse sin siste tilgjengelige lokasjon ved et nødanrop. Dette for å få en så nøyaktig peiling av klienten som mulig. Det er hovedsakelig to metoder for lokasjonsoppdatering:

[6] Network Address Translation

- Klienten kan jevnlig spørre om sin lokasjon. Dette fører til mye overhead i nettverket og det er også vanskelig å bestemme et tidsintervall mellom hver spørring. Dersom tidsintervallet er på fem minutter vil klientens lokasjon ha forandret seg mye hvis klienten befinner seg på en buss eller på et tog.

- Klienten kan spørre om sin lokasjon ved oppsett av samtale. Dette fører til en ekstra tidforsinkelse som kan vise seg å være kritisk ved et nødanrop.

3.4.4 Lokasjonsinformasjon

Lokasjonsinformasjon består av forskjellige lokasjonsparametre, som ofte er sammensatt i et *lokasjonsobjekt*. [BR07] fastslår at alle lokasjonsobjekter **må** leveres til nødsentralen. I enkelte tilfeller kan lokasjonsobjekter fra forskjellige lokasjonskilder forekomme, og da må alle disse sendes til nødsentralen. [BR07] ønsker å tilstrebe en løsning der nødsentralen selv tolker lokasjonsinformasjonen.

For å forenkle nødsentralens tolkning av lokasjonsinformasjonen er det nødvendig med enkelte obligatoriske lokasjonsparametre, uavhengig av lokasjonsobjektets format. Tabell 3.1 beskriver de viktigste lokasjonsparametrene.

Lokasjonsparametre	**Forklaring**
Lokasjon	Sivil eller geodetisk. Det bør også angis hvilken type koordinatformat som er benyttet.
Kilde	Metoden benyttet for å anskaffe lokasjonen. (For eksempel GPS, manuellt inntastet, aksessnettverket). Muliggjør blant annet prioritering hvis nødsentralen mottar flere lokasjonsobjekter fra samme terminal.
Generator	Frembringer av lokasjonsinformasjonen. Kan brukes som lokasjonsindikasjon hvis lokasjonen er ødelagt eller villedende. Generator er ofte autoriteten som har signert lokasjonen. For eksempel kan en generator være "NTNU", som følgelig betyr at anropet må rutes til nødsentralen som har Trondheim som ansvarsområde.
Rutinginformasjon	Definerer hvilken lokasjonsinformasjon som blir brukt til ruting, slik at alle rutingavgjørelser baserer seg på lik informasjon.

Tabell 3.1: De viktigste lokasjonsparametrene som skal bli sendt til nødsentralen ifølge [BR07].

3.4.5 Transport av lokasjonsinformasjon

Lokasjonsinformasjonen må sendes med anropet. Hvis SIP brukes som signaleringsprotokoll kan SIP-meldingene modifiseres, ved å legge til ekstra informasjon.

[JP07] beskriver en *geolocation header*, som kan legges ved de fleste typer av SIP-meldinger (INVITE, REGISTER, OPTIONS, UPDATE, MESSAGE, SUBSCRIBE og NOTIFY). Geolocation header inneholder enten en referanse til en lokasjon eller et lokasjonsobjekt i meldingskroppen. Forskjellen på disse er beskrevet i kapittel 3.4.6. Et

eksempel på et lokasjonsobjekt er gitt i kapittel 3.4.7.

I [MH06] benyttes ekstra attributtfelt for å utvide SIP-meldingene slik at de kan benyttes i nødanropstjenesten. Denne løsningen vedlegger lokasjonsparametrene som sos-attributter i SIP-meldingen uten å lage en egen header:

```
a=<attribute>:<value>
a=sos:lengdegrad/breddegrad/IP adresse/NAP MAC-adresse
```

Kodeeksempel 3.1: sos-attributter i SIP INVITE-melding

Det mest hensiktsmessige vil være å legge med lokasjonsinformasjonen i SIP INVITE-meldingen. Denne sendes fra anroper før samtalen er etablert, og mottageren får lokasjonsinformasjonen før de svarer på anropet.

3.4.6 Lokasjonsinformasjon som fast verdi eller som referanse

Endepunktet kan tilegne seg lokasjonsinformasjon enten som en fast verdi eller som en referanse/peker til lokasjonsregisteret. Dersom den faktiske verdien benyttes, kan klienten sende denne videre med i signaleringsmeldingen, og det vil være mulig for mellomliggende nettverkselementer å øyeblikkelig benytte seg av denne informasjonen for videre ruting. Ulempen dette medfører er større overhead på signaleringsmeldingene (også avhengig av formatet på lokasjonsinformasjonen). Fordelen med å sende lokasjonsinformasjon som en peker er at overheaden på meldingene blir mindre. Pekeren består av en URI som beskriver hvilket lokasjonsregister som skal benyttes, og hvilken klient som skal finnes. På denne måten må nettverkskomponentene selv gjøre en spørring mot lokasjonsregisteret for å finne klientens faktiske lokasjon. Dette er en prosess som tar tid og bør derfor ikke utføres flere ganger ved sesjonsoppsettet. Et annet kritisk problem oppstår hvis registeret ikke er tilgjengelig på det tidspunktet spørringen utføres. Den største fordelen ved bruk av en pekerverdi er at lokasjonen er ukjent for alle nettverkskomponentene, det vil si også for ondsinnede aktører som kan utnytte slik informasjon. Ved kontrollert brukertilgang til lokasjonsregistrene kan disse aktørene holdes utenfor.

3.4.7 Eksempel på lokasjonsformat: PIDF-LO

Lokasjonsinformasjon kan representeres på forskjellige måter, men det er hensiktsmessig å utforme en felles standard. [Pet05] beskriver et XML-basert objektformat for å transportere geografisk informasjon over Internett. Dette lokasjonsobjektformatet er basert på *Presence Information Data Format (PIDF)*, som ble laget med hensyn på transport av personvernsensitiv tilstedeværelsesinformasjon. Det nye formatet er kalt *PIDF-LO*, der LO betyr lokasjon.

PIDF-LO utvider elementet kalt *status* i XML-skjemaet til PIDF, med et element kalt *geopriv* (GeoPriv er en personvernbasert arkitektur beskrevet i kapittel 3.7.6). geopriv-elementent inneholder to obligatoriske og to valgfrie underelement, henholdsvis:

- *location-info:* Lokasjonsinformasjon. Herunder **må** et GML[7]-basert element vedlegges, og i tillegg kan et valgfritt sivillokasjonsformat definert i [Pet05] vedlegges.

[7] Geography Markup Language

Det GML-baserte elementet er beskrevet i [Wik07b], og angir forskjellige lokasjonsparametre.

- *usage-rules:* Fire valgfrie anvendelsesregler:
  - *retransmission-allowed:* Angir om mottakeren av lokasjonsinformasjonen kan dele den med en tredjepart. Verdien settes til ja eller nei, men vil **alltid** være nei om ikke annet er oppgitt.
  - *retention-expires:* Angir en absolutt dato for når mottageren av lokasjonsinformasjonen ikke lenger kan besitte den. Standard verdi er 24 timer etter tidsstempelet som finnes i PIDF-objektet. Hvis tidsstempelet ikke finnes, er det 24 timer fra da lokasjonsinformasjonen ble mottatt. Hvis tidsstempelet er tilbake i tid, vil lokasjonsobjektet bli avvist.
  - *ruleset-reference:* URI til en definisjon av regler som gjelder for lokasjonsobjektet.
  - *note-well:* Tekstfelt med andre generelle regler for personvern.
- *method:* Metode som er benyttet for å bestemme lokasjonen (for eksempel GPS).
- *provided-by:* Entitet som anskaffet lokasjonen.

Eksempel på et PIDF-LO lokasjonsobjekt (hentet fra [Pet05]):

```
1  <?xml version="1.0" encoding="UTF-8"?>
2   <presence xmlns="urn:ietf:params:xml:ns:pidf"
3       xmlns:gp="urn:ietf:params:xml:ns:pidf:geopriv10"
4       xmlns:gml="urn:opengis:specification:gml:schema-xsd:feature:v3.0"
5       entity="pres:geotarget@example.com">
6    <tuple id="sg89ae">
7     <status>
8      <gp:geopriv>
9       <gp:location-info>
10        <gml:location>
11          <gml:Point gml:id="point1" srsName="epsg:4326">
12            <gml:coordinates>37:46:30N 122:25:10W</gml:coordinates>
13          </gml:Point>
14         </gml:location>
15       </gp:location-info>
16       <gp:usage-rules>
17         <gp:retransmission-allowed>no</gp:retransmission-allowed>
18         <gp:retention-expiry>2003-06-23T04:57:29Z</gp:retention-
               expiry>
19       </gp:usage-rules>
20     </gp:geopriv>
21    </status>
22    <timestamp>2003-06-22T20:57:29Z</timestamp>
23   </tuple>
24  </presence>
```

Kodeeksempel 3.2: PIDF-LO-lokasjonsobjekt, som inneholder et geopriv-element og underelementene *location-info* og *usage-rules*.

3.5 Geografisk ruting

Det finnes flere forskjellige kriterier for ruting av IP-pakker. Dette skyldes ulike behov fra tjenester og i infrastukturen. For eksempel kan IP-pakkene rutes på grunnlag av linkkapasitet. Det vil si at pakkene rutes videre på den linken som yter best for øyeblikket. Geografisk ruting betyr at IP-pakkene rutes på grunnlag av brukerlokasjon. En nødsentral har ansvarsområde for en by eller en kommune. Det kan også være ulike sentraler for ulike tjenester; brann, politi og ambulanse. Klienter som foretar nødanrop i dette ansvarsområdet skal da havne hos den tilhørende nødsentralen. For å hindre store forsinkelser er det essensielt at anropet havner hos riktig nødsentral.

Det er ikke nødvendig med en helt eksakt lokasjon ved geografisk ruting. Det vil ofte være nok med en identifikator av nettverket eller eventuelt tilkoblet aksesspunkt. Et nødanrop som originerer fra Trådløse Trondheim er nødt til å komme fra Trondeim (så sant ikke VPN-teknologi benyttes), og skal derfor rutes til nødsentralen i byen. For større ISP-nettverk er det ofte nødvendig å vite hvor i nettverket brukeren er tilknyttet.

Avhengig om det er en statisk, nomadisk eller mobil brukerterminal, er det flere framgangsmåter for geografisk ruting til korrekt nødsentral [EMT06]:

- *Det geografiske området til IP-adressen er kjent:* Dette er en realitet på landsbasis. En brukerterminal kan mappes til en nasjon og en ISP, men på grunn av dynamiske IP-adresser er det ikke mulig å få en bedre lokasjon enn dette.
- *Lokasjon til aksesspunkt kjent:* Som nevnt over er det nok å vite aksesspunktets lokasjon for å foreta geografik ruting til korrekt nødsentral.
- *Bruker oppdaterer rutinginformasjon ved bruk av tjenesten:* Ved et nødanrop sørger bruker selv for å oppdatere rutinginformasjon i henhold til lokasjonsinformasjon. Dette er et alternativ som er best egnet for statiske brukerterminaler da disse vil benytte seg av samme nødsentral ved hvert anrop.
- *Nettverket oppdaterer rutinginformasjon ved bruk av tjenesten:* I stedet for å la brukeren oppdatere rutinginformasjonen, kan denne funksjonen legges i nettverket. Nettverket må da ha lokasjonsinformasjon for brukeren.

I [TH07] spesifiserer IETF en protokoll for geografisk ruting. Protokollen oversetter lokasjonsinformasjon til en tjeneste-URL slik at det er mulig å finne nødsentral med jurisdiksjon tilsvarende lokasjonen og ønsket tjeneste [kap. 3.7.3.3].

3.6 Lokasjonstjenester

Hvilken metode som benyttes for å innhente lokasjon avhenger av hvilket scenario som er mest aktuelt. I dette delkapittelet beskrives de tre lokasjonstjenestene som ble vurdert i implementeringen; GPS, GeoPos/Cisco Location Appliance og lokasjonsdatabase basert på terminalens MAC-adresse. Funksjonaliteten og anvendeligheten til disse tre blir beskrevet nedenfor, basert på egenskaper en lokasjonstjeneste innehar.

3.6.1 Egenskaper til lokasjonstjenester

Det er hensiktsmessig å definere de viktigste egenskapene til lokasjonstjenester i et nødmeldesystem, fordi lokasjonstjenestene kan ha forskjellige egenskaper, eller tilfredstille egenskapene i forskjellig grad. Når man skal velge en best egnet lokasjonstjeneste er det derfor viktig å prioritere de mest relevante egenskapene i forhold til hvordan totalsystemet skal fungere.

Egenskaper til lokasjonstjenester:

- *Oppstartsforsinkelse (sekunder):* Den ekstra tiden det tar for en terminal å innhente posisjonen når en terminal blir slått på.
- *Tidsforsinkelse (sekunder):* Tiden det tar for klienten å innhente posisjonen.
- *Feilmargin (meter):* Avvikende avstand fra den reelle posisjonen.
- *Administrasjon:* Arbeid som kreves for å opprettholde driften av lokasjonstjenesten.
- *Overhead i nettverket:* Ekstra trafikk i nettverket på grunn av lokasjonstjenesten.
- *Innendørs dekning:* I hvilken grad lokasjonstjenesten har støtte for innendørs dekning.
- *Uavhengig av underliggende nettverk:* I hvilken grad lokasjonstjenesten er uavhengig av det underliggende nettverket.
- *Uavhengig av klientens terminal:* Om lokasjonstjenesten er avhengig av ekstra funksjonalitet eller programvare på terminalen for å fungere.
- *Forskjellige lokasjonskilder:* Hvorvidt lokasjonstjenesten har flere alternativer for å innhente posisjon. For eksempel om den kan innhente posisjonen til både IP-baserte terminaler og mobiltelefoner.
- *Beskrivede data:* Hvor beskrivende posisjonsdataene innhentet av lokasjonstjenesten er. For eksempel om de inneholder høyde over havet, etasjenummer, siviladresse etc.

3.6.2 GPS

GPS opererer uavhengig av underliggende nettverk, og er avhengig av applikasjonsstøtte i terminalen til klienten i form av en GPS-mottager. En slik GPS mottager kan kalkulere posisjonen utfra et tidsstempel, satelittposisjonen og forsinkelsen av det mottatte signalet.

GPS har sin største styrke i lav feilmargin og uavhengighet av det underliggende nettverket. For sivile GPS-mottagere er feilmarginen innenfor 15 meter 95% av tiden. I de aller fleste tilfeller vil feilmarginen ligge mellom 5 og 10 meter under normale forhold. Våre tester viser imidlertid at GPS er avhengig av å være "varm" for å gi tilfredsstillende resultat [kap. 5.3]

GPS er uavhengig av det underliggende nettverket, noe som gjør at enhver terminal kan benytte GPS (hvis GPS-mottager er implementert). Dette er altså en plausibel løsning for både mobiltelefoner og IP-baserte terminaler. Uavhengigheten medfører også minimal belastning på nettverket, det vil si ingen ekstra overhead og ingen nettverksadministrasjon. Hvis en ser bort fra oppstartsforsinkelsen, er tidsforsinkelsen på en GPS-forespørsel lav nok til en nødmeldetjeneste, men dette er avhengig av at GPS-mottageren er aktivert. En annen viktig fordel med GPS er at den kan kalkulere Z-koordinater, som angir høyde over havet. Dette er mulig fordi koordinatene blir kalkulert av fire satelitter.

GPS har to kritiske svakheter. For det første gir GPS-teknologien per dags dato tilnærmet ingen dekning innendørs. Dette er åpenbart en forutsetning for et fullt funksjonibelt nødmeldesystem. Løsningen på problemet kan imidlertid ligge i den tekologiske utviklingen. GPS er et satsningsområde både innenfor militært bruk og kommersialiserte navigasjonstjenester. Nye teknologiske løsninger for å øke anvendbarheten til GPS, som for eksempel A-GPS [kap. 2.4.2.2], beviser dette. Den andre kritiske svakheten til GPS er oppstartsforsinkelsen. Når en terminal slås på må GPS-mottageren orientere seg, og søke opp satelitter. GPS-mottageren på vår pocket PC må kontakte fire satelitter før den kan kalkulere posisjonen. Oppstartsforsinkelsen varierer veldig, men vanligvis vil den ligge over 3 minutter. Dette betyr at hvis et nødnummer blir forsøkt oppringt med en terminal som er avslått, så vil posisjonsinnhenting ved hjelp av GPS være altfor tidkrevende. Man er altså avhengig av at terminalen har vært på en liten stund, slik at GPS-mottageren har rukket å initialisere seg. GPS har også en praktisk svakhet per dags dato, ved at den ikke er standard på terminaler, verken for mobiltelefoner eller IP-baserte terminaler. Man kan nok argumentere med at GPS-teknologien øker, og det er sannsynlig at den vil bli standard på terminaler om ikke lang fremtid. Likevel vil det være begrensende for nødmeldesystemet å basere seg på en lokasjonstjeneste som ikke alle terminaler har tilgang til. En annen svakthet knyttet til GPS for vårt formål er mangel på beskrivende output. Dette er ikke en viktig faktor, da GPS gir koordinater til der GPS-mottageren befinner seg. Og utfra disse koordinatene kan annen stedsinformasjon regnes ut. Likevel kan det være nyttig med mer informasjon i enkelte tilfeller. Dette er også avhengig av serversideimplementeringen som skal tolke lokasjonsinformasjonen som blir sendt med anropet.

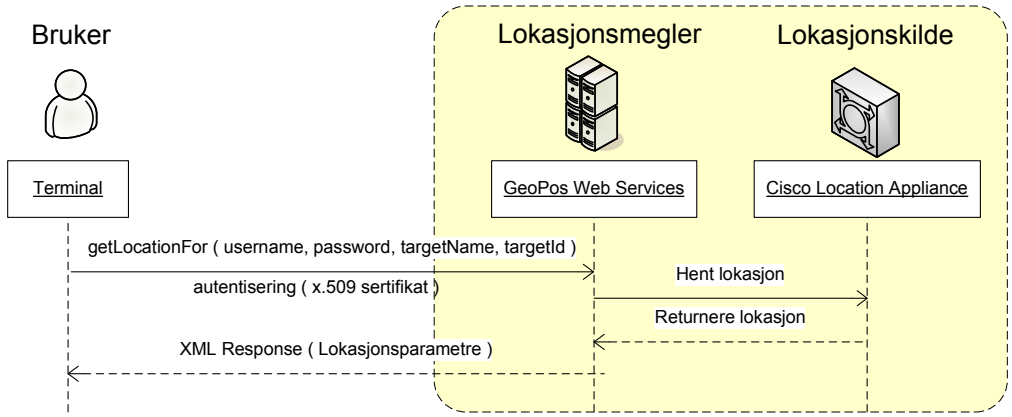
GPS er den av de tre lokasjonskildene som returnerer den mest nøyaktige posisjonen, og den gir også lav tidsforsinkelse så lenge GPS-mottageren er aktiv. GPS er tilgjengelig på alle former for terminaler, så lenge de har en GPS-mottager. Dette gjør GPS til en passende teknologi for terminaler som ikke oppholder seg innendørs, og i situasjoner der feilmarginen må være minimal.

3.6.3 GeoPos

GeoPos fungerer som en lokasjonsmegler, hvilket betyr at den kan benyttes uavhengig av lokasjonskilden den henter posisjonsdata fra. I Trådløse Trondheim blir Cisco Location Appliance benyttet, som klarer å finne lokasjonen til terminaler i store WiFI nett. Men det er også mulig å koble til andre lokasjonskilder, for eksempel for mobiltelefoner i mobile nett. Dette kan gjøres uavhengig av terminalen, som bare kommuniserer med mellomleddet GeoPos, via GeoPos Web Services.

Klienten kan koble seg opp mot GeoPos Web Services for å spørre om lokasjon til en klient, basert på MAC- eller IP-adresse. For å kunne koble seg opp kreves et tilpasset klientprogram. Dette programmet kan lages manuelt, eller genereres ved hjelp av en åpent tilgjengelig WSDL[8]-fil. For å få tilgang på posisjonsdata er det nødvendig med en brukerkonto på GeoPos, med brukernavn og passord i tillegg til et signert x.509-sertifikat. Ved vellykket autentisering, brukes SOAP-protokollen. Denne er standard i Web Services, og brukes for å sende XML-baserte meldinger over datanettverk.

Kommunikasjonen mellom klient, GeoPos og lokasjonskilde illustreres i figur 3.2. GeoPos Web Service inneholder en metode som heter "getLocationFor". Denne metoden tar inn brukernavn, passord, targetType og targetId som parametre. Disse parametrene er forklart i tabell 3.2. Brukernavn må inneholde hvilket nettverk brukeren er tilknyttet. Dette kan for eksempel være TT for Trådløse Trondheim, eller AMK for AMK-sentralen. "targetType" viser om det spørres etter MAC- eller IP-adressen til en terminal, og "targetId" er denne adressen. For at brukeren skal innhente sin egen posisjon må terminalen finne sin egen MAC- eller IP-adresse, og legge ved denne i forespørselen til GeoPos.



Figur 3.2: GeoPos fungerer som en lokasjonsmegler mellom bruker og lokasjonskilde. I "Trådløse Trondheim" er denne lokasjonskilden Cisco Location Applicance.

Den XML-baserte svarmeldingen fra GeoPos inneholder enten posisjonsdata eller en feilmelding som sier at brukeren ikke kan finnes på nettverket. Posisjonsdataene har to standardformater, MAC XML og IPv4 XML, avhengig av hvilken "targetType" som blir brukt i spørringen fra brukeren. Figur 3.3 viser hvordan en standard MAC XML-melding ser ut. Posisjonsmeldingen inneholder mye informasjon, men til vårt bruksområde er fel-

[8] Web Service Description Language

Parameter	Forklaring
username	Brukernavn:Requestor (for eksempel "olanor:AMK")
password	Passord
targetType	Adresseformat på forespørselen (for eksempel "MAC" eller "IPv4")
targetId	MAC- eller IP-adressen til terminalen som skal posisjoneres

Tabell 3.2: Parameterforklaring til metoden *getLocationFor*

tene med koordinater, *longitude* og *latitude*, mest relevant. En annen viktig attributt er *floorID* som angir hvilken etasje anropet originerer fra. Videre sendes de innhentede posisjonsdataene med anropet i en SIP-melding, der plassen er begrenset utfra størrelsen på UDP-pakken som skal sendes. Derfor er det nødvendig at klientprogrammet har en XML-parser som filtrerer ut nødvendig informasjon fra posisjonsdataene.

Koordinatene i posisjonsmeldingen er på formatet UTM, i motsetning til GPS som returnerer koordinater på formatet WGS84. Dette fører til unødvendig konvertering, en oppgave vi har tilegnet serversiden. Det hadde også vært hensiktsmessig om svarmeldingen fra GeoPos inneholdt verdier for signalstyrke og hvilket aksesspunkt terminalen er tilkoblet.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<GposResponse>
      <ResponseHeader sessionID="NOT-SET"/>
      <ResponseBody requestID="reqIdNotImplemented" version="1.0"
      locationType="CURRENT">
            <ErrorList/>
            <XYPosition>
                  <X>1200.04</X>
                  <Y>500.62</Y>
                  <Longitude>569477.0</Longitude>
                  <Latitude>7034368.0</Latitude>
                  <FloorId>23</FloorId>
                  <Elem>Sone06</Elem>
                  <Elem>Sone06</Elem>
                  <Elem>Midtbyen_Group</Elem>
                  <Elem>Midtbyen</Elem>
            </XYPosition>
            </ResponseBody>
</GposResponse>
```

Figur 3.3: Posisjonsdata fra GeoPos i MAC XML-format.

For å kunne benytte GeoPos er terminalen avhengig av ekstra funksjonalitet. Denne oppgaven beskriver arkitektur og implementering av en plug-in løsning som tilfører denne nødvendige funksjonaliteten [kap. 3.8.4]. I motsetning til GPS, der terminalen er avhengig av ekstra funksjonalitet i form av en fysisk GPS-mottager, er den ekstra funksjonaliteten nødvendig for å anvende GeoPos ikke avhengig av en fysisk modul. Plug-in løsningen er mobil og klientuavhengig, og kan i teorien lastes ned fra Internett og konfigureres til

bruk. Vår plug-in løsning er imidlertid avhengig av en VoIP-applikasjon med støtte for SIP, men dette kan også lastes ned fra Internett hvis det ikke allerede finnes på terminalen.

GeoPos er under stadig utvikling, men preges av at den ikke er en kommersialisert tjeneste. Følgene av dette er varierende tidsforsinkelse og feilmargin, avhengig av belastningen på tjenesten. Likevel er disse svakhetene tilknyttet programvare og maskinvare, og vil derfor bli forbedret i samsvar med utviklingen av CLA, GeoPos og Trådløse Trondheim.

3.6.4 Cisco Location Appliance (CLA)

CLA har høyere feilmargin enn GPS, men unngår de største svakhetene som oppstartsforsinkelse og mangel på innendørs dekning (så lenge det er nettverksdekning). I tillegg er ikke terminalen avhengig av en egen fysisk modul for å fungere, men ekstra programvare for å kommunisere med GeoPos som igjen kommuniserer med CLA. Dette gjør GeoPos og CLA til en god løsning for bynett over et begrenset geografisk område. Spesielt i områder der GPS vil fungere dårlig, er CLA kun avhengig av nettverksdekning for å fungere tilstrekkelig. Ved VoIP vil anroperen uansett være avhengig av nettverksdekning, så dermed er det implisitt at CLA er tilstedeværende ved nødanrop (forutsatt at anroperen er tilkoblet et nettverk med CLA implementert).

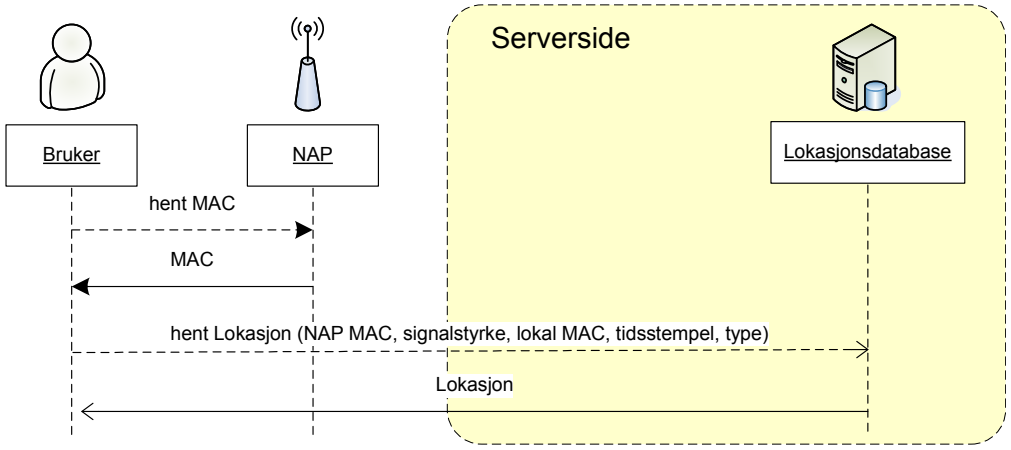
3.6.5 Lokasjonsdatabase basert på MAC

Lokasjonsdatabaser baserer seg på å lagre posisjonen til aksesspunktene i nettverket, og så tilegne samme posisjon til alle terminaler tilknyttet det samme aksesspunktet. Den største fordelen med denne løsningen er den lave tidsforsinkelsen. Når terminalen skal innhente posisjonen er denne allerede lagret, så tiden det tar å innhente posisjonen er tiden det tar å gjøre et oppslag i en database på en lokasjonsserver. Det vil heller ikke være noen oppstartsforsinkelse tilknyttet en slik løsning. I likhet med GeoPos er det nødvendig med ekstra funksjonalitet på klientsiden, i form av programvare som for eksempel en plug-in løsning, for å sende de riktige parametrene til lokasjonsserveren. Dette muliggjør en løsning uavhengig av terminaltype. Lokasjonsdatabaseløsningen har også støtte for innendørs dekning. Hvis en terminal befinner seg innendørs og er tilkoblet et aksesspunkt vil terminalen få tilegnet samme posisjon som aksesspunktet i databasen. Lokasjonsdatabaseløsningen forutsetter at aksesspunktene er statiske.

Figur 3.4 illustrerer kommunikasjon mellom bruker og lokasjonsserver. Brukeren sender NAP MAC (kan være en BSSID[9]), signalstyrke, lokal MAC og tidsstempel til serveren. Dette forutsetter at terminalen er i stand til å finne verdier til disse parametrene på egen hånd. Disse parametrene er forklart i tabell 3.3. Et alternativ til denne løsningen er å plassere en lokasjonsmegler, for eksempel GeoPos, mellom lokasjonsdatabasen og brukeren. En slik løsning ville sett ut som i figur 3.2, med lokasjonsdatabase i tillegg til, eller i stedet for, CLA.

Ved oppslag i databasen sammenlignes NAP MAC med databasens liste over NAP MAC, og den tilhørende posisjonen blir returnert. Denne lokasjonstjenesten er derfor avhengig av endel administrasjon for å kunne tillby en oppdatert lokasjonsdatabase til enhver tid.

[9] Basic Service Set Identifier



Figur 3.4: MAC-adressen til aksesspunktet til en terminal er oftest statisk, og posisjonen til denne lagres i en database slik at terminalen får samme posisjon som aksesspunktet med en viss feilmargin.

Parameter	**Forklaring**
NAP MAC	MAC-adressen til nettverksaksesspunktet. Brukes for å stadfeste hvilken NAP terminalen er tilkoblet. I trådløse IEEE 802.11-nettverk blir NAP MAC kalt BSSID.
Signalstyrke	Signalstyrken til nettverksaksesspunktet, altså NAP signalstyrke.
Lokal MAC	Terminalens MAC-adresse. Brukes blant annet til å autentisere terminalen
Tidsstempel	Tiden for forespørsel. Kan senere innhentes for å stadfeste hvor fersk lokasjonen er.
Type	Valgfritt felt som oppgir spesielle vilkår for forespørselen.

Tabell 3.3: Parameterforklaring for metoden som innhenter lokasjon for lokasjonsdatabaser basert på MAC

Feilmarginen er avhengig av hvordan terminalen er tilkoblet aksesspunktet:

- *Fast kobling:* Man bruker vanligvis en TP-kabel for å koble en terminal til et aksesspunkt. Denne kan være opptil 100 meter lang, men er vanligvis 1-5 meter. Man kan bruke SNMP[10] til å bestemme Ethernet svitsjporten til en spesifikk MAC-adresse. Slik finnes terminalens fysiske Ethernet-kontakt og lokasjon (som rom og bygning). Denne løsningen er avhengig av en nøyaktig database over ledningsnettet, men vil uansett kunne gi endel feilmargin avhengig av lengden på TP kabelen [HS02].

- *Trådløs kobling:* Det trådløse signalets rekkevidde varierer avhengig av bygningsmasse og landskap. I Trådløse Trondheim benyttes WiFi-sendere som har signalstyrke på 30-100 meter.

Lokasjonsdatabaser har noen svakheter sammenlignet med GPS og GeoPos. Den viktigste svakheten er feilmarginen. Ved å lagre posisjonen til aksesspunktet som posisjonen til terminalen vil det alltid oppstå en feilmargin. Dette vil få størst konsekvens i et trådløst nett, der det blant annet umuliggjør fastsettelse av høyde over havet. Ved å sende med signalstyrken til WiFi-signalet kan man lettere kalkulere avstanden fra aksesspunktet, men feilmarginen vil i de fleste tilfeller likevel være for høy for bruk i en nødmeldetjeneste. En annen essensiell svakhet med lokasjonsdatabaser er kostnadene ved å administrere og oppdatere databasesystemet som kreves for lagringen av posisjonen til alle aksesspunktene. I Trådløse Trondheim er det over 100 aksesspunkter, og i et større nettverk vil antallet kunne være betydelig høyere.

Lokasjonsdatabaseløsningen vil gi lavere tidsforsinkelse enn GeoPos, men betydelig høyere feilmargin. I tillegg er det høye administrasjonskostnader tilknyttet denne løsningen. Lokasjonsdatabaseløsningen er derfor en god løsning når tidsforsinkelsen skal være minimal, og litt feilmargin er akseptabelt. Dette er for eksempel tilfellet ved geografisk ruting. Her kreves bare en tilnærmet riktig posisjon for å kunne geografisk rute et anrop til rikig område. Denne egenskapen gjør lokasjonsdatabase til en relevant lokasjonstjeneste i forhold til hybride løsninger [kap. 3.6.7].

3.6.6 Alternative metoder for å innhente posisjon

I tillegg til lokasjonstjenestene denne oppgaven fokuserer på, finnes det andre foreslåtte metoder for å innhente posisjon over et IP-basert nettverk. [HS02] oppsummerer alternative metoder, der de mest relevante er:

- *Manuell konfigurasjon:* Brukeren taster manuellt inn lokasjonen sin hver gang terminalen forflytter seg. Denne løsningen er langt fra ideell, men kan være hensiktsmessig i situasjoner der terminalen sjeldent forflyttes. I tillegg til lokasjon må brukeridentitet være tilgjengelig, eventuellt kan det defineres at terminalen bare benyttes av en bruker.

- *Intelligent Ethernet:* Tilpasse Ethernet-svitsjene til å sende periodiske kringkastingspakker på hver port, som identifiserer lokasjonen. Følgelig mottar hver terminal

[10] Simple Network Management Protocol

flere kringkastingspakker, men disse vil inneholde mer og mer detaljert lokasjon, for eksempel "Bygning 1" og "Rom 22".

- *Intelligente plugger:* Enkelte kommersielle produkter[11] tilbyr nettverksplugger som kan spørres etter tilknyttede MAC-adresser. 3Com har introdusert nettverksplugger som inneholder Ethernet-svitsjer.
- *Trådløst:* Innendørs dekning er en begrensning for enkelte trådløse teknologier, for eksempel WiFi og GPS. Det finnes andre foreslåtte metoder, som å bruke digitale TV-stasjonsignaler for lokasjon. Men slike signaler har ofte 100 meter feilmargin, som er for høyt for nødmeldetjenester.
- *Infrarød/Radiofrekvens (IR/RF):* IR-sendere og sensorer kan fungere i enkelte miljøer, men kostnaden tilknyttet denne teknologien er så høy at den ikke passer seg for utbredt sivil utbygging.

3.6.7 Hybride løsninger

I realiteten kan det være mest hensiktsmessig med en hybrid løsning der to eller flere lokasjonstjenester kombineres. Dette kan gjøres på to hovedmåter:

- Prioritering
- Ettersendelse

Prioritering går ut på å benytte to eller flere lokasjonskilder i serie eller parallell, for å så benytte den "beste" posisjonen utfra en gitt tidsramme. Prioritering i serie går ut på at lokasjonstjenestene prioriteres i en angitt rekkefølge, for eksempel GPS, GeoPos, lokasjonsdatabase. Så angis det en tidsramme for hvor lang tid hver av dem kan bruke på å innhente posisjonen. For eksempel kan GPS være først i prioritetsrekkefølgen, og hvis GPS ikke klarer å innhente posisjonen innenfor den gitte tidsrammen, blir neste lokasjonstjeneste prøvd. Hvis ingen av dem klarer å innhente posisjonen innenfor en total tidsramme, blir anropet sendt uten posisjonsdata. Prioritering i parallell går ut på at flere lokasjonstjenester blir kontaktet samtidig. Da benyttes enten den tjenesten som først gir svar, eller ut fra en prioritert rekkefølge innenfor en tidsramme. Vanligvis vil GPS gi raskest svar. Derfor kan for eksempel GeoPos prioriteres foran, så hvis GeoPos gir svar innenfor tidsrammen så blir GeoPos benyttet, ellers brukes GPS. Svakheten med å benytte prioritering i parallell er redundansen dette skaper. Hvis tre lokasjonstjenester benyttes, vil to av spørringene være bortkastet, og medføre unødvendig ressursbruk. Denne løsningen vektlegger lav feilmargin og at tidsforsinkelsen aldri overskrider en gitt grense.

Ettersendelse av posisjonsdata er løsning som baserer seg på minimal tidsforsinkelse. Her er det hensiktsmessig å kombinere to lokasjonstjenester etter hverandre. Den første lokasjonstjenesten trenger bare å forsyne eksakte nok posisjonsdata til geografisk ruting. Den indikerer altså i hvilket område anropet originerer. Lokasjonsdatabase er en passende lokasjonstjeneste til dette formålet. Etter at anropet er avsluttet kan en annen lokasjonstjeneste finne en eksakt posisjon, og så ettersende denne til hjelpemannskapet.

Fordelen med hybride løsninger er at feilmargin og tidsforsinkelse kan minimeres.

[11] PanView (Panduit) og PatchView (RiT Technologies)

Svakheten er at flere lokasjonstjenester må være tilgjengelig, samt at utnyttelsen av flere lokasjonstjenester for en spørring krever mer ressurser og skaper mer overhead i nettverket.

3.7 Arkitektoniske løsningsmodeller

Dette kapittelet beskriver forskjellige løsningsmodeller for arkitektur til et nødmeldesystem. Vi skal først kartlegge hvilke muligheter som er aktuelle og deretter skal vi se på konkrete forslag fra ECRIT og 3GPP.

3.7.1 Strukturelle hensyn

3.7.1.1 Tykke og tynne klienter

Ved initialisering av et nødanrop legges lokasjonsinformasjonen ved i sesjonsbeskrivelsen. Dette kan enten gjøres helt i begynnelsen, av brukerklienten, eller underveis i meldingsforløpet, av en av nettverkselementene i infrastrukturen. Dersom logikken for denne funksjonen ligger hos klienten snakker vi om en "tykk klient", og hvis logikken ligger i infrastrukturen, en "tynn klient". Hybride løsninger er også mulig.

Den største forskjellen mellom klientside- og serversidebasert arkitektur er utplassering og utrulling av lokasjonstjenesten. Ved klientsidebasert arkitektur må alle klientene selv finne sin lokasjon, det vil si at hver klient må implementere funksjonen. Ved en programvareoppdatering må da også alle klienter oppdateres. I motsetning til serversidebasert arkitektur krever dette ingen forandringer i infrastrukturen. Tynne klienter krever ingen ekstra funksjonalitet for å benytte seg av lokasjonstjenesten ved nødanrop.

Klientsidebasert arkitektur betyr at hver av klientene har direkte tilgang til lokasjonstjenesten. Denne løsningen stiller også større krav til sikkerhet, særlig i tilfeller hvor et lokasjonsregister benyttes. Et aksessnettverk, som for eksempel Trådløse Trondheim, kan ha oversikt over lokasjonen til alle tilknyttede klienter i et register. Dette er sensitiv informasjon som ikke må misbrukes, og derfor kan ikke registeret være tilgjengelig for uautoriserte brukere. Dersom aksessnettet har én utgående SIP-proxy vil også alle VoIP-anrop generert fra brukere i nettet gå gjennom denne proxy-serveren. Her kan det være aktuelt å legge til lokasjonsinformasjon. På denne måten er det bare proxy-serveren som kommuniserer med lokasjonsregisteret, som medfører større kontroll over autoriserte brukere.

En ulempe med tykke klienter er at programvaren må tilpasses en mengde ulike typer brukterterminaler og plattformer. Dette kan være tidkrevende og vanskelig å få til. Tynne klienter vil ikke kreve ytterligere programvare, det er kun enkelte elementer i infrastrukuteren som må modifiseres. Det betyr også at det er færre punkter som kan feile ved transmisjon.

3.7.1.2 Signaleringsprotokoll

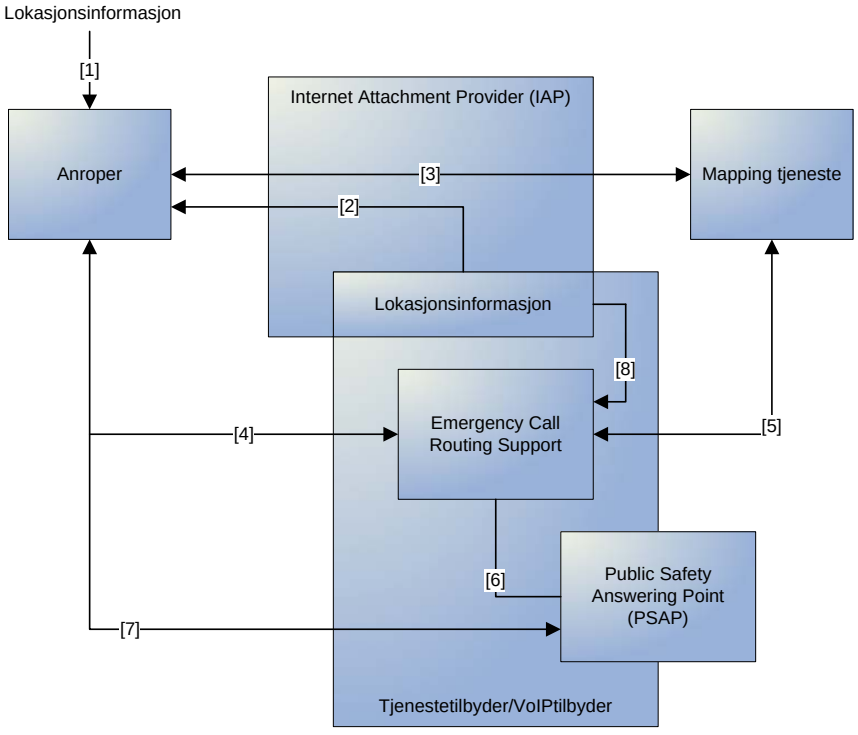
SIP og H.323 er protokollstandarder fra henholdsvis IETF og ITU for signalering av mediestrømmer over IP. Det finnes også andre interdomene signaleringsprotokoller som for eksempel XMPP[12]/Jingle og ISUP[13], men disse er ikke like godt etablerte som de førstnevnte.

[12] Extensible Messaging and Presence Protocol
[13] ISDN User Part

SIP ble designet som en generisk transaksjonsprotokoll for initiering av sesjoner uavhengig av formatet på mediestrømmen, mens fokuset for H.323 var å håndtere audio- og multimedieanrop. Dette gjør SIP mer skalberbar og fleksibel. SIP kan enkelt integreres med forskjellige applikasjoner som for eksempel Instant Messaging og også mot ulike webgrensesnitt. Det er lettere for utviklere å implementere SIP i applikasjoner fordi protokollen er tekstbasert, i motsetning til H.323 som er binær, og derfor kreves også mindre kode. Alle H.323-komponentene må bevare tilstandsinformasjon ved sesjonsoppsett. Ved oppsett av en sesjon i SIP trenger kun brukerklientene å bevare tilstandsinformasjons (kan også ha tilstandsbaserte SIP-proxyer). Dette gjør SIP mer robust. Til tross for dette har H.323 bedre administreringskapasitet, og bedre funksjonalitet for anropskontroll og konferanse [Qui04].

3.7.2 Generelt rammeverk for ende-til-ende IP-basert nødnett

I [HS07] skisserer ECRIT et generelt rammeverk for et ende-til-ende IP-basert nødnett, illustrert i figur 3.5. Figuren illustrerer infrastrukturen til et nødnett, og hvordan hver av komponentene i infrastrukturen kommuniserer sammen. Grensesnittene mellom komponentene er utelatt fra denne oppgaven. ECRIT stiller også en mengde funksjonelle krav til rammeverket. Under forklares komponentenes funksjonalitet nærmere, samt meldingsforløpet ved et nødanrop.



Figur 3.5: Figuren viser hvilke komponenter som tar del i et nødanrop og hvordan de kommuniserer sammen. Det er flere mulige sammensetninger og kommunikasjonsveier.

Elementer i rammeverket:

- *Anroper:* Bruker som utfører nødanropet ved hjelp av en VoIP-klient.
- *Lokasjonsinformasjon:* Data som beskriver klientens lokasjon.
- *Internettaksesstilbyder:* Tilbyder av det fysiske grensesnittet mellom bruker og resten av Internett. Dette kan for eksmpel være en DSL eller en optisk nettverkstilkobling.
- *Mappingtjeneste:* Tilbyr informasjon om PSAP eller videre rutinginformasjon.
- *Emergency Call Routing Support (ECRS):* Nettverkskomponent som er del av infrastrukturen til nødnettet. Dette kan for eksempel være en SIP-proxy.
- *Public Safety Answering Point (PSAP):* Sentral for mottak av nødanrop.
- *Tjenestetilbyder:* Tilbyder av tjenester som VoIP og MMoIP.

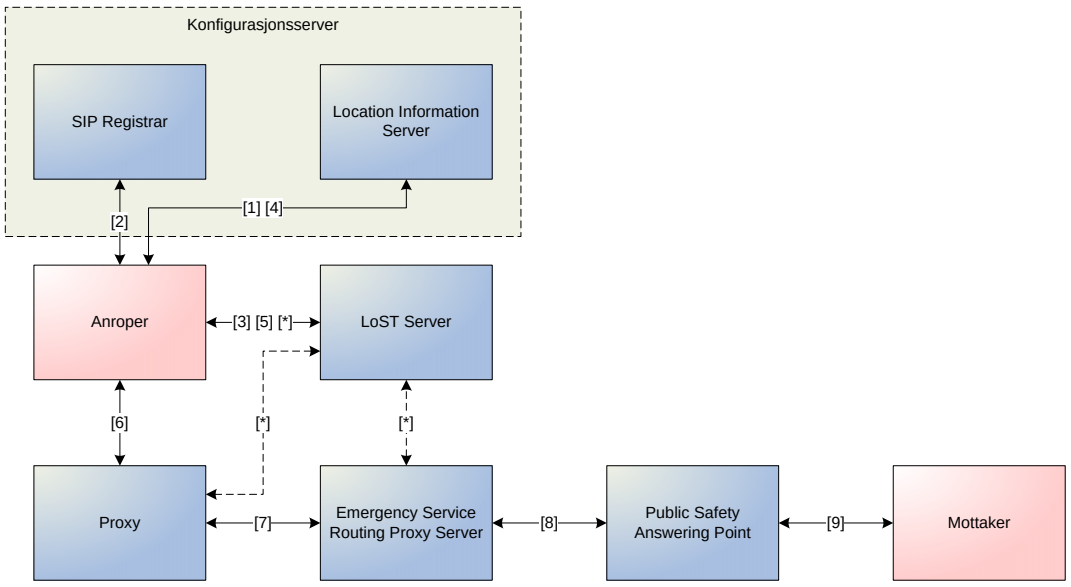
Figuren viser et generelt rammeverk hvor det er flere implementeringsløsninger. For eksempel kan lokasjonsinformasjon tilegnes på to forskjellig måter; klienten kan selv finne sin lokasjon ved å spørre en tredjepart eller så kan den benytte eksisterende funksjoner i infrastrukturen. Noen av elementene overlapper også hverandre. Dette betyr at en instans kan ha funksjonaliteten til begge elementene. For eksempel kan tjenestetilbyder og Internettaksesstilbyder være en og samme instans. PSAP har også mulighet til å være tjenestetilbyder i denne konteksten.

Meldinger i rammeverket:

1. Lokasjonsinformasjon kan anskaffes av klienten direkte (for eksempel ved hjelp av GPS).
2. Internettaksesstilbyder kan forsyne klienten med lokasjonsinformasjon. Dersom Internettaksesstilbyderen har kartlagt sin infrastruktur, med posisjon til rutere og kabling, kan en klient lokaliseres relativt nøyaktig ved hjelp av IP adressen.
3. Mappingtjenesten kan forsyne klienten direkte med rutinginformasjon eller eventuelt informasjon om PSAP.
4. Klienten kan få hjelp av komponenter i infrastrukturen til ruting av nødanropet. I tilfeller hvor SIP blir brukt som signaleringsprotokoll, kan disse komponentene være SIP-proxy.
5. Mappingtjenesten kan forsyne infrastrukturen med routinginformasjon eller eventuelt informasjon om PSAP.
6. Infrastrukturen sørger for å videresende nødanrop fra klienten basert på rutinginformasjon fra mappingtjenesten.
7. Klienten kan kontakte PSAP direkte uten å benytte en infrastruktur.
8. Lokasjonsinformasjonen benyttes av ECSR for å bestemme korrekt PSAP for den aktuelle klienten.

3.7.3 Rammeverk for IP-basert nødmeldesystem

IETF har, gjennom arbeidsgruppen ECRIT [kap. 1.5.1], foreslått et rammeverk for et ende-til-ende IP-basert nødmeldesystem, illustrert i figur 3.6. Dette rammeverket introduserer en rekke protokoller og nettverkskomponenter spesielt designet for nødtjenesten, men samtidig bygger den videre på eksisterende og godt etablerte teknologier som DHCP, SIP og RTP med tilhørende og underliggende teknologier. Hensikten med rammeverket er å tilby forskjellige nødmeldetjenester (inkluderer også muligheten for andre lokasjonsbaserte tjenester) til IP-baserte terminaler. Ved bruk av IP-nettverket kan tjenestene også variere i format, det vil si at det vil være mulig å starte en videosesjon ved et nødanrop.



Figur 3.6: ECRITs rammeverk for et ende-til-ende IP-basert nødmeldesystem slik det er spesifisert i IETF draftet [BR07].

Meldingsforløp ved et nødanrop (punkt 1-3 forekommer ved tilkobling til nettverket):

1. Ved tilkobling til aksessnettet ber klienten om sin lokasjon fra en konfigurasjonsserver. Denne svarer så med lokasjonsinformasjonen, enten i geodetisk eller sivil format.

2. Klienten registrerer seg hos en SIP registrar.

3. Klienten sender så en spørring mot en LoST server. Spørringen inneholder blant annet klientens lokasjon. LoST serveren svarer med en PSAP URI, det vil si adressen til nødsentralen med klientens lokasjon som ansvarsområde. Grensesnittet her baserer seg på LoST protokollen [kap. 3.7.3.3].

4. Ved initiering av nødanrop ber klienten LIS-serveren om en lokasjonsoppdatering.

5. Den nye lokasjonen mappes over til korrekt PSAP URI ved hjelp av LoST-serveren.
6. SIP-meldingen rutes videre gjennom nettverket på vanlig vis.
7. SIP-meldingen rutes videre gjennom nettverket til en Emergency Service Routing Proxy som er innkommende proxy i domenet til nødmeldesystemet.
8. Basert på PSAP tilstand og lokasjonsinformasjon sender ESRP meldingen videre til korrekt PSAP.
9. En kobling er nå opprettet mellom anroper og nødsentralen.

** PSAP URI kan læres av flere komponenter i kommunikasjonsveien. En løsning kan være at utgående proxy i klientens nettverk håndterer denne mappingen på vegne av klienten.*

3.7.3.1 Konfigurasjonsserver

En konfigurasjonsserver er ansvarlig for konfigurasjonsinformasjon til klienter i det tilhørende aksessnettverket. Dette kan typisk være en DHCP-server som gir ut IP-adresser. I tilfellet hvor det er aktuelt med nødanrop over IP og SIP, kan konfigurasjonsserveren også være en SIP registrar. Klienten må da registrere seg hos denne. Location Information Server (LIS) er en type konfigurasjonsserver, og denne tilbyr lokasjonsinformasjon til klientene, enten som en fast verdi eller som en peker til entiteten som oppbevarer lokasjonsinformasjonen (se 3.4.6).

3.7.3.2 Grensesnitt for konfigurasjon av lokasjon

Konfigurasjon av lokasjon er prosessen hvor klienten tilegner seg sin fysiske lokasjon [BR07]. Dette kan gjøres ved hjelp av lokale funksjoner (for eksempel GPS eller manuell konfigurasjon) eller ved å spørre det underliggende aksessnettet. Location Configuration Protocol (LCP) er en generell betegnelse for protokoller benyttet til å finne klientens lokasjon via aksessnettet, og det finnes flere forslag for implementering av denne funksjonen:

- *Dynamic Host Configuration Protocol (DHCP):* [JP04] spesifiserer et eget opsjonsfelt i DHCP for koordinatbasert lokasjonsinformasjon. DHCP-tjeneren finner klientens lokasjon ved å oversette fra tilknytningspunkt i nettverk til lokasjon. For å få til dette kreves det at tjeneren har en fullstendig oversikt over nettverkets infrastruktur.
- *Link Layer Discovery Protocol for Media Endpoint Devices (LLDP-MED):* LLDP er en linklagsprotokoll som annonserer klientinformasjon periodisk til naboer i samme nettverk [Ass06]. LLDP-MED er en utbedring av LLDP-protokollen, som blant annet er designet for kartlegging av nettverkstopologi og lokalisering av klienter i nettverket.
- *HTTP Enabled Location Delivery (HELD):* XML-basert protokoll tilhørende applikasjonslaget og uavhengig av sesjonslaget. HTTP over TCP og TLS er spesifisert som en mulig sesjon-/transportprotokoll. Protokollen støtter både nomadiske og ikke-nomadiske terminaler. Lokasjon tilføres enten ved verdi (by-value) eller ved referanse (by-referanse) [JW07].

I tillegg til disse protokollene finnes det flere andre forslag for konfigurasjon av lokasjon i endepunktet. Felles for protokollene nevnt over er at de fungerer som et grensesnitt mellom terminalen og tjenesten.

3.7.3.3 Mapping fra lokasjon til tjeneste

Når en klient har tilegnet seg sin lokasjon, er det nødvendig å bestemme videre rute til nødsentralen. Nødsentralene har sine geografiske grenser og jurisdiksjoner, og da er det også viktig at meldingen sendes til den sentralen med ansvarsområde som dekker den aktuelle klientens lokasjon. IETF har foreslått en XML-basert protokoll, Location to Service Translation (LoST), for å håndtere denne translasjonen [TH07]. LoST oversetter en lokasjon til en tjeneste-URL, for eksempel SIP. Lokasjonen kan både være i geodetisk og sivil format. Klienten sender en forespørsel med et tjenestefelt og lokasjonsinformasjon som beskriver ønsket tjeneste. Dersom tjenesten eksisterer for gitt lokasjon returnerer serveren et svar som beskriver måten å kontakte tjenesten på (URL). Hvis tjenesten ikke finnes i området, sendes enten en feilmelding eller URL til en alternativ tjeneste.

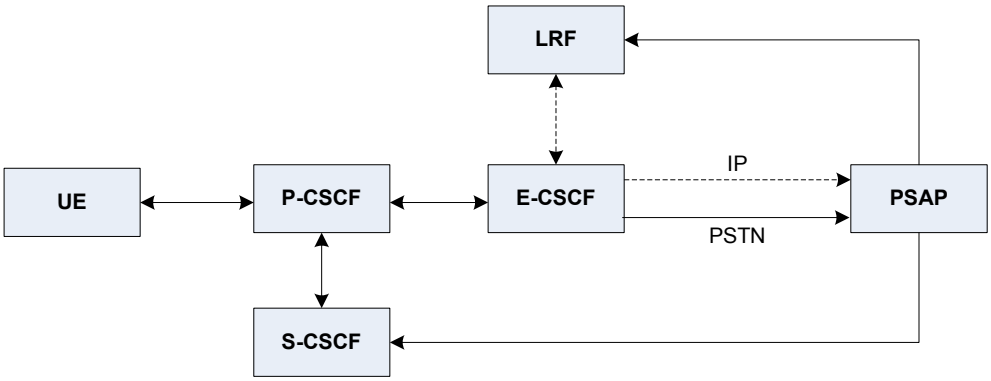
```
<?xml version="1.0" encoding="UTF-8"?>
<findService
    xmlns="urn:ietf:params:xml:ns:lost1"
    xmlns:p2="http://www.opengis.net/gml"
    serviceBoundary="value"
    recursive="true">
    <location profile="geodetic-2d">
        <p2:Point id="point1" srsName="urn:ogc:def:crs:EPSG::4326">
        <p2:pos>37.775 -122.422</p2:pos>
        </p2:Point>
    </location>
    <service>urn:service:sos.police</service>
</findService>
```

Kodeeksempel 3.3: Tjenesteforespørsel med lokasjonsinformasjon. Serveren svarer med en URL

3.7.4 IMS-arkitektur

IP Multimedia Subsystem (IMS) er et arkitektonisk rammeverk for teleoperatører som vil tilby IP-multimediatjenester. Det bruker en VoIP-implementering som baserer seg på den 3GPP-standardiserte implementeringen av SIP. IMS støtter både IP og tradisjonelle telefonitjenester i PSTN.

[3GP06] beskriver en implementering av nødtjenester i IMS ved å definere abstrakte krav, en arkitektonisk modell, en funksjonell beskrivelse og prosedyrer for etablering av nødanrop. Figur 3.7 illustrerer IMS-arkitekturen.



Figur 3.7: IMS arkitektur for nødmeldetjenester. Denne arkitekturen introduserer en emergency call session control function (E-CSCF), som for eksempel håndterer ruting av nødanrop (figuren er modifisert fra [3GP06]).

IMS-arkitekturen består av flere proxyer og SIP-servere, kollektivt kalt "Call Session Control Function (CSCF)", som håndterer SIP-signaleringspakker i IMS. I en IMS-arkitektur for nødmeldetjenester får noen av entitetene tilleggfunksjonalitet for å håndtere nødanrop:

- *UE (User Equipment):* Brukerens terminal, som initierer et nødanrop. Nødanropet består av en parameter som angir at det er et nødanrop, en nødbrukeridentifikasjon og hvis tilgjengelig, nødtjenestetype og lokasjon. UE kan spørre IP-CAN om lokasjon.
- *P-CSCF (Proxy CSCF):* Mellomliggende proxy som detekterer nødanrop. Kan avvise anropet hvis det ikke tilfredsstiller visse krav. Velger en E-CSCF til å håndtere nødanropet. Sørger for prioritering av nødanropet.
- *S-CSCF (Serving-CSCF):* SIP-server som besørger sesjonskontroll. Har ingen nevneverdig ekstrafunksjonalitet i forhold til nødmeldetjenester.
- *E-CSCF (Emergency CSCF):* Mottar nødanropet fra en P-CSCF. Hvis anropet ikke inneholder lokasjonsdata, kan E-CSCF spørre LRF om lokasjonsdata. Ellers kan E-CSCF spørre LRF om validering av lokasjonsdata. E-CSCF spør LRF om rutinginformasjon til aktuell PSAP, og håndterer så selve rutingen av nødanropet.

- *LRF (Location Retrieval Function):* Ansvarlig for å tolke lokasjonsdataene i anropet, som så brukes til rutinginformasjon og andre parametre som blir sendt til E-CSCF.
- *PSAP:* Nødsentral som mottar nødanropene [kap. 2.1.3].
- *IP-CAN (IP-Connectivity Access Network):* Nettverksentitetene og grensesnittene som besørger underliggende tilkobling for IP-kommunikasjon mellom UE og IMS (for eksempel GPRS[14]).
- *MGCF/MGW (Media Gateway Controller Function):* Kontrollprotokollkonvertering mellom SIP og ISUP. Har ingen nevneverdig ekstrafunksjonalitet i forhold til nødmeldetjenester.

IMS-arkitekturen innfører altså en E-CSCF som håndterer ekstra funksjonalitet for nødanrop. Figur 3.8 illustrerer de tre primære måtene (A, B og C) et nødanrop blir opprettet på, og hvordan lokasjonen innhentes av enten UE eller IMS. I tillegg til disse, er det mulig for IMS å innhente lokasjonsdata fra IP-CAN, på samme måte som UE gjør i (B) [3GP06].

Forklaring til figur 3.8:

- *A:* IMS spør LRF om lokasjon og rutinginformasjon, hvis det er nødvendig.
- *B:* UE innhenter lokasjonen ved å spørre IP-CAN. UE kan også innhente posisjonen på egen hånd, for eksempel ved hjelp av GPS.
- *C:* IMS-kjernen spør LRF om lokasjonsdata. Lokasjonsdata fra LRF betegnes som *midlertidig*, og gir bare en indikasjon på lokasjonen. LRF mottar disse lokasjonsdataene fra enten UE eller PSAP, og de er ment som reserveløsning for å kunne rute anropet til PSAP hvis ikke lokasjonen kan finnes ved andre metoder.

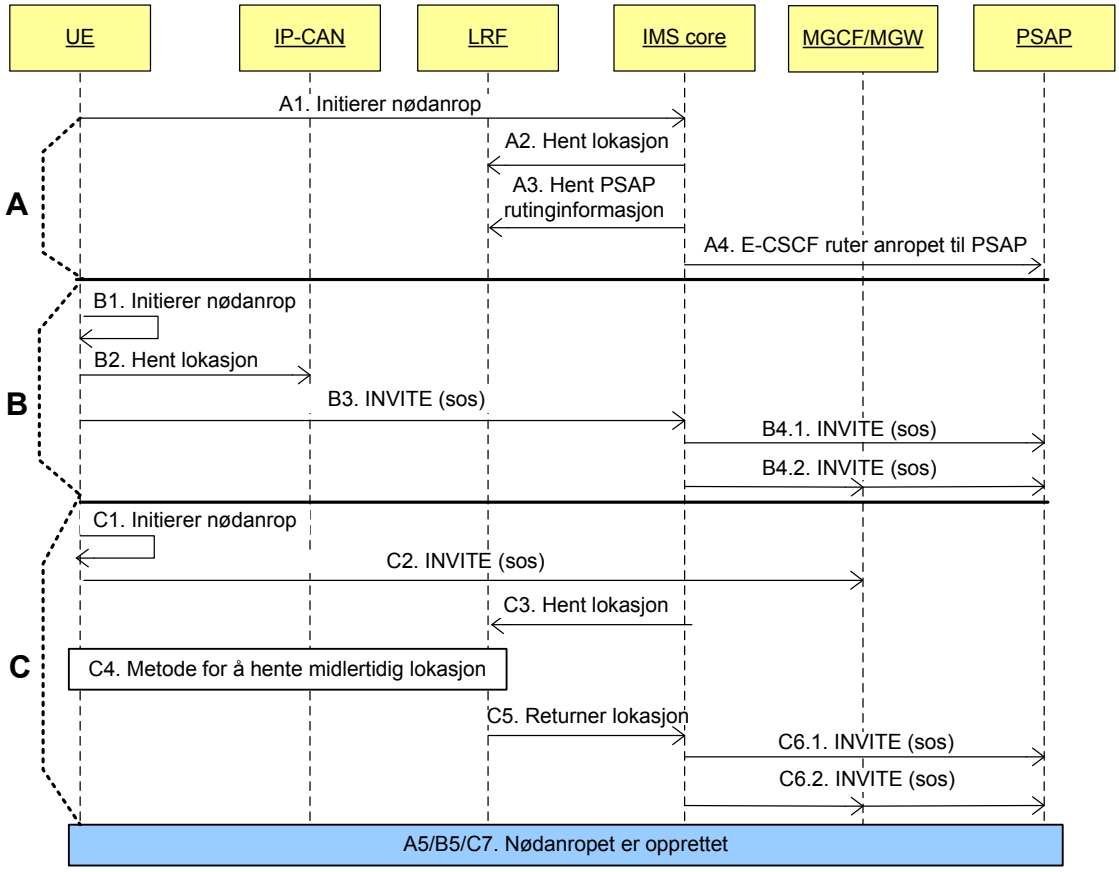
3.7.5 IMS-kompatibel arkitektur tilpasset GeoPos

Figur 3.9 viser en IMS-kompatibel arkitektur som opprettholder våre krav for posisjonsinnhenting. Arkitekturen er basert på skisser for et GeoPos-demonstrasjonsprosjekt ved NTNU, inspirert av [3GP06].

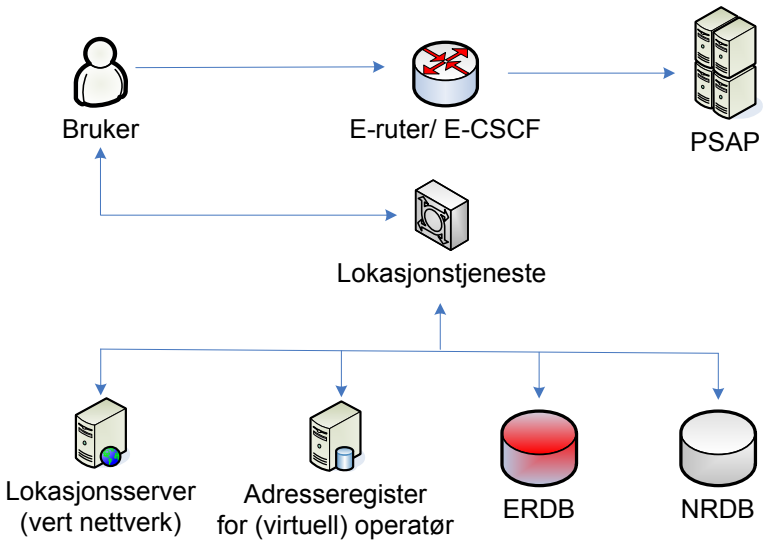
IMS-arkitekturen innfører en "Emergency Call Session Control Function" (E-CSCF) som håndterer nødtjenestefunksjonaliteten [kap. 3.9]. I følge [3GP06] skal E-CSCF være koblet til lokasjonstjenesten, og utføre spørringen etter lokasjon. I vår implementering er det satt som krav at klienten selv skal anskaffe sin lokasjon, følgelig er lokasjonstjenesten koblet direkte mot brukeren. E-CSCF sin oppgave blir da å tolke lokasjonsdata i anropet, og viderekoble anropet til riktig PSAP.
Komponentforklaring for figur 3.9:

- *Bruker:* Terminalen som utfører nødanropet. Sender en lokasjonsforespørsel til lokasjonstjenesten, og sender så lokasjonsdata med anropet til E-CSCF.

[14] General Packet Radio Service



Figur 3.8: IMS MSC-diagram som viser hvilke tre måter et nødanrop kan bli opprettet på, og hvordan lokasjonen innhentes (figuren er modifisert fra [3GP06]).



Figur 3.9: IMS-kompatibel arkitektur for å tilby lokasjonsdata til PSAP. Brukeren henter først sin lokasjon, og sender så denne til E-CSCF, som tolker lokasjonsdata, og viderekobler anropet til riktig PSAP.

- *E-CSCF:* Nødanrop er klassifisert, og blir viderekoblet til en felles nødruter (E-CSCF), som tolker lokasjonsdata, og videresender anropet til riktig PSAP.

- *Lokasjonstjeneste (LRF):* Det eksisterer forskjellige metoder for å finne lokasjon [kap. 3.6]. Denne arkitekturen er tilpasset GeoPos, men kan også utføres av en annen tjeneste for posisjonsinnhenting. Lokasjonstjenesten henter lokasjon, og returnerer denne til bruker. Lokasjonstjenesten kan sammenlignes med LRF-entiteten i IMS-arkitekturen.

- *Lokasjonsserver:* Tilhører teleoperatøren i vertnettverket.

- *Adresseregister:* Tilhører den virtuelle teleoperatøren. Mottar en ID som parameter, for eksempel et telefonnummer eller en SIP URL. Adresseregisteret gjør så et oppslag basert på denne IDen, og returnerer en IP-adresse til en lokasjonsserver som må spørres for å få vite lokasjonen. Adresseregisteret benyttes altså for å finne ut hvor man kan henvende seg for å finne eksakt lokasjon.

- *NRDB - Nasjonal Referansedatabase [AS]:* Tilbyr lokasjonsmegleren rutinginformasjon til den aktuelle operatørens adresseregister. Operatøren må da sørge for at denne rutinginformasjonen er korrekt.

- *ERDB - Emergency Reference Database:* Returnerer rutinginformasjon til PSAP basert på en lokasjonsreferanse (f.eks koordinater).

- *PSAP:* PSAP mottar anropet med lokasjonsdata, og tolker dette etter gitte bestemmelser.

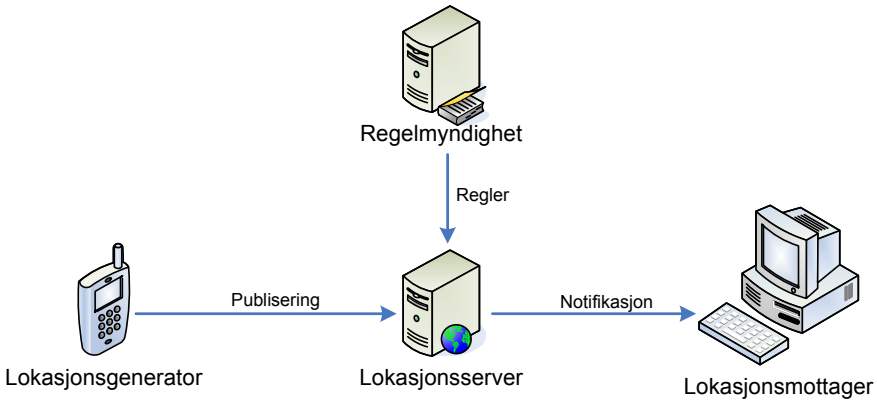
3.7.6 Personvernbasert arkitektur

Personvern i forhold til lokasjon er ikke en del av denne oppgaven [kap. 1.3], men det er likevel relevant å se på hvilke konsekvenser dette kan ha for arkitekturen.

[Tsc06] foreslår en løsningsmodell for en personvernbasert arkitektur, kalt "GeoPriv", som tar utgangspunkt i at:

- Mange entiteter kjenner lokasjonen din.
- Ofte kan du ikke kontrollere systemene som finner din lokasjon.
- Ofte er lokasjon ett dataelement i en større kontekst, der konteksten også trenger beskyttelse av personvern.
- Personvern er et arkitektonisk problem, og trenger sjelden kryptografi som løsning.

GeoPriv er en SIP-basert standard for overføring av lokasjonsinformasjon over Internett, som fokuserer på personvernhensyn og sikkerhetshensyn, både med tanke på det teknologiske perspektivet og hvilke regler som skal gjelde. Realiseringen består av en containerklasse definert som sikker. Lokasjonsinformasjon og regler for distribusjon av lokasjonsinformasjonen transporteres i containerklassen. Det særegne ved GeoPriv er at den introduserer en regelmyndighetentitet og konseptet med en *using protocol* (bruksprotokoll), som transporterer et GeoPriv-lokasjonsobjekt. Disse bruksprotokollene bestemmer personvernegenskapene til GeoPriv. Fordelen med dette er at det kan brukes eksisterende protokoller som tilbyr sikkerhetsmekanismer, som for eksempel støtte for anonymitet.



Figur 3.10: De viktigste entitetene i en GeoPriv-arkitektur består av lokasjonsgenerator, lokasjonsmottager, lokasjonsserver og regelmyndighet. (Figuren er modifisert fra [Tsc06])

Elementer i GeoPriv-arkitekturen:

- *Lokasjonsgenerator:* Publiserer sin lokasjon til lokasjonsserveren via et publiseringsgrensesnitt. For eksempel en bruker av et nødmeldesystem.

- *Lokasjonsmottager:* Kan abonnere på lokasjonsinformasjon fra en kjent lokasjonsgenerator. Enten periodisk oppdatering eller engangoppdatering.
- *Lokasjonsserver:* Distribuerer lokasjonsinformasjon til lokasjonsmottagerne via et notifikasjonsgrensesnitt, i henhold til reglene satt av regelmyndighet. For eksempel AMK-sentralen i et nødmeldesystem.
- *Regelmyndighet:* Bestemmer reglene som skal følges via et regelgrensesnitt.

Regelmyndighetentiteten som blir introdusert i GeoPriv-arkitekturen innehar regler for hvilke lokasjonsmottagere som har tilgang på lokasjonen til de forskjellige lokasjonsgeneratorene. I enkelte tilfeller kan lokasjonsserveren eksistere sammen lokasjonsgeneratoren, for eksempel hvis det benyttes en GPS-modul eller lokasjonsinformasjon fra aksessnettet. For at autorisasjonen skal kunne fungere må regelmyndighet sende sine regler, i form av betingelser, handlinger og transformeringer, til lokasjonsserveren. I enkelte tilfeller kan også lokasjonsgeneratoren fungere som regelansvarlig.

3.8 Nødmeldesystem i Trådløse Trondheim

Ved å bruke Trådløse Trondheim som nettverksplattform skal vi studere en arkitektur der klienten selv fremskaffer sin lokasjon og inkluderer denne i anropet. Dette delkapittelet beskriver et nødmeldesystem for Trådløse Trondheim med hensyn til funksjonalitet og arkitektur. Under kapittelet for resultater beskrives en implementering av dette systemet med tilhørende testing av de benyttede lokasjonstjenestene.

3.8.1 Overordnet skisse av systemets funksjonalitet

Figur 3.11 viser den abstrakte funksjonaliteten til systemet. Terminalen som utfører nødanropet finner sin egen lokasjon ved hjelp av en lokasjonstjeneste, og lokasjonsdata blir sendt med anropet. Geografisk ruting sørger for at anropet viderekobles til nærmeste nødsentral, som tar situasjonsavhengige avgjørelser angående tilkalling av nødvendig hjelp.

3.8.2 Systemvalg

I henhold til krav og utfordringer definert i denne oppgaven, skal vårt foreslåtte system inneha følgende egenskaper:

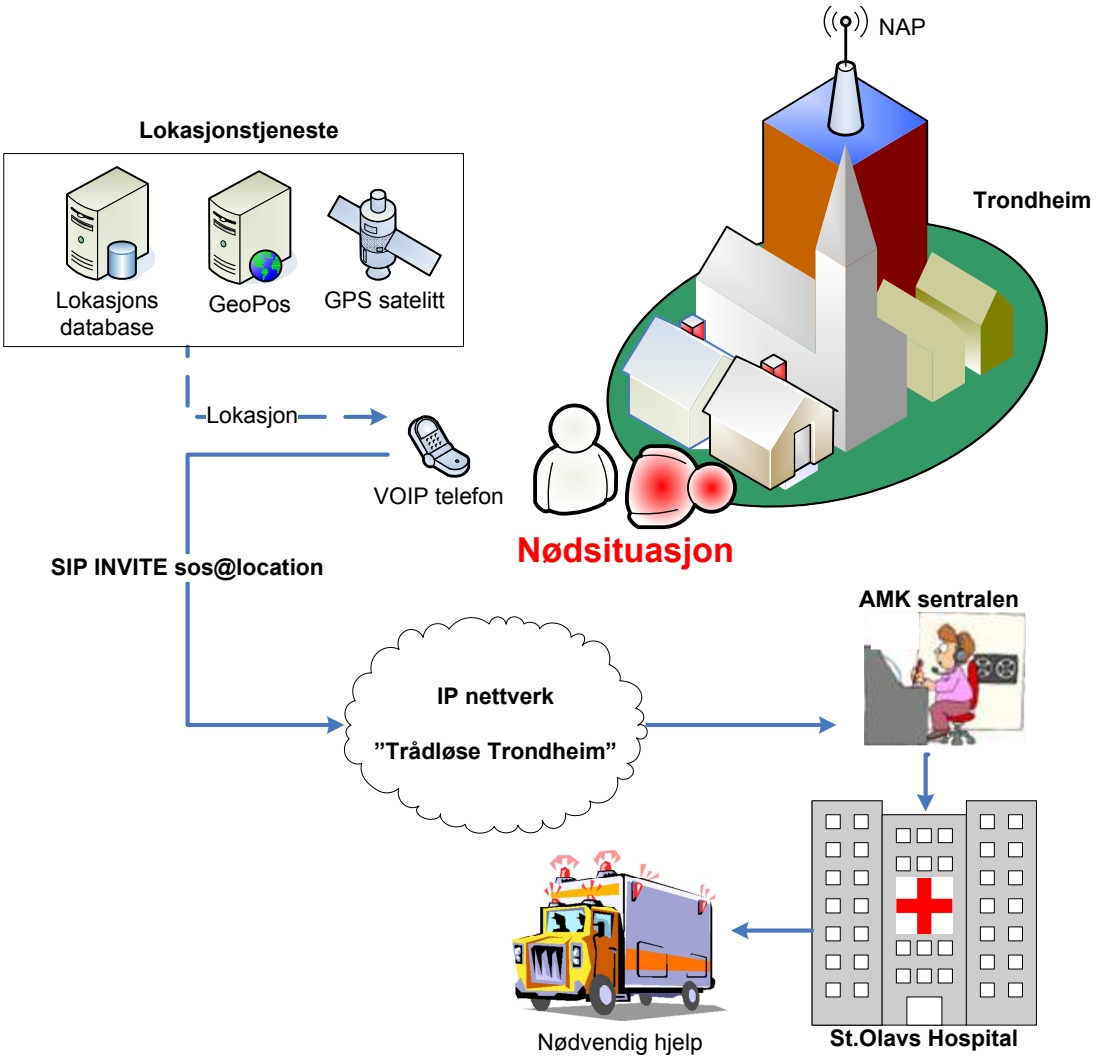
- Bruke SIP som signaleringsprotokoll [kap. 3.7.1.2].
- Basere seg på en "tykk klient"-løsning [kap. 3.7.1.1].
- Klienten anskaffer selv sin lokasjon ved å benytte lokasjonstjenestene GPS, GeoPos eller lokasjonsdatabase basert på MAC [kap. 3.6].
- Klienten henter lokasjon ved oppsett av samtale [kap. 3.4.3].
- Sender lokasjonsinformasjon som sos-attributter i SIP INVITE-meldingen [kap. 3.4.5].
- Sender lokasjonsinformasjon som fast verdi [kap. 3.4.6].
- Serversiden tolker lokasjonsparametrene. Det trengs ingen konvertering eller prosessering av lokasjonsinformasjon på klientsiden [kap. 3.4.4].

Begrunnelsen av disse valgene finnes i kapittel 5.2.

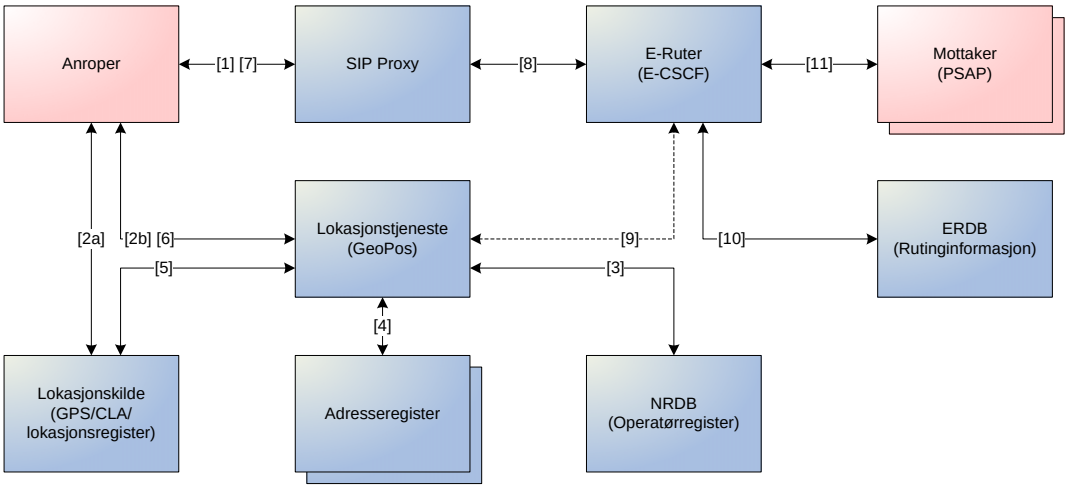
3.8.3 Arkitektur

Figur 3.12 beskriver arkitekturen for et fullstendig ende-til-ende IP-basert nødmeldesystem. Arkitekturen er spesielt rettet mot Trådløse Trondheim og benytter lokasjonmegleren GeoPos utviklet ved NTNU. Foreløpig har GeoPos kun et grensesnitt mot Cisco Location Appliance, men det er hensiktsmessig å utvide GeoPos med flere grensesnitt og lokasjonskilder slik at arkitekturen kan tilpasses andre infrastrukturer. For videre generalisering av arkitekturen benyttes SIP-teknologien for signalering.

Arkitekturen introduserer en rekke komponenter. De fleste av disse er beskrevet nærmere under delkapittel 3.7.4 og 3.7.5. Under forklares kommunikasjonsforløpet ved et nødanrop:



Figur 3.11: Nødmeldesystemets kretsløp, fra nødsituasjonen oppstår til hjelpemannskap er på vei



Figur 3.12: De forskjellige komponentene, samt interaksjonen mellom disse, som tar del i en arkitektur for støtte av nødanrop i Trådløse Trondheim.

1. Klienten registrerer seg hos en SIP-proxy disponert av en VoIP-tilbyder. Dette kan være en lokal instans i klientens aksessnettverk eller en ekstern uavhengig instans.
2. Posisjonsinnhenting:
   (a) Klienten kan spørre en posisjoneringsfunksjon i brukerterminalen (for eksempel GPS).
   (b) Klienten sender en forespørsel om lokasjonsinformasjon til lokasjonstjenesten GeoPos. Med i forespørselen er det informasjon som identifiserer brukerklienten og klientens nettoperatør.
3. GeoPos kommuniserer med et operatørregister (NRDB). Registeret svarer GeoPos med en referanse til den aktuelle operatørens adresseregister i form av en IP-adresse.
4. Fra GeoPos mottar adresseregisteret en URN som identifiserer brukeren. Registeret svarer med en referanse, i form av en IP-adresse, til en lokasjonskilde aktuell for det aksessnettverket brukeren er tilknyttet til. I Trådløse Trondheim kan dette være Cisco Location Appliance.
5. Lokasjonskilden mottar en identifikator av brukerklienten (for eksempel MAC-adressen) fra GeoPos. På bakgrunn av denne lokaliseres klienten og lokasjonsinformasjonen returneres til GeoPos (enten på sivilt eller geodetisk format).
6. GeoPos sender lokasjonsinformasjonen tilbake til brukerklienten.
7. SIP-meldingene rutes gjennom IP-nettverket på vanlig vis.
8. SIP-meldingene rutes gjennom IP-nettverket til nærmeste E-Ruter.
9. E-Ruteren kommuniserer med GeoPos. På denne måten kan brukerlokasjonen valideres og/eller eventuelt ny brukerlokasjon kan legges til i meldingene.

10. Kommuniserer med ERDB for rutinginformasjon. Lokasjon oversettes til en PSAP-URL.

11. SIP-meldingene rutes videre til korrekt PSAP.

3.8.3.1 Posisjonsinnhenting

Posisjonsinnhenting blir gjort av brukerklienten idet brukeren foretar et nødanrop fra SIP-agenten. Brukerklienten kan finne sin lokasjon enten ved å spørre en integrert GPS-mottaker eller lokasjonstjenesten (GeoPos). Kommunikasjon med GeoPos skjer med XML-meldinger over SOAP og HTTP. GeoPos returnerer en lokasjonsobjekt i form av en XML-melding med lengdegrad og breddegrad.

GeoPos utnytter seg av en lokasjonskilde for å finne brukerens lokasjon. Lokasjonskildene benytter forskjellige teknologier avhengig av brukerens aksessnett. For eksempel har Trådløse Trondheim utplassert trådløse aksesspunkt og LAN-kontrollere som sender nettverksdata til en sentralisert enhet som beregner brukerklientens lokasjon ut i fra disse dataene [kap. 3.6.4]. GeoPos er nødt til å vite hvilken lokasjonskilde den skal spørre. NRDB og adresseregistrene hjelper GeoPos med å identifisere operatøren for nettverket og også lokasjonskilden. Grensesnitt mot disse enhetene er ikke spesifisert i denne oppgaven.

3.8.3.2 Geografisk ruting

E-ruteren sørger for geografisk ruting ved å behandle lokasjonsinformasjon i anropet. På bakgrunn av denne informasjonen sender ruteren en forespørsel til en ERDB. ERDB er ansvarlig for å oversette lokasjonsinformasjon til en tjeneste-URL. Lokasjonen kan være på sivilt format, i form av en gateadresse, eller på geodetisk format, i form av geografiske koordinater (UTM, WGS84) [kap. 3.4.4]. For eksempel kan ERDB motta en forespørsel med lokasjon “Kongens gate 11, 7013, Trondheim, Norway”. ERDB sender så en SIP-URL som respons: sip:sos@eksempel.no. LoST-protokollen [kap. 3.7.3.3] spesifiserer et XML-basert grensesnitt for denne funksjonen.

3.8.4 Plug-in løsning

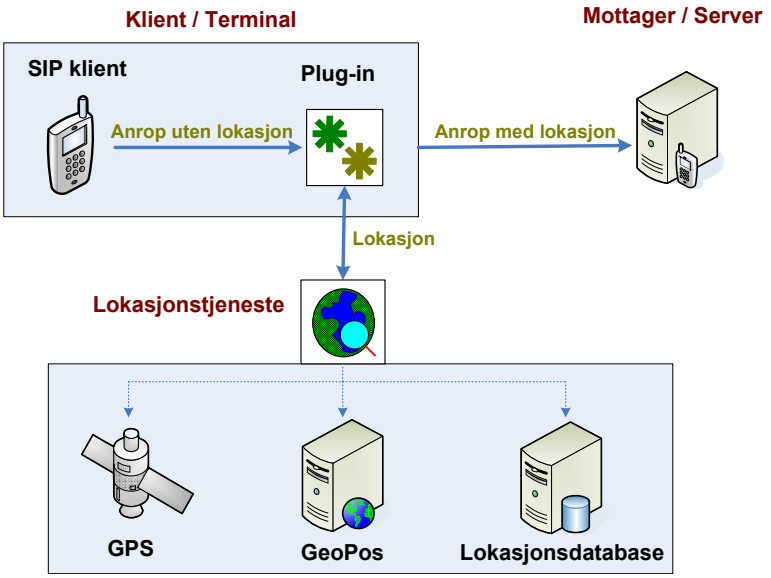
En “tykk klient”-løsning betyr ekstra funksjonalitet på klientsiden for å håndtere nødanrop. For å implementere denne funksjonaliteten foreslår vi en “plug-in”-løsning.

Figur 3.13 illustrerer en plug-in løsning der mellomliggende arkitektur er utelatt. Plug-in løsningen består av en liten applikasjon som installeres på samme plattform som VoIP-applikasjonen som terminalen benytter for telefoni.

Prinsippene for implementering av plug-in løsningen:

- Plug-in løsningen er avhengig av en VoIP-applikasjon som besørger selve anropet.
- Plug-in løsningen installeres på terminalen, med minimum konfigurasjon av den eksisterende VoIP-applikasjonen.
- Brukeren skal kunne benytte sin kjente VoIP-applikasjon for anrop.

- Plug-in løsningen kjører i bakgrunnen på terminalen, og startes automatisk ved operativsystetmets oppstart. Slik blir plug-in løsningen "gjemt" for brukeren.
- Etter at plug-in løsningen er installert på terminalen, skal den ikke kreve ytterligere konfigurasjon.
- Plug-in løsningen skal være uavhengig av type VoIP-applikasjon (så lenge VoIP-applikasjonen baserer seg på SIP.)



Figur 3.13: Overordnet skisse over plug-in arkitekturen. Mellomliggende arkitektur (mellom klient, mottager og lokasjonstjeneste) er utelatt fra denne figuren. Her kunne også GeoPos (som lokasjonsmegler) hatt ansvaret for videre kommunikasjon med lokasjonsdatabasen.

Plug-in løsningen fungerer som en agent eller proxy, og kommuniserer med VoIP-applikasjonen, lokasjonstjenesten og mottager av anropet (eller mellomliggende proxy). VoIP-applikasjonen blir konfigurert til å kommunisere med plug-in, men i praksis vil den oppfatte kommunikasjonen som direkte med mottager av anropet (eller mellomliggende proxy).

Funksjonaliteten til plug-in løsningen består av:

1. Innhente utgående anrop, i form av SIP-meldinger.
2. Sjekke om de inneholder en indikator. (For eksempel en SOS-parameter hvis det er nødanrop.)
3. Innhente lokasjon fra en lokasjonstjeneste.
4. Legge lokasjonen med SIP-meldingen i form av SOS-parametre
5. Videresende anropet til mottager (eller mellomliggende proxy).

6. Fungere som en proxy for resten av SIP-transaksjonene (sørge for at SIP-meldingene blir sendt til riktig adresse).

Kapittel 4

Resultater

Den praktiske delen av oppgaven består av å utarbeide et utkast til en fleksibel løsning for en modifisert SIP-klient i terminalen til brukeren, der posisjonsdata sendes med anropet. Resultatene beskriver framgangsmåten for å utvikle en demonstrator av en nødmeldetjeneste og er delt i tre hovedavsnitt; design, implementering og testing. Først beskrives den overordnede tankegangen og den konseptuelle modellen i designavsnittet, dvs. hvordan oppgaven er gjennomført. Implementasjon beskriver de tekniske komponentene i arbeidet, med kodeeksempler og UML klassediagram. Til slutt skal vi se på resultatene av testgjennomførelse. Dette inkluderer oppsett og analyse.

4.1 Design

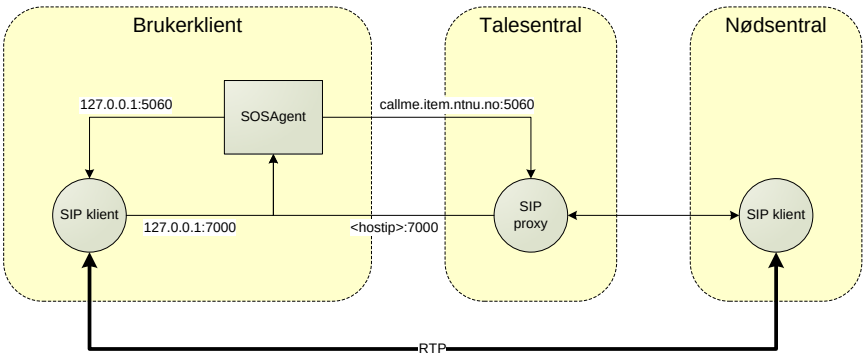
Før det overordnede designet av nødmeldesystemet kan forklares er det viktig å presisere hvilke komponenter som tar del i designet og hvilken funksjon hver enkelt komponent har i denne settingen:

- *Brukerklient:* Den fysiske terminalen som benyttes av brukeren.
- *VoIP-klient:* Programvaren som muliggjør en VoIP-sesjon over IP nettverket.
- *SOS-agent:* Programvaren som sørger for å identifisere et nødanrop initialisert fra VoIP-klienten, og som snakker med lokasjonstjenestene for å hente brukerens lokasjon.
- *SIP-proxy:* Talesentral som behandler SIP-forespørsler på vegne av VoIP-klienten, dette inkluderer registrering av klienten.
- *Fjerntliggende vert:* Korresponderende motpart til den som setter i gang en VoIP eller MMoIP sesjon.
- *GPS:* Lokasjonstjeneste basert på satellitt. Innebygd i brukerklienten.
- *GeoPos:* Tredjeparts meglertjeneste for posisjonsinnhenting. Ekstern i forhold til brukerklienten.
- *Nettverksinfrastruktur:* Eksisterende IMS infrastruktur.

En forutsetning ved implementering av nødmeldesystemet er at kommunikasjon skal foregå over eksisterende nettverksprotokoller og klientprogramvaren skal også kunne benytte seg av standard grensesnitt for disse protokollene. Det vil si at både klient-programvaren for VoIP og infrastrukturen i nettverket er uavhengig av programvaren for nødanropstjenesten. Med dette vil logikken for tjenesten befinne seg i brukerklienten, som da blir en tykk klient.

Nødanropstjenesten består av en SOS-agent. Agenten er en prosess som kjører i bakgrunnen på operativsystemet til brukerklienten. Den befinner seg mellom en SIP-klient og en SIP-proxy (illustrert i figur 4.1), og behandler forespørsler fra begge disse. Det vil si at meldinger som kommer fra SIP-klienten, fanges opp av agenten, som så videresender disse meldingene til en proxy. Agenten vil også fange opp innkommende meldinger og sørge for at klienten får disse.

Når SOS-agenten mottar en melding, vil den forandre innholdet i meldingen. SIP-meldingshodene inneholder blant annet felter som forteller hvor meldingen kommer fra, hvor den skal, og hvor den har vært. Disse feltene forandres slik at meldingen kan rutes videre til riktig endepunkt. Et viktig tillegg for nødmeldesystemet er at dersom klienten ringer nødnummeret SOS, vil agenten finne brukerens lokasjon og legge ved denne i SIP-meldingen. Lokasjonen finnes ved hjelp av lokasjonstjenester. Disse lokasjonstjenestene henter brukerklientens posisjon ved initialisering av anropet.



Figur 4.1: Figuren viser kommunikasjonsforløpet mellom to SIP-klienter. Klienten som benytter seg av SOS-tjenesten ringer via agenten på et lokalt grensesnitt. Agenten sørger så for å videresende SIP-meldingene på vegne av klienten. VoIP og RTP-trafikken foregår som normalt.

4.1.1 Tilleggstjenester

Slik SOS-agenten er designet blir nødanropet identifisert av en eller flere nødidentifikatorer (for eksempel sos eller 113). Identifikatorene er spesifisert lokalt hos klienten i en liste og bestemmer hvorvidt lokasjonsinformasjon skal legges til i anropet. Dette er en funksjonalitet som også kan være aktuell for andre tjenester. Agenten kan for eksempel utvides til å behandle andre identifikatorer og URNer som for eksempel taxi@norgestaxi.no. Lokasjonsinformasjon kan da innhentes, og basert på denne kan anropet rutes til drosjesentral aktuell for anroper. Det bør også være mulig å oppdatere lista over et nettbasert grensesnitt eller eventuelt gjøre et oppslag direkte mot et eksternt register ved hjelp av en registerreferanse. Et alternativ til dette er en funksjon i agenten hvor brukeren foretar en spørring mot lokasjonstjenesten manuelt, for så å legge til lokasjonsinformasjon i anropet.

4.2 Implementasjon

Microsofts Visual Studio 2005 ble benyttet for å utvikle en løsning av SOS-agenten for Pocket PC. Rammeverket .NET Compact Framework er et subsett av Microsoft .NET Framework og kan brukes til å utvikle applikasjoner for mobile innretninger med operativsystemer som for eksempel Windows CE, Microsoft Pocket PC og Windows Mobile. Utviklingsspråket C# ble benyttet for å utvikle disse applikasjonene. En fullstendig liste over rammeverk og verktøy benyttet i den praktiske delen finnes i appendiks B.

Under følger en kort forklaring med kodeeksempler av de viktigste komponentene på klientsiden, og til slutt beskrives funksjonaliteten på serversiden. Fullstendig klassediagram for klient- og serversiden finnes i appendiks D. Noen variabelnavn og metodenavn presentert i kodeeksemplene i dette kapittelet vil varierer noe fra vedlagt kildekode, men funksjonaliteten vil være den samme.

4.2.1 SOSUserAgent

SOSUserAgent-klassen sørger for kommunikasjon mellom SIP-klienten og proxy/mottaker ved hjelp av klassebibliotekene System.Net og System.Net.Sockets som er en del av .NET Compact Framework. Tre forskjellige nettverksadresser spesifiseres med klassen System.Net.EndPoint:

```
EndPoint localEP = (EndPoint)new IPEndPoint(IPAddress.Any, 7000);
EndPoint clientEP = (EndPoint)new IPEndPoint(localhost, sipPort);
EndPoint serverEP = (EndPoint)new IPEndPoint(callme, sipPort);
```

Kodeeksempel 4.1: Spesifisering av IP-endepunkter med nettverksadresse og port.

clientEP og serverEP er de fjerntliggende endepunktene agenten skal snakke med. Begge konfigureres til port 5060, som er den aktuelle porten for SIP-tjenester. localEP er det endepunktet som skal ta imot og sende data. Fordi agenten skal kunne ta imot data både fra klient og proxy, må IPAddress.Any brukes som parameter. Det vil si at alle nettverksgrensesnittene er tilgjengelige for dette endepunktet. Til slutt bindes det lokale endepunktet til en UDP-nettverkssocket som muliggjør transmisjon av UDP-pakker.

SOS-agenten kommuniserer asynkront med både klient og proxy. Metodene *BeginReceiveFrom* og *BeginSendTo* starter en asynkron overføring med et spesifisert endepunkt. Når overføringen er ferdig kalles delegatmetodene *EndReceiveFrom* eller *EndSendTo*. Disse sørger for å returnere resultatet av den gitte dataoverføringen. Asynkron kommunikasjon legger ikke bånd på ressursene, som i dette tilfellet er SOS-agentprosessen, og derfor er det mulig å motta og sende samtidig.

Måten agenten ruter SIP-meldinger er ved å sjekke hvilket endepunkt meldingene kommer fra. Dersom det er klienten som sender en forespørsel, vil endepunktet tilsvare lokal vert (dvs. 127.0.0.1), og hvis ikke dette er tilfellet er endepunktet IP-adressen til proxyserveren (callme.item.ntnu.no). Meldingshodene i SIP forandres slik at svarmeldingene rutes riktig vei tilbake i forhold til forespørslene.

SOS-agentens viktigste funksjon er å identifisere et nødanrop og eventuelt legge ved nødvendig lokasjonsdata. SOSUserAgent og SOSParser-klassene sørger for å sjekke innkommende INVITE meldinger fra klienten for nødanropsidentifikatoren "sos". SOSUserAgent inneholder også instanser av lokasjonstjenestene (GeoPos, GPS og MAC), og samarbeider med disse for å hente brukerens lokasjon dersom INVITE forespørselen inneholder sos-identifikatoren. Lokasjonsdata blir lagt til som en del av sesjonsbeskrivelsen (Session Description Protocol) i kroppen til forespørselen.

I samsvar med 3.4.5 definerer vi sos-attributter for å transportere lokasjonsinformasjonen. Tabell 4.1 beskriver de sos-attributtene som sendes via SIP INVITE-meldingen.

SOS-attributt	**Forklaring**
soscoord	Koordinatene på form <koordinat-x koordinat-y>
sosformat	Formatet på koordinatene. For eksempel "UTM" eller "WGS84"
sossource	Lokasjonskilden. For eksempel "GPS" eller "GeoPos"
sosmac	MAC adressen til terminalen
sosnapmac	MAC adressen til nettverksaksesspunktet terminalen er tilknyttet

Tabell 4.1: SOS-attributtene som sendes via INVITE-meldingen i vår implementering.

Disse sos-attributtene er valgt ut fra kapittel 3.4.4, som beskriver hvilke lokasjonsdata som er nødvendig å sende til nødsentralen. Det grunnleggende prinsippet er å sende lokasjonsdataene til nødsentralen uten prosessering, og så la nødsentralen besørge prosesseringen (for eksempel konvertering mellom koordinater). Et fullverdig eksempel på en SIP INVITE-melding med sos-attributter finnes i appendiks C. Kapittel 4.2.6 beskriver hvordan vi håndterer lokasjonsdata på serversiden i vår implementering.

Kodeeksempelet under viser metoden *BeginReceiveFrom()* som asynkront mottar pakker fra endepunktet remoteEP. Delegatmetoden *endListen()* sørger for å avslutte den pågående overføringen ved hjelp av metoden *EndReceiveFrom()*. Endepunktet sjekkes så for å finne ut hvor pakken kommer fra, klienten eller proxy, og hvor den skal rutes videre. Når pakken er sendt er agenten klar for å motta nye pakker.

```
1  private void beginReceive()
2  {
3      try
4      {
5          globalBuffer = new byte[1200];
6          socket.BeginReceiveFrom(globalBuffer, 0, globalBuffer.Length,
               SocketFlags.None, ref remoteEP, new AsyncCallback(endListen)
               , null);
7      }
8      catch
9      {
10         throw;
11     }
12 }
13
14 private void endReceive(IAsyncResult iar)
15 {
16     try
17     {
18         int bytesReceived = socket.EndReceiveFrom(iar, ref remoteEP);
19
20         byte[] buffer = new byte[bytesReceived - 1];
21         Array.Copy(globalBuffer, buffer, bytesReceived - 1);
22
23         //forward to proxy if received from client
24         if (remoteEP.Equals(localhost))
25         {
26             sipParser.changeOutgoing(ref buffer);
27             beginForwardToServer(buffer);
28         }
29         //forward to client
30         else
31         {
32             sipParser.changeIncoming(ref buffer);
33             beginForwardToClient(buffer);
34         }
35         beginReceive();
36     }
37     catch
38     {
39         throw;
40     }
41 }
```

Kodeeksempel 4.2: Metodene beginReceive() og endReceive()

4.2.2 GPS-biblioteket

GPS-klienten er hentet fra et kodeeksempel fra Microsoft. Kodeeksempelet inneholder blant annet klassen Gps. Denne klassen fungerer som grensesnitt mellom applikasjonsutvikler og GPS API (tilhører Windows Mobile 5.0 SDK). SOS-agenten bruker Gps-

klassen ved å instansiere et objekt av typen Gps. I tillegg til dette oppretter agenten to funksjonspekere av typen LocationChangedEventHandler og DeviceStateChangedEventHandler. Disse håndterer hendelser generert av GPS-innretningen. Dersom GPS-innretningen rapporterer en forandring på brukerens lokasjon, blir hendelsen LocationChanged satt i gang. Denne blir så håndtert av Gps-objektet som kaller funksjonen *gps_ LocationChanged*. I denne metoden lagres de nye verdiene for breddegrad og lengdegrad.

Metoden *gps.Open* kalles ved oppstart av SOS-agenten. Denne metoden åpner en kobling til GPS-innretningen og gjør klar for å motta data fra den. Det vil si at SOS-agenten også legger bånd på GPS-innretningen. Det vil ikke være mulig å bruke GPS til andre formål så lenge agenten kjører, og visa versa. Når agenten lukkes kalles *gps.Close* for å frigjøre ressursen.

4.2.3 GeoPos-biblioteket

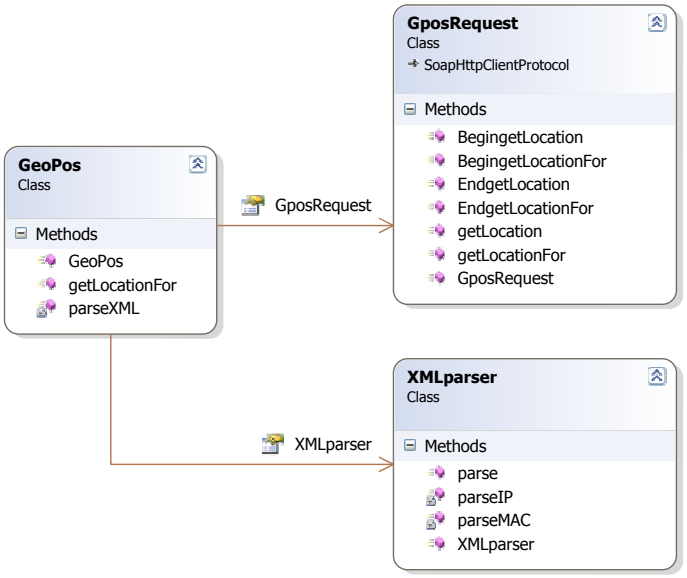
GeoPos-biblioteket brukes til kommunikasjon med GeoPos ved hjelp av GeoPos Web Services. Figur 4.2 illustrerer oppbyggingen av GeoPos-biblioteket.

GeoPos-klassen initierer et GposRequest-objekt. Metoden *getLocationFor()* kalles så på GposRequest-objektet. Parametrene i dette metodekallet er beskrevet i 3.6.3, og de angir innstilligene som GposRequest-objektet skal benytte i kommunikasjonen med GeoPos. Parameteren "TargetId" skal enten inneholde MAC-adressen eller IP-adressen til terminalen. Man kan da anvende koden implementert i 4.2.4 for å finne disse verdiene.

GposRequest-klassen er generert av WSDL-filen til GeoPos Web Services. Den er så modifisert til å passe vår applikasjon. GposRequest har også en metode som heter *getLocationFor()* (kodeeksempel nedenfor). Dette er den viktigste metoden i denne klassen. Ved bruke et SOAP Remote Procedure Call, sender den en forespørselsmelding til GeoPos-serveren, som innhenter posisjon og returnerer en XML-basert svarmelding.

GeoPos-klassen initierer så et XML parser-objekt som har til hensikt å tolke svaret fra GeoPos. Metoden *parse(string type, string response, string responsetype)* blir kalt på XML-objektet, der type er enten "MAC" eller "IP" og responsen er den XML-baserte svarmeldingen fra GeoPos. Formålet med responsetype er å muliggjøre ekstrahering av spesielle felter i meldingen.

XML-klassen inneholder to private metoder for å tolke svaret fra GeoPos. De to metodene blir benyttet avhengig av om det er en forespørsel basert på en MAC-adresse eller en IP-adresse, og de heter henholdsvis *parseMAC()* og *parseIP()*. Avhengig av responstype blir enten hele meldingen eller deler av meldingen oversatt til lesbar tekst.



Figur 4.2: Klassediagram for GeoPos-biblioteket, med tilhørende variabler og metoder. GeoPos-klassen initialiserer et GposRequest-objekt og et XML parser-objekt. GposRequest-objektet blir brukt til kommunikasjon med GeoPos, mens XML parser-objektet brukes til å tolke svaret fra GeoPos.

```
1  [System.Web.Services.Protocols.SoapRpcMethodAttribute("",
       RequestNamespace="http://webservice.gpos.geofinder",
       ResponseNamespace="http://webservice.gpos.geofinder", Use=System.
       Web.Services.Description.SoapBindingUse.Literal)]
2  [return: System.Xml.Serialization.XmlElementAttribute("
       getLocationForReturn")]
3  public string getLocationFor(string in0, string in1, string in2,
       string in3) {
4      try
5      {
6          object[] results = this.Invoke("getLocationFor", new object[]
               {
7                  in0,
8                  in1,
9                  in2,
10                 in3});
11         return ((string)(results[0]));
12     }
13     catch (Exception ex)
14     {
15         return ex.Message;
16     }
17 }
```

Kodeeksempel 4.3: Metoden getLocationFor, som benytter SOAP Remote Procedure Call for å kommunisere med GeoPos.

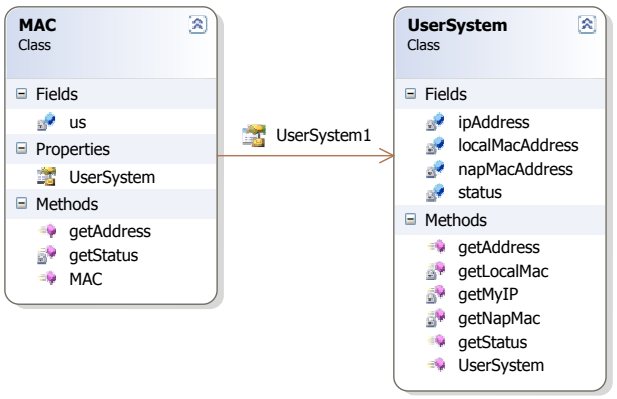
4.2.4 MAC-biblioteket

MAC-biblioteket benyttes for å innhente terminalens MAC-adresse og IP-adresse, samt MAC-adressen til det trådløse nettverksaksesspunktet den er tilkoblet, såkalt NAP MAC. MAC-klassen initierer et UserSystem-objekt, som benytter OpenNETCF utvidelsesrammeverket for å få tilgang på de to MAC-adressene. Figur 4.3 illustrerer oppbyggingen av MAC-biblioteket.

MAC-klassen inneholder metoden *getAddress(string adressetype)* som tar inn en av strengene LMAC (lokal MAC), NMAC (NAP MAC) eller IP som parameter, og kalles på UserSystem-objektet. Dette objektet inneholder de tre metodene *getLocalMac()*, *getNapMac()* og *getMyIp()*, som bruker klassene i OpenNETCF utvidelsesrammeverket for å kunne returnere verdier i henold til forespørselen.

4.2.5 SIPparser-biblioteket

SIPparser-biblioteket benyttes til å modifisere SIP-meldingene som blir sendt mellom klienten og SIP-proxyen. Oppbygningen til dette biblioteket er illustrert i figur 4.4. SOS-agenten ligger mellom disse, og må tilpasse meldingene slik at de blir sendt rikitg. En SIP-melding inneholder blant annet felter som from, to, contact og via. I tillegg til dette består den øverste linjen i meldingen ofte av et SIP nøkkelord etterfulgt av en adresse.



Figur 4.3: Klassediagram for MAC-biblioteket, med tilhørende variabler og metoder. MAC-klassen initialiserer et UserSystem-objekt, som skaffer informasjon om brukerens system og det tilkoblede aksesspunktet

SIPparser-klassen inneholder to hovedmetoder, *changeIncoming()* og *changeOutgoing()*. Disse tar inn SIP-meldingen som parameter, henholdsvis meldingen som kommer inn til SOS-agenten fra proxyen og meldingen som kommer inn fra klientapplikasjonen. Disse blir så modifisert ved å anvende de andre change-metodene. Det er en metode for hvert felt som må modifiseres. For eksempel vil metoden *changeVia()* parse ut adressen som må forandres i meldingens VIA-linje, og forandre denne til ønsket verdi.

Kodeeksempelet nedenfor viser to SIP REGISTER-meldinger, som en SIP-bruker sender for å registrere seg i SIP-proxyen. Den øverste meldingen er sendt fra klientapplikasjonen til SOS-agenten, og den nederste er sendt fra SOS-agenten til proxyen. Ved å sammenligne feltene i meldingen vises hvilke felter som har blitt forandret av SOS-agenten.

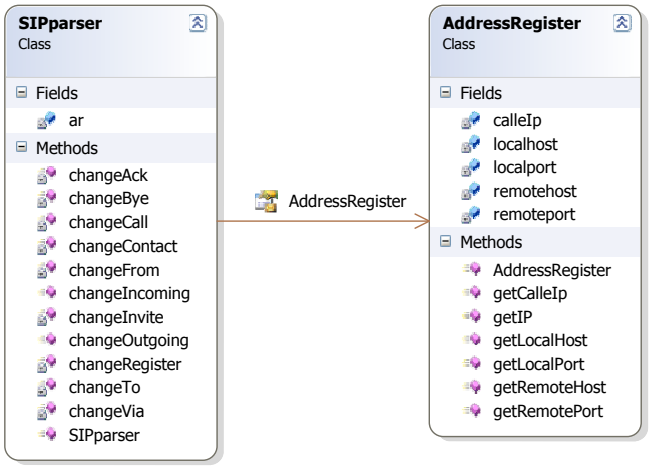
```
1 REGISTER sip:127.0.0.1:7000 SIP/2.0
2 Via: SIP/2.0/UDP 127.0.0.1;rport;branch=
      z9hG4bK81f1deba000000104649b43100001732000000001
3 Content-Length: 0
4 Contact: <sip:hal@127.0.0.1:5060>
5 Call-ID: 906AAF10-DC9B-4295-86A3-2DA029B4AD2E@129.241.222.186
6 CSeq: 1 REGISTER
7 From: <sip:hal@127.0.0.1:7000>;tag=10370634323990
8 Max-Forwards: 70
9 To: <sip:hal@127.0.0.1:7000>
```

Kodeeksempel 4.4: SIP REGISTER-melding før den har vært gjennom SIP-parseren

```
1 REGISTER sip:callme.item.ntnu.no:5060 SIP/2.0
2 Via: SIP/2.0/UDP 127.0.0.1;rport=7000;branch=
      z9hG4bK81f1deba000000104649b3750000425800000003
3 Content-Length: 0
4 Contact: <sip:hal@129.241.222.186:7000>
5 Call-ID: 1E35F49F-CA9D-4677-BE9C-E65095C50870@192.168.1.101
6 CSeq: 2 REGISTER
7 From: <sip:hal@127.0.0.1:7000>;tag=10351867119627
8 Max-Forwards: 70
9 To: <sip:hal@127.0.0.1:7000>
```

Kodeeksempel 4.5: SIP REGISTER-melding etter den har vært gjennom SIP-parseren

SIPparser-klassen initierer et AdresseRegister-objekt. Dette er en typisk registerklasse som holder orden på adressen og porten som skal brukes av SOS-agenten for å nå proxyen og klienten. I tillegg inneholder den IP-adressen til mottageren av anropet, som den fanger opp i SIP-meldingene.



Figur 4.4: Klassediagram for SIPparser-biblioteket, med tilhørende variabler og metoder. SIPparser-klassen initierer et AdresseRegister-objekt som fungerer som et register med adresser og porter som skal brukes i parsingen.

4.2.6 Funksjonalitet på serversiden

Funksjonalitet på serversiden er egentlig utenfor oppgavens omfang [kap. 1.3], men for å utføre en mest mulig virkelighetsnær demonstrator implementerte vi en applikasjon til bruk i en AMK-sentral.

Applikasjonen fungerer som en nettverkssniffer og har følgende funksjonalitet:

1. Fange opp alle IP-pakker forbundet med en angitt nettverksadapter, sendt til en angitt port (vanligvis standard SIP-port 5060).

2. Sortere ut hvilke IP-pakker som inneholder SIP-meldinger.

3. Sortere ut hvilke av SIP-meldingene som er *sos-meldinger*.
4. Finne alle *sos-parametre* hvis det er en sos-melding.
5. Bruke sos-parameteren "Format" til å finne ut hvilket format koordinatene er sendt på.
6. Hvis koordinatene ikke er sendt på WGS84-formatet må de konverteres ved hjelp av klassen GeoTrans.
7. Aktivere en kartapplikasjon og legge ved koordinater av WGS84-format.

Applikasjonen henter kartet fra en hjemmeside drevet av Google Maps[1], som tar inn breddegrad, lengdegrad og lokasjonstjeneste benyttet som parametre. Videre blir kartet lastet inn i applikasjonen, og en stedsmarkør angir koordinater for posisjonen samt hvilken lokasjonstype som er benyttet. Dette kan være til nytte for hjelpemannskapene, da lokasjonstjenestene varierer i forhold til feilmargin.

Resultatet er en applikasjon som kjører i bakgrunnen på en maskin med støtte for VoIP. Når en SIP INVITE-melding ankommer med sos-parametre blir kartapplikasjonen automatisk aktivert og vises over hele skjermen. En fullverdig SIP INVITE-melding med sos-attributter finnes i appendiks C, og et skjermbilde av serversidens kartapplikasjon ved innkommende nødanrop finnes i appendiks E.

[1] http://maps.google.com

4.3 Testing

Testingen omfatter feilmarginer og tidsforsinkelse for lokasjonstjenestene GPS og GeoPos i Trådløse Trondheim. Generell testing av GPS og GeoPos er utenfor oppgavens omfang, men feilmarginer og tidsforsinkelse er relevant for et nødmeldesystem. Selve GeoPos er en lokasjonsmegler, så i realiteten var det CLA [kap. 2.3.3] som ble testet.

4.3.1 Testoppsett

Tabell 4.2 viser teststedene vi valgte for å utføre testingen, og figur 4.5 viser fordelingen av teststedene. Koordinatene i tabell 4.2 er hentet fra "Nasjonal Vegdatabank", og beskriver utgangspunktet for hvert teststed.

4.3.1.1 Utstyr/Forutsetninger

Spørringen mot GPS ble foretatt av en *Fujitsu Siemens Loox N95 Pocket PC* med innebygd GPS. Spørringen mot CLA ble gjort av en bærbar datamaskin som simulerte programmet beskrevet under implementering. Den bærbare datamaskinen benyttet en trådløs nettverksadapter av typen *Intel(R) PRO/Wireless 2200BG Network Connection*, og programvare for nettverksovervåkningen var *WirelessWon v2.0*.

4.3.1.2 Testmetode

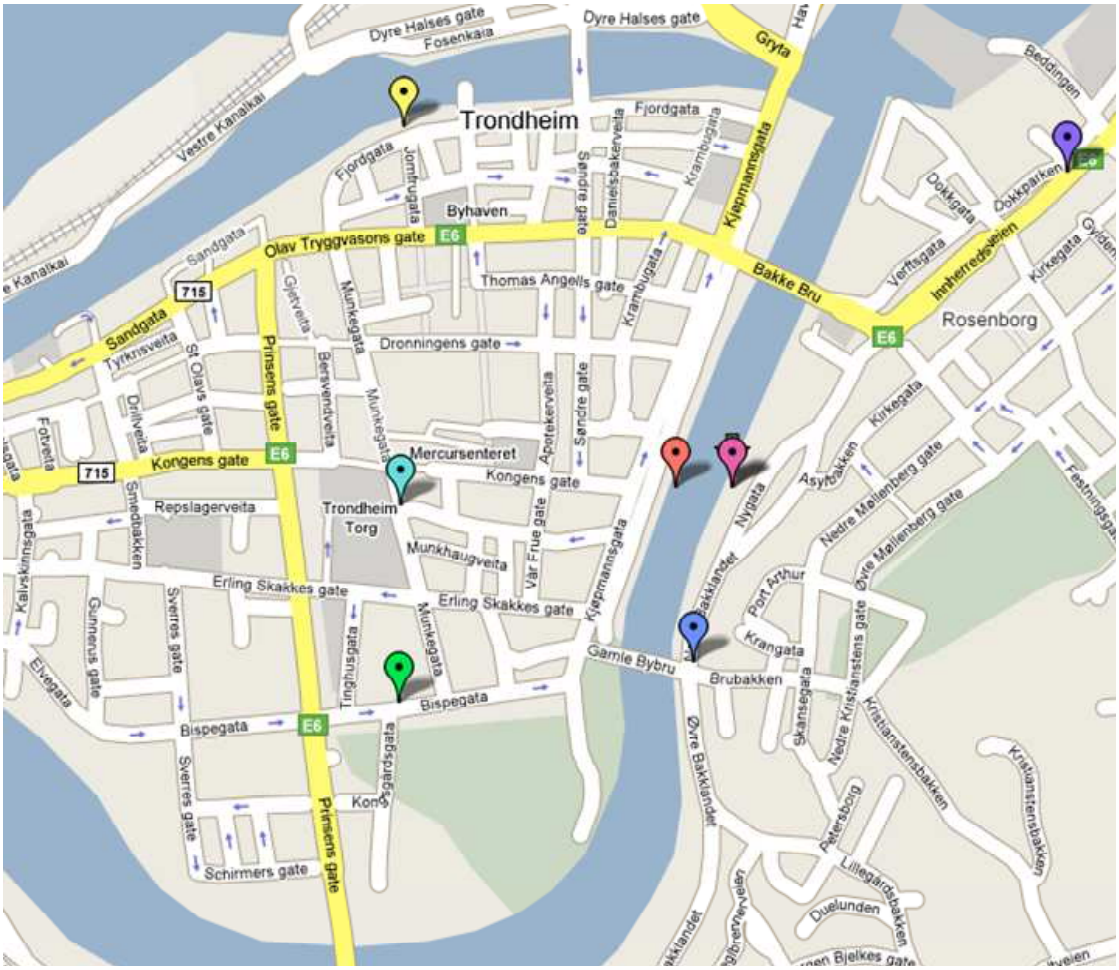
Feilmarginene er kalkulert som luftavstand fra koordinatene oppgitt av CLA og GPS i forhold til utgangspunktet. Tidsforsinkelsen gjelder bare for CLA og er tiden det tok å innhente lokasjonen. For hvert teststed ble det gjort tre målinger på tidsforsinkelse, der gjennomsnittet av de tre er vist i tabell 4.4.

Tidsforsinkelsen for GPS er utelatt fordi den er avhengig av å være *varm*. Det vil si at GPSen må være påslått en viss tid før den får kontakt med et tilstrekkelig antall satellitter. GPSen brukt i testingen brukte rundt 5 minutter for å bli varm, og etter det var lokasjonen kontinuerlig tilgjengelig.

Signalstyrken er målt i % og desibel. Desibelverdien er negativ, og lavere verdi betyr svakere signal. -80 dBm er grensen for hvor lav signalstyrken kan være før det forsvinner. I tillegg er antall aksesspunkter med samme SSID inkludert. I vårt tilfelle er dette antall WiFi-sendere som sender ut signal for Trådløse Trondheim.

Markør	Sted	Koordinater utgangspunkt
	Bakklandet (ved Dromedar)	+63° 25' 41.52", +10° 24' 11.08"
	Kjøpmannsgata (ved Peppes Pizza)	+63° 25' 48.94", +10° 24' 9.31"
	Trondheim Katedralskole	+63° 25' 39.74", +10° 23' 42.89"
	Torget	+63° 25' 48.17", +10° 23' 43.13"
	Fjordgata (ved KPMG)	+63° 26' 4.39", +10° 23' 43.34"
	Solsiden (ved Choco Boco)	+63° 26' 2.45", +10° 24' 46.75"
	Nygata 12	+63° 25' 48.96", +10° 24' 14.80"

Tabell 4.2: Stedsmarkører og koordinater for stedene der testingen ble utført.



Figur 4.5: Stedsmarkørene viser på hvilke steder testingen ble utført, ut fra tabell 4.2

4.3.2 Resultater

Appendiks F inneholder skjermbilder fra målingene vi foretok på de forskjellige teststedene. I dette kapittelet blir resultatene fra målingene presentert og analysert.

4.3.2.1 Feilmarginer

Tabell 4.3 viser feilmargin i meter for GPS og CLA i forhold til utgangspunktet gitt av stedsmarkørene i tabell 4.2. Den siste feilmarginen er luftlinjeavstanden mellom koordinatene angitt av GPS og CLA. Denne avstanden viser altså CLA sin feilmargin om det forutsettes at GPS-målingen er korrekt, eller omvendt.

Sted	GPS	CLA	GPS - CLA
Bakklandet (Dromedar)	11,5466	5,9513	15,4402
Trondheim Katedralskole	10,3311	43,2095	33,1269
Kjøpmannsgata (Peppes)	1,7258	44,0808	42,5071
Torget	1,2448	11,4071	12,4339
Fjordgata (KPMG)	16,1053	28,5594	14,0306
Solsiden (Choco Boco)	15,3451	6,44545	10,8735
Nygata 12 (Delvis innendørs)	46,8764	88,2175	51,8533

Tabell 4.3: Feilmarginer i meter for GPS, CLA og avstanden mellom GPS og CLA. Figur 5.1 illustrerer tabellen som graf.

4.3.2.2 Tidsforsinkelse

Tabell 4.4 viser tiden det tar for CLA å innhente posisjonen til en terminal. Dette er den ekstra tidsforsinkelsen et nødanrop blir belastet med ved å benytte CLA som lokasjonskilde. Det ble utført tre målinger for hvert teststed, og gjennomsnittet er angitt i denne tabellen.

Sted	Tidsforsinkelse
Bakklandet (Dromedar)	0,7000
Trondheim Katedralskole	0,6719
Kjøpmannsgata (Peppes)	0,7188
Torget	0,6875
Fjordgata (KPMG)	0,6563
Solsiden (Choco Boco)	0,6406
Nygata 12 (Delvis innendørs)	1,1836

Tabell 4.4: Gjennomsnittstiden CLA bruker på å innhente posisjonen til en terminal. Figur 5.2 illustrerer tabellen som graf.

4.3.2.3 Feilmargin i forhold til signalstyrke

Tabell 4.5 viser antall aksesspunkter og signalstyrke i % og desibel for teststedene.

Sted	Antall aksesspunkt	Ss i %	Ss i dBm
Bakklandet (Dromedar)	2	42%	-62
Trondheim Katedralskole	1	45%	-59
Kjøpmannsgata (Peppes)	2	33%	-70
Torget	4	53%	-52
Fjordgata (KPMG)	4	25%	-77
Solsiden (Choco Boco)	6	37%	-66
Nygata (delvis innendørs)	1	22%	-80

Tabell 4.5: Antall aksesspunkter og signalstyrken på teststedene. Signalstyrken oppgis i % og desibel (dBm). Figur 5.3 illustrerer tabellen som graf.

Kapittel 5

Diskusjon

I dette kapittelet skal vi gjøre rede for foreslått arkitektur fra hoveddelen. Vi tar for oss hver enkelt byggekloss i arkitekturen og ser på hvordan disse medvirker i et nødmeldesystem, både i positiv og i negativ forstand. Vi skal også se på diverse konkrete systemvalg og gi en kort begrunnelse for hvorfor nettopp disse valgene er tatt. Deretter gir vi en oppsummering og analyse av testresultater. Lokasjonstjenestene vurderes ut fra denne analysen. Til slutt skal vi se på nytteverdien for lokasjonsbaserte systemer i andre tjenester.

5.1 Foreslått arkitektur

Figur 3.8 illustrerer vår foreslåtte arkitektur for et nødmeldesystem. Arkitekturen er delt opp i tre hoveddeler for funksjonalitet; klient-, lokasjons- og nødfunksjonalitet. Et av hovedpoengene med vårt forslag til arkitektur er å skille disse tre delene fra hverandre. Denne arkitekturen støtter de egenskapene beskrevet i kapittel 3.8.2.

5.1.1 Klientfunksjonalitet

5.1.1.1 Tykk klient

Et valg for arkitekturen er bruken av tykke klienter, det vil si at brukerterminalen håndterer det meste av logikken i stedet for det underliggende nettverket. I dette tilfellet er det brukerterminalen som selv er ansvarlig for å innhente sin lokasjon. Den største fordelen med dette er at det muliggjør bruk av terminalbaserte lokasjonskilder som for eksempel satellittbaserte posisjoneringssystem. Denne teknologien er en svært aktuell lokasjonskilde etterhvert som satelittmottakere integreres i ulike brukerterminaler. Satellittsystemene er også uavhengig av nettverksinfrastrukturer.

Tykke klienter har direkte tilgang til lokasjonstjenesten. Dette utgjør en større sikkerhetsrisiko enn ved indirekte tilgang gjennom nettverket, og det er nødvendig med brukerautentisering for bruk av tjenesten. Samtidig gir fri tilgang til tjenesten mulighet for utviklere til å produsere andre lokasjonsbaserte applikasjoner. GeoPos tilbyr lokasjonstjenesten i form av en Web Service, som er i tråd med en utvikling som stadig fokuserer på service-orientert arkitektur[1].

Alternativet er å plassere all funksjonalitet i nettverket, slik at tilpasning av programvare til forskjellige terminaler unngås. Denne løsningen umuliggjør bruk av terminalbaserte lokasjonskilder, og er derfor forkastet. En mer aktuell løsning er en hybrid modell, der brukeren er koblet mot en terminalbasert lokasjonskilde, mens nettet sørger for kontakt med lokasjonsmegleren (kobling fra E-ruteren til lokasjonsmegleren). Denne løsningen ville ført til ekstra funksjonalitet både på brukersiden og i nettverket. Vår arkitetkur har altså valgt å plassere all funksjonalitet for kommunikasjon med lokasjonsdelen på brukersiden.

5.1.2 Lokasjonsfunksjonalitet

5.1.2.1 Lokasjonsmegler

Den største fordelen med en lokasjonsmegler er at den tilbyr et enkelt grensesnitt til klientsiden, som ikke trenger å kjenne til hvilke lokasjonskilder som benyttes.

En arkitektonisk løsning uten lokasjonsmegler ville hatt en entitet mindre. Denne ekstra entiteten vil påføre systemet større tidsforsinkelse og et ekstra **kritisk avhengighetspunkt**. Hvis lokasjonsmegleren er ute av drift (for eksempel på grunn av stor pågang), vil ikke lokasjonskildene kunne nåes, selv om de er operative. Lokasjonsmegleren vil også være en mulig feilkilde (for eksempel ved å velge "feil" lokasjonskilde). Med andre ord øker systemets sårbarhet ved å innføre en ekstra entitet. Løsningen på dette kan være

[1] SOA

å innføre flere lokasjonsmeglere i parallell. En slik løsning vil sikre systemets oppetid tross svikt i en av lokasjonsmeglerne. Spesielt for et nødmeldesystem er det kritisk at oppetiden er høyest mulig (tilnærmet 100%).

5.1.2.2 NRDB og adresseregister

NRDB og adresseregisterne gir nødmeldesystemet en skaleringsevne. Lokasjonsmegleren behandler forespørsler fra brukerklienter som sendes videre til NRDB. NRDB inneholder en referanseliste til adresseregisteret til de forskjellige operatørene. I dette registeret er operatøren selv ansvarlig for å tilby en eller flere referanser til lokasjonskilder for lokalisering av brukeren i nettverket. Skalering av systemet forekommer ved at nye operatører legger til rutinginformasjon for sine registre.

5.1.3 Nødfunksjonalitet

5.1.3.1 ERDB

Nødfunksjonaliteten består av E-ruter (E-CSCF), ERDB og PSAP. I vår foreslåtte arkitektur er ERDB koblet mot E-ruteren. Alternativt kunne ERDB vært koblet direkte mot lokasjonsmegleren [kap. 3.7.5] eller brukeren. Fordelen med å koble ERDB mot E-ruteren er at nødfunksjonaliteten skilles fra resten av systemet. ERDB blir skjult for andre entiteter enn E-ruteren. Hvis ERDB var koblet mot lokasjonsmegleren, måtte lokasjonsmegleren innføre ekstra funksjonalitet og mer kompleksitet. Lokasjonsmegleren kan ofte være flaskehalsen i systemet, og det kan være hensiktsmessig å avlaste den så mye som mulig.

Den store svakheten ved å koble ERDB direkte mot lokasjonsmegleren er hvis brukeren benytter en lokasjonskilde som ikke er avhengig av lokasjonsmegleren, for eksempel GPS. I dette tilfellet må E-ruteren spørre lokasjonsmegleren om rutinginformasjon, og vi får et komplisert interaksjonsmønster mellom enititetene. Løsningen her kunne vært at brukeren selv hadde kontaktet ERDB for rutinginformasjon. Da unngås den ekstra runden fra E-ruter til lokasjonsmegler til ERDB. I tillegg ville all funksjonalitet ligget på klientsiden, som ville muliggjort et enkelt nett. Dette tilfellet ville krevet et grensesnitt mellom brukerterminalen og ERDB, og nødmeldesystemet ville vært totalavhengig av at terminalen klarte å finne både lokasjon og rutinginformasjon.

Ved innføring av ERDB følger også drifting og vedlikehold. Registeret skal dekke nødsentralenes jurisdiksjoner. Det vil si at det skal kunne oversette lokasjoner fra et gitt landeområde til den aktuelle nødsentralens adresse. Dette kan gjøres enten ved hjelp av én sentralisert database eller ved hjelp av distribuerte databaser som kommuniserer sammen, eksempelvis en database for hver jurisdiksjon. På den måten kan ansvaret for drifting og vedlikehold fordeles.

5.1.3.2 E-ruter (E-CSCF)

E-ruteren er grensesnittet mot nødsentralen (PSAP). Denne må følgelig kobles direkte mot PSAP. I et system der brukeren selv ikke anskaffer sin lokasjon, kan E-ruteren være direkte koblet mot lokasjonsmegleren, og ha ansvaret for anskaffelsen av lokasjon. Siden vi har definert at brukeren selv skal anskaffe sin lokasjon, er ikke dette tilfellet i vår arkitektur. E-ruteren er likevel tilkoblet lokasjonsmegleren for å kunne validere lokasjon.

5.2 Valgte løsninger for nødmeldesystemet

5.2.1 Signaleringsprotokoll

SIP brukes for å sette opp sesjoner for dataoverføring. Protokollen er fleksibel til forskjellige datatyper og transportprotokoller. I tillegg til dette er SIP-meldingene tekstbaserte. Dette gjør protokollen til et naturlig valg for nødmeldesystemet. Fordi meldingene og sesjonsbeksrivelsen er i klartekst er det intuitivt å tolke de nødvendige parametrene og eventuelt legge til ekstra attributter i sesjonsbeskrivelsen.

5.2.2 Lokasjonsformat

Kapittel 3.4.5 beskriver to metoder for transport av lokasjonsparametre; lokasjonsobjekt og sos-attributter. De standarder som er under utvikling foreslår lokasjonsobjektet PIDF-LO som lokasjonsformat. I vårt forslag til nødmeldesystem foreslår vi derimot bruk av sos-attributter.

PIDF-LO er et omfattende XML-skjema, som beskriver lokasjonsinformasjonen og regler for hvordan den skal kunne benyttes av anropets mottager. I et nødmeldesystem er det ikke mange lokasjonsparametre som **må** transporteres. Kapittel 3.4.4 beskriver de viktigste lokasjonsparametrene for et nødmeldesystem. I vår implementering har vi benyttet fem sos-attributter; lokasjon (koordinater eller adresse), format (type koordinatformat eller adresse), lokasjonskilde, MAC-adresse til terminalen og NAP MAC-adresse til aksesspunktet terminalen er tilkoblet. Hvis GPS er lokasjonskilden vil ikke NAP MAC-adressen være nødvendig.

I et nødmeldesystem der lav tidsforsinkelse er et av hovedkravene, er det hensiktsmessig med en løsning som minsker datavolumet som skal transporteres. Ved å legge til fire eller fem sos-attributter til SIP INVITE-meldingen vil nødvendig lokasjonsinformasjon transporteres til nødsentralen enkelt og effektivt, uten å modifisere SIP-meldingene i stor grad. Dette vil også kreve mindre kompleksitet på klientsiden.

I et nødmeldesystem styrt av nasjonale myndigheter kan det settes regler for hvordan lokasjonsinformasjonen skal behandles ut fra personvern og sikkerhet slik at brukeren er trygg på at sensitiv informasjon blir ivaretatt. I andre systemer trenger ikke dette være tilfelle. I systemer der det er hensiktsmessig å sette regler for hvordan lokasjonsinformasjonen kan benyttes vil bruk av sos-attributter være utilstrekkelig. I slike formål passer PIDF-LO utmerket. Man kan argumentere med at en lik standard for alle systemer er ønskelig, men ut fra de strenge kravene tilknyttet et nødmeldesystem har vi valgt det vi mener er den mest effektive løsningen ut fra våre forutsetninger.

5.2.3 Lokasjonsoppdatering

Lokasjonsoppdateringen kan hovedsaklig foregå på to måter:

- Kontinuerlig
- Oppslag ved anrop

Kontinuerlig lokasjonsoppdatering er når klienten innhenter sin posisjon ved faste intervall. Slik vil klienten alltid ha sin posisjon tilgjengelig uten tidsforsinkelse. Denne løsningen har to primære svakheter. For det første vil ikke posisjonsdataene alltid være ferske. Hvis intervallet for å innhente posisjonen er på T sekunder, er den maksimale feilmarginen lik avstanden klienten har forflyttet seg i løpet av tiden T. Hvis klienten befinner seg i et transportmiddel eller er i en annen form for bevegelse, kan denne avstanden bli så stor at den innhentede lokasjonen er verdiløs. Den andre svakheten er at kontinuerlig lokasjonsoppdatering tilfører ekstra overhead i nettverket. Ved å innhente posisjon i et intervall på T sekunder, blir altså antall spørringer i minuttet $S(\text{min}) = 60/T$. Hvis kontinuerlig lokasjonsoppdatering skal benyttes, må faktoren S avveies i forhold til hvor fersk lokasjon som er nødvendig kontra den ekstra belastning på nettverket.

Oppslag ved anrop er når klienten innhenter sin posisjon kun når anropet initialiseres. Dette skaper minimum belastning på nettverket, og lokasjonen er alltid fersk. Svakheten ved denne metoden er den ekstra tidsforsinkelsen som utsetter samtaleoppkoblingen.

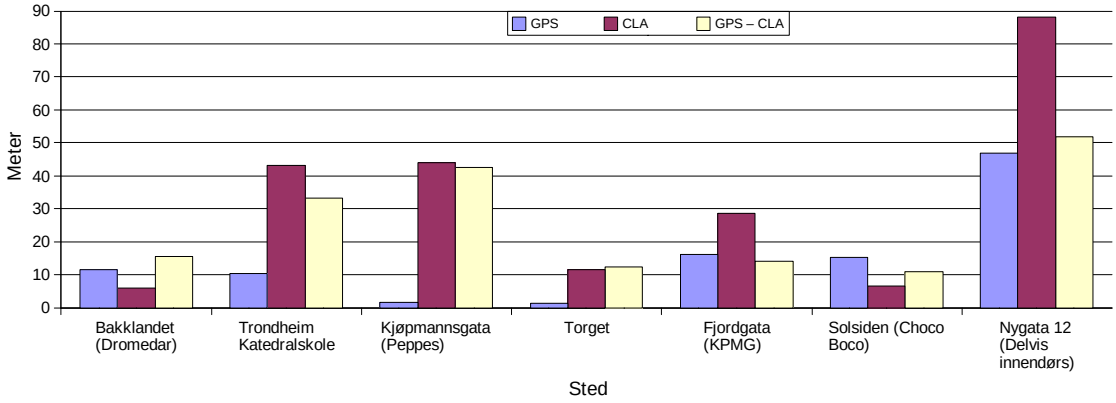
Det går også an å tenke seg hybride løsninger for lokasjonsoppdatering. Hvis oppslag ved anrop er begrenset av en tidsgrense, og denne brytes, kan lokasjonen som allerede finnes fra den kontinuerlige lokasjonsoppdateringen benyttes. Dette vil imidlertid medføre enda mer overhead i nettverket, så da kan S-faktoren justeres så oppdateringen ikke skjer så ofte. En løsning er å innhente lokasjonen hver gang klienten skifter trådløst aksesspunkt, og så benytte denne som reserve hvis oppslag ved anrop overskrider tidsgrensen.

I et nødmeldesystem vil en nøyaktig lokasjon være mer verdt enn ekstra tidsforsinkelse, iallfall hvis den ekstra tidsforsinkelsen kan begrenses. Derfor har vi i vårt system valgt å bruke oppslag ved anrop. Kombinert med GeoPos som lokasjonsmegler har våre tester vist akseptabel tidsforsinkelse ved oppsett av anrop [kap. 5.3.2]. En annen mulig løsning er å benytte ettersendelse av lokasjon, som vil gi minimal tidsforsinkelse. Men et slikt system vil medføre enda mer kompleksitet både på klient- og serversiden.

5.3 Analyse av testresultatene

Figur 5.1 illustrerer feilmarginene for GPS og CLA. Illustrasjonen er basert på tabell 4.3.

5.3.1 Feilmargin



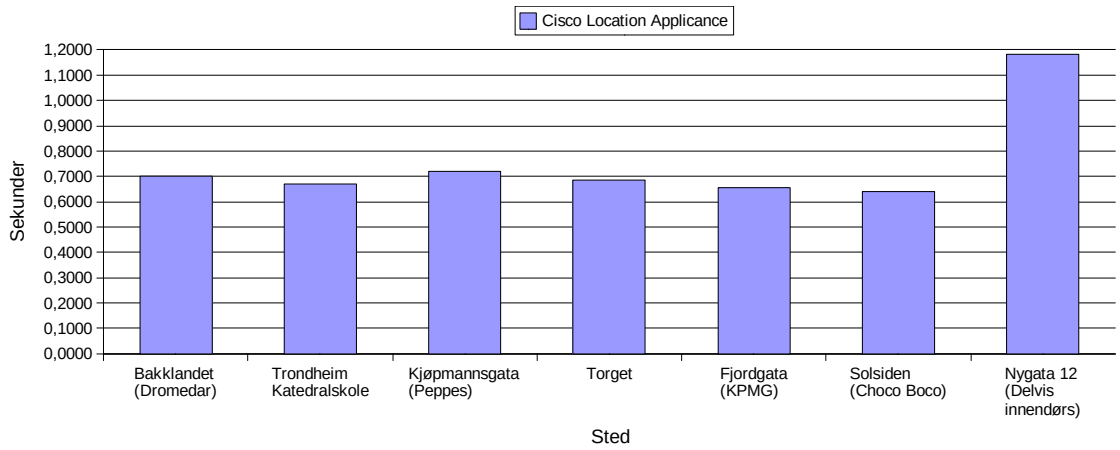
Figur 5.1: Feilmarginer i meter for GPS og CLA, og avstanden mellom lokasjonen angitt av GPS og CLA. Basert på tallene i tabell 4.3.

Feilmarginene er relativt varierende for CLA. GPS gir en lav feilmargin (<10-15 meter) så lenge målingen blir foretatt i et åpent område. Målingen som avviker fra dette er målingen for Nygata. Dette avviket skyldes sannsynligvis at målingen ble foretatt i vinduet på en leilighet, dermed delvis innendørs. CLA hadde også sin høyeste feilmargin i denne målingen. Vegger og bygninger svekker signalene til både GPS og WiFi-senderne i Trådløse Trondheim, og kan dermed gjøre at kalkuleringen av lokasjonen blir feil. Utgangspunktskoordinatene hentet fra Nasjonal Vegdatabank er også en mulig feilkilde for enkelte av teststedene. Likevel viser noen av GPS-målingene under 2 meter i feilmargin, noe som vil tilsi at utgangspunktkoordinatene er rimelig nøyaktige.

5.3.2 Tidsforsinkelse

Figur 5.2 illustrerer gjennomsnittlig tidsforsinkelse for CLA. Figuren er basert på tabell 4.4.

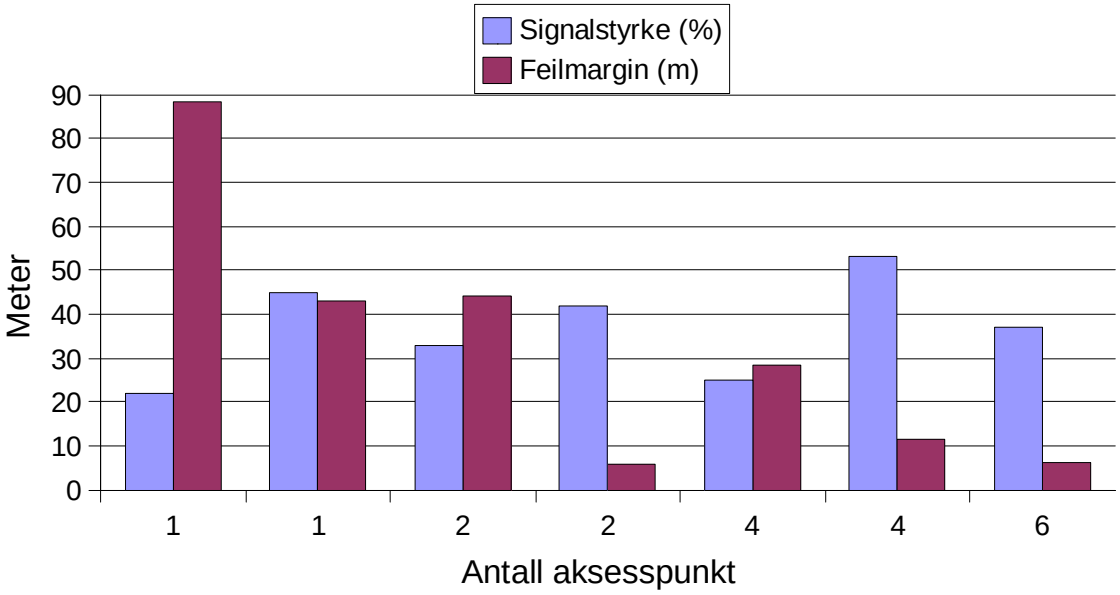
Gjennomsnittstiden CLA brukte for å innhente lokasjonen til en terminal lå jevt mellom 0,64 og 0,72 sekunder, med unntak for Nygata som var den eneste målingen på over 1 sekund. Dette skyldes trolig lav signalstyrke og dårlig dekning i dette området. Denne gjennomsnittstiden kan øke på en terminal med lavere utregningskraft, og siden kallet etter lokasjon går via Internett kan en tilkobling med lav hastighet øke tidsforsinkelsen. I tillegg vil noe av forsinkelsen være forårsaket av lokasjonsmegleren (GeoPos) i spørringen mot CLA. Likevel vil mesteparten av tidsforsinkelsen grunnes CLA (eller en annen



Figur 5.2: Gjennomsnittstiden det tar for CLA å innhente posisjonen til en terminal. Basert på tallene fra tabell 4.4.

lokasjonskilde) som søker etter terminalens lokasjon. Vi kan derfor konkludere med at gjennomsnittstiden er jevnt lav for CLA, og vil være det uavhengig av terminal.

5.3.3 Feilmargin i forhold til signalstyrke



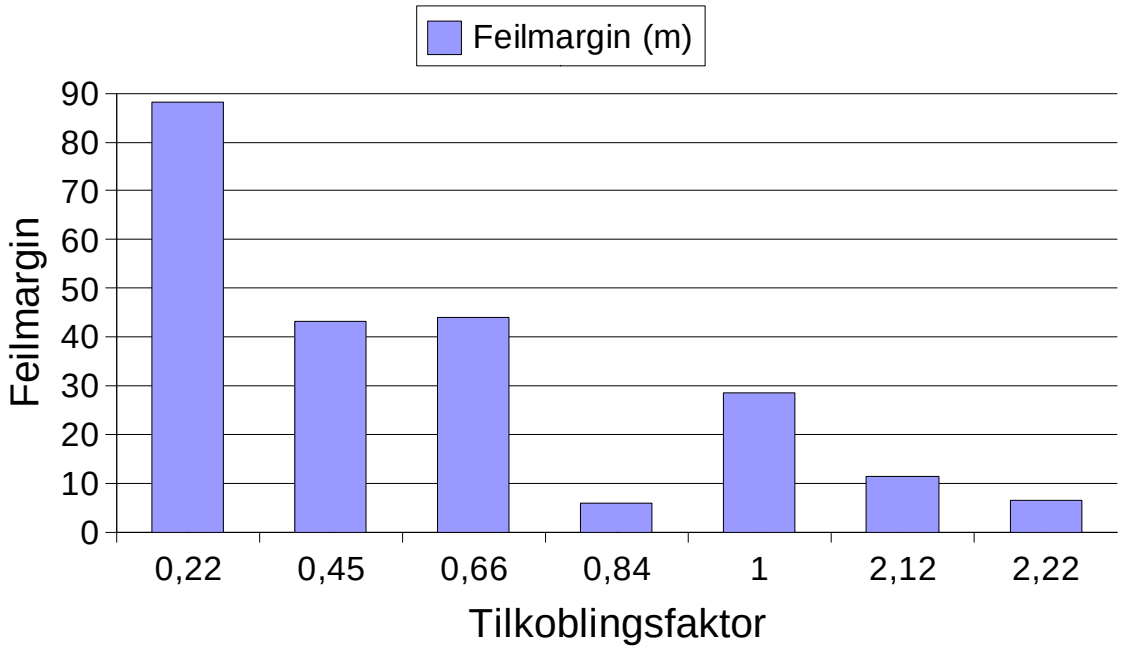
Figur 5.3: CLA signalstyrke i forhold til antall aksesspunkter. I tillegg vises signalstyrken i %, slik at sammenhengen kan ses mellom signalstyrke og feilmargin på steder med like mange aksesspunkter. Basert på tallene i tabell 4.5.

Figur 5.3 illustrerer feilmarginen i forhold til antall aksesspunkter. For hvert sted med like mange aksesspunkter vises også signalstyrken i %. Figuren viser at feilmarginen er lavere jo høyere antall aksesspunkter som finnes på et sted. I tillegg viser figuren at på steder

med like mange aksesspunkter vil feilmarginen være lavere jo sterkere signalstyrken er. Signalstyrken er sterkere jo nærmere aksesspunktene terminalen er, og derfor vil også denne avstanden ha betydning for resultatet.

Dette forklarer feilmarginene i figur 5.1 med at CLA fungerer godt i åpent terreng som Torget, Bakklandet og Solsiden. CLA fungerer dårlig i utkanten av Trådløse Trondheim, altså der WiFi-signalene blir svakere. Ved Kjøpmannsgata, Nygata og Trondheim Katedralskole var signalstyrken svekket, og CLA ga høyest feilmargin ved disse områdene.

Figur 5.4 introduserer en *tilkoblingsfaktor*, som er lik antall aksesspunkter multiplis-



Figur 5.4: CLA tilkoblingsfaktor, som er lik antall aksesspunkter multiplisert med signalstyrke i prosent. Figuren viser hvor høy feilmarginen er i forhold til tilkoblingsfaktoren.

ert med signalstyrke i prosent. Figuren illustrerer hvor høy feilmarginen er i forhold til denne tilkoblingsfaktoren. Poenget med figuren er å bedre illustrere konklusjonen fra figur 5.3, nemlig at feilmarginen blir lavere desto høyere tilkoblingsfaktoren er. For å få et nøyaktig resultat fra CLA er terminalen altså avhengig av både antall aksesspunkter og signalstyrke. Utfra figuren kan vi konludere med at en tilkoblingsfaktor < 1 gir varierende feilmargin, og at en tilkoblingsfaktor > 2 gir jevnt lav feilmargin. CLA er altså avhengig av høyest mulig tilkoblingsfaktor, helst høyere enn 2. (For eksempel fire aksesspunkter med gjennomsnittlig 50% signalstyrke).

5.4 Valg av lokasjonstjeneste for nødmeldesystem

Trådløse Trondheim er et nettverk tilknyttet en by. Likevel er de trådløse aksesspunktene basert på WiFi-signaler, som vanligvis har svært dårlig innendørs dekning. Dette vanskeliggjør posisjonsinnhentingen, og de tre lokasjonstjenestene vi har beskrevet i kapittel 3.6 har ulike fordeler og ulemper som illustrert i figur 5.5.

Kapittel 5.3 viser testresultatene våre grafisk. De fleste av testene ble utført i forhold til

Kriterier/Lokasjonstjeneste	GPS	CLA	Lokasjonsdatabase
Oppstartsforsinkelse (sekunder)	Høy	Lav	Lav
Tidsforsinkelse (sekunder)	Ingen	Middels	Lav
Feilmargin (meter)	Lav	Middels	Høy
Administrasjon	Ingen	Ingen	Høy
Overhead i nettverket	Ingen	Middels	Lav
Innendørs dekning	Nei	Ja	Ja
Uavhengig av underliggende nettverk	Ja	Nei	Nei
Uavhengig av klientens terminal	Nei	Ja	Ja
Forskjellige lokasjonskilder	Nei	Ja	Nei
Beskrivende output	Nei	Ja	Nei

Figur 5.5: Kriteriene til de tre aktuelle lokasjonstjenestene, og i hvilken grad de blir oppfylt. De tre gradene er merket med fargekoder, der grønn er bra, rød er dårlig og svart er middels.

CLA, da det er denne lokasjonskilden det er knyttet mest usikkerhet til. Analysen viser at CLA har jevnt lav tidsforsinkelse, som er innenfor kravene til et nødmeldesystem. Feilmarginen er varierende, men analysen viser at den er avhengig av *tilkoblingsfaktoren*, nemlig hvor mange aksesspunkter terminalen er tilknyttet og signalstyrken til disse. Analysen viser også at GPS har en lav feilmargin, så lenge den er *varm*. Lokasjonsdatabase basert på MAC ble ikke testet, da vi anser dette som en sekundærløsning på grunn av høy feilmargin. I kapittel 3.6.5 foreslår vi at lokasjonsdatabase basert på MAC kan brukes i hybride løsninger for å gi en indikasjon på lokasjon nøyaktig nok til å gjennomføre geografisk ruting.

Sammenligner vi analyseresultatene med figur 5.5, kan vi konkludere med at GPS er det beste valget med tanke på feilmargin og tidsforsinkelse. GPS er passende i tilfeller der det er strenge krav til lav feilmargin. Men de svake sidene ved GPS, som oppstartsforsinkelse og mangel på innendørs dekning gjør GPS til en begrenset løsning for en nødmeldetjeneste. Lokasjonsdatabase oppfyller krav om lav tidsforsinkelse, men feilmarginen er for høy til å kunne brukes som primærløsning i en nødmeldetjeneste. Som alenestående lokasjonstjeneste fremstår derfor CLA som best egnet for vår nødmeldetjeneste. CLA har ingen store svakheter, men varierende feilmargin er et usikkerhetsmoment. Etterhvert som nettverksteknologien utvikler seg er det rimelig å anta at feilmargin og tidsforsinkelse vil bli lavere for CLA.

På grunnlag av dette har vi valgt en hybrid løsning, med GPS og GeoPos i parallell. Hovedprinsippet for denne løsningen er at lokasjonsdata fra GPS benyttes hvis de er tilgjengelige, og hvis ikke brukes GeoPos for å innhente lokasjon fra en annen lokasjonskilde (for eksempel CLA). Dette gjelder for situasjoner der GPS ikke har blitt varm, eller innendørs der det er nettverksdekning. For vår plug-in løsning har vi implementert både GPS og GeoPos slik at brukeren kan velge hvilken lokasjonstjeneste som benyttes. Ved å kombinere GPS og GeoPos lager vi en hybrid løsning som innehar alle de positive egenskapene til GPS, og i tillegg tilbyr lokasjon i situasjoner der GPS ikke strekker til.

5.5 Andre bruksområder

Arkitekturen vi har beskrevet er først og fremst tilpasset et nødmeldesystem, men det vil også være aktuelt å benytte arkitekturen som grunnlag for andre lokasjonsbaserte tjenester. Klienten har direkte tilgang til lokasjonsmegleren gjennom et web-API. Dette gjør det enkelt for utviklere å lage nye applikasjoner som benytter seg av lokasjonsmegleren. På denne måten kan forskjellige applikasjonstyper finne klientens lokasjon gjennom dette grensesnittet. Som tidligere nevnt er megleren et kritisk avhengighetpunkt, og den håndterer mye av nettverkslasten ved et lokasjonsoppslag. Derfor bør megleren ha en funksjon for å prioritere disse oppslagene slik at lokasjonsoppslag for nødanrop kan prioriteres.

Dersom et anrop skal rutes basert på lokasjonsinformasjon, må sesjonsmeldingene gå via E-ruteren og ERDB. Dette er også en svakhet i arkitekturen. E-ruteren er primært en del av nødfunksjonaliteten i systemet. For å unngå store trafikkmengder i ruteren bør derfor kun nødanrop behandles av disse. For mange tjenester vil ikke geografisk ruting være like viktig som posisjonsinnhenting. Det er først og fremst for landsomfattende tjenester som for eksempel ruteopplysning og vegtrafikksentralen det kan være aktuelt med geografisk ruting på samme måte som for et nødmeldesystem.

Kapittel 6

Konklusjon

Vi har utarbeidet et forslag til en arkitektur som baserer seg på signaleringsprotokollen SIP. Vi har delt arkitekturen opp i tre deler basert på funksjonalitet for klient, posisjonsinnhenting og nødanropshåndtering. Arkitekturen er laget med Trådløse Trondheim som nettverksplattform, men har skaleringsevne for nasjonalt omfang. Løsningen vår baserer seg på et "tykk klient"-prinsipp, der funksjonaliteten for å innhente lokasjon ligger på klientsiden, i form av en plug-in løsning i terminalen. Vi har implementert denne løsningen i en IP-basert terminal, samt laget funksjonalitet for håndtering av nødanrop. På denne måten kan et fullverdig nødanrop med posisjonsinnhenting simuleres. Løsningen er testet med hensyn på forskjellige lokasjonskilder.

Plug-in løsningen vi har implementert anskaffer lokasjon ved nødanrop, enten fra en terminalbasert lokasjonskilde (GPS) eller en lokasjonsmegler (GeoPos). GPS har lav tidsforsinkelse og lav feilmargin, men er avhengig av å være *varm* og har ikke dekning innendørs. GeoPos kan kobles til flere lokasjonskilder, for eksempel CLA som er den beste alenestående løsningen ut fra våre evalueringskriterier og tester. Testene foretatt viser at CLA har jevnt lav tidsforsinkelse, og lav feilmargin så lenge tilkoblingsfaktoren (antall aksesspunkt i forhold til signalstyrke) er på et akseptabelt nivå. Vi har valgt en hybrid løsning med GPS og GeoPos for å dra nytte av begges egenskaper. GPS benyttes hvis lokasjonen er tilgjengelig. Hvis ikke benyttes GeoPos til å innhente lokasjonen fra en annen lokasjonskilde.

Et IP-basert nødmeldesystem vil etterhvert komme. Dette systemet vil inneha større nytteverdi i form av nye nødmeldetjenester. Det er likevel viktig at brukeren kjenner igjen funksjonene fra dagens PSTN-baserte system. Et nødanrop er kritisk, og et nødmeldesystem vil alltid kunne forbedres slik at hjelpen kommer fram raskere. Utfordringen er å skape et effektivt system med lav feilprosent og høy tilgjengelighet. I framtiden vil et slikt system kunne utnyttes slik at det i større grad er mulig å gjennomføre behandling utenfor sykehuset, i form av fjernhjelp eller andre kommunikasjonsmetoder. Vi håper at denne oppgaven kan bidra i arbeidet med å spesifisere fremtidens nødmeldesystem.

6.1 Videre arbeid

For videreføring av denne oppgaven er dette emner som kan utredes:

- *Forbedre samarbeidet mellom GPS og GeoPos i den hybride løsningen:* Definere kriteriene for når de to lokasjonstjenestene skal benyttes, med fokus på hvor grensen går for at GPS ikke skal benyttes. For eksempel kan det ses på antall satelitter GPS har kontakt med, og hvor fersk lokasjonen er.
- *Legge inn SSID-sjekk i GeoPos:* Per dags dato bruker GeoPos mye tid på å finne ut at en brukers MAC-adresse ikke er tilknyttet nettverket. Hvis brukeren sender med sin SSID til GeoPos vil den først kunne utføre en "dummy"-sjekk som sjekker at brukeren faktisk er tilkoblet riktig nettverk. På denne måten avlastes GeoPos for unødvendige henvendelser.
- *Lokasjonsdatabase basert på MAC:* Implementering og testing av denne løsningen, gjerne med GeoPos som lokasjonsmegler, spesielt med tanke på feilmargin og tidsforsinkelse.
- *Grensesnitt mellom entitetene i arkitekturen:* Definere grensesnitt mellom alle entitetene og all kommunikasjon innad i nødmeldesystemet. Interaksjon mellom entitetene kan illustreres ved hjelp av MSC-diagrammer.
- *Prototype:* Demonstratoren som ble utviklet er basert på Trådløse Trondheim. Denne kunne blitt utviklet som prototype med en reell PSAP og bruk av geografisk ruting. Et slikt reellt system kunne så blitt testet i henhold til våre kriterier. Man kunne også utviklet et nasjonalt nødmeldesystem, for å teste skalering.
- *Implementeringsverdien for andre lokasjonsbaserte tjenester:* Lokasjonsinformasjon om brukeren muliggjør lokasjonsbaserte tjenester
- *Innføre lokasjonskilder for andre nett:* Først og fremst er en lokasjonskilde for mobiltelefoner ønskelig, men også andre lokasjonskilder kan være hensiktsmessig å implementere.
- *Sikkerhet:* Sikkerhet er selvfølgelig et viktig poeng i alle deler av et nødmeldesystem. Sensitive opplysninger blir kommunisert, og det er viktig å hindre misbruk av nødmeldesystemet.
- *Personvern:* Lokasjonen til en bruker kan åpenbart misbrukes. Derfor er det viktig å ivareta personvern. Dette kan løses innenfor både sikkerhet og arkitektur. I tillegg må brukeren bli klar over hvordan et lokasjonsbasert system fungerer. For eksempel kan brukeren velge å bare sende ved lokasjon til enkelte tjenester.

Bibliografi

[3GP06] 3GPP. *IP Multimedia Subsystem (IMS) emergency sessions.* 3GPP, ts 23.167 v7.2.0 edition, september 2006.

[AA07] C. Militeau A. Akundi. *Location Acquisition and Location Parameter Conveyance for Internet Access Networks in Support of Emergency Services.* ATIS, 010407-037 edition, januar 2007.

[And07] Steinar Andresen. *Om den norske modellen for medisinsk nødmelding og hvorfor vi trenger direkte innvalg til medisinsk hjelp*, juni 2007.

[AS] NRDB AS. *Nasjonal Referanse Database NRDB.* `http://www.nrdb.no/`.

[Ass06] Telecommunications Industry Association. *Link Layer Discovery Protocol for Media Endpoint Devices.* Telecommunications Industry Association, 2006. `http://www.tiaonline.org/standards/technology/voip/documents/ANSI-TIA-1057_final_for_publication.pdf`.

[BR07] J. Polk A. Newton B. Rosen, H. Schulzrinne. *Framework for Emergency Calling in Internet Multimedia.* IETF, 2007. `http://tools.ietf.org/html/draft-ietf-ecrit-framework-01`.

[Com01] European Commission. *State of implementation of the single European emergency call number '1-1-2'.* EU, oktober 2001. `http://ec.europa.eu/environment/civil/pdfdocs/112surv-2001.pdf`.

[Cor03] Intel Corporation. *Overcoming Barriers to High-Quality Voice over IP Deployments.* Intel Corporation, 2003. `http://www.intel.com/network/csp/pdf/8539.pdf`.

[EMT06] EMTEL. *Emergency calls and VoIP: Possible short and long term solutions and standardisation activities.* ETSI, tr 102 4776 v.0.0.4 edition, september 2006.

[FCC06] FCC. *Consumer facts: Wireless 911 services.* FCC, mars 2006. `http://www.fcc.gov/cgb/consumerfacts/wireless911srvc.html`.

[Fir03] FireNet. *History of the 999 system and fire brigades.* FireNet, 2003. `http://www.fire.org.uk/advice/999history.htm`.

[HS02] K. Arabshian H. Schulzrinne. *Providing Emergency Services in Internet Telephony.* Columbia University, 2002. `http://www1.cs.columbia.edu/~knarig/911.pdf`.

[HS04] B. Rosen H. Schulzrinne. *Emergency Services for Internet Telephony Systems.* IETF, juli 2004.
http://tools.ietf.org/html/draft-schulzrinne-sipping-emergency-arch-02.

[HS06] J. Polk H. Schulzrinne. *Communications Resource Priority for the Session Initiation Protocol (SIP).* IETF, 2006.
http://tools.ietf.org/html/rfc4412.

[HS07] R. Marshall H. Schulzrinne. *Requirements for Emergency Context Resolution with Internet Technologies.* IETF, februar 2007.
http://tools.ietf.org/html/draft-ietf-ecrit-requirements-13.

[Hun06] S. Hun. *Legevaktorganisering i Norge.* Unifob Helse, juli 2006.
http://www.unifobhelse.no/admin2/Sidefiler/189.RAPPORTFRAregister11.07.06.pdf.

[Inc07] Cisco Systems Inc. *Cisco Wireless Location Appliance.* Cisco Systems Inc., 2007.
http://www.cisco.com/application/pdf/en/us/guest/products/ps6386/c1650/cdccont_0900aecd80293728.pdf.

[JK07] D. Sisalem J. Kuthan. *SIP: More Than You Ever Wanted To Know About.* Tekelex, mars 2007.

[JL02] J. DeSalas J. LaMance, J. Jarvinen. *Assisted GPS: A Low-Infrastructure Approach.* GPS World, mars 2002.
http://www.gpsworld.com/gpsworld/article/articleDetail.jsp?id=12287.

[JP04] M. Linsner J. Polk, J. Schnizlein. *Dynamic Host Configuration Protocol Option for Coordinate-based Location Configuration Information.* IETF, 2004.
http://tools.ietf.org/rfc/rfc3825.txt.

[JP07] B. Rosen J. Polk. *Session Initiation Protocol Location Conveyance.* IETF, februar 2007.
http://tools.ietf.org/html/draft-ietf-sip-location-conveyance-07.

[J.R02] J.Rosenberg. *SIP: Session Initiation Protocol.* IETF, juni 2002.
http://tools.ietf.org/html/rfc3261.

[JW07] B. Stark J. Winterbottom, M. Thomson. *HTTP Enabled Location Delivery (HELD).* IETF, 2007.
http://tools.ietf.org/html/draft-winterbottom-http-location-delivery-05.

[MH06] C. Perkins M. Handley, V. Jacobson. *SDP: Session Description Protocol.* IETF, juli 2006.
http://tools.ietf.org/html/rfc4566.

[MMH05] H. Schulzrinne X. Wu M. Mintz-Habib, A. Rawat. *A VoIP Emergency Services Architecture and Prototype.* IEEE, juni 2005.
http://ieeexplore.ieee.org/iel5/10216/32582/01523929.pdf.

[MT07a] J. Winterbottom M. Thomson. *GEOPRIV PIDF-LO Usage Clarification, Considerations and Recommendations.* IETF, april 2007.
http://tools.ietf.org/html/draft-ietf-geopriv-pdif-lo-profile-07.

[MT07b] J. Winterbottom M. Thomson. *Revised Civic Location Format for PIDF-LO.* IETF, februar 2007.
http://tools.ietf.org/html/draft-ietf-geopriv-revised-civic-lo-05.

[OH05] D. Gurle O. Hersent, J. Petit. *IP Telephony - Deploying Voice-over-IP protocols : The session initiation protocol (SIP)*, pages 159–261. Wiley, 2005.

[Pet05] J. Peterson. *A Presence-based GEOPRIV Location Object Format.* IETF, desember 2005.
http://tools.ietf.org/html/rfc4119.

[Qui04] J. M. Quijada. *H.323 and SIP Overview/Comparison.* EETS, 2004.
http://phoenix.labri.fr/documentation/sip/Documentation/Papers/SIP/Presentation/SIPH323-jq.pdf.

[Ran05] B. Rankin. Does ip address reveal my physical location? *Ezine*, november 2005.
http://ezinearticles.com/?Does-IP-Address-Reveal-My-Physical-Location?&id=94220.

[Sch06] H. Schulzrinne. *Emergency Services URI for the Session Initiation Protocol*, januar 2006.
http://tools.ietf.org/html/draft-ietf-sipping-sos-02.

[TH07] H. Schulzrinne H. Tschofenig T. Hardie, A. Newton. *LoST: A Location-to-Service Translation Protocol.* IETF, 2007.
http://tools.ietf.org/html/draft-ietf-ecrit-lost-05.

[Tro07] Trådløse Trondheim. *Om Trådløse Trondheim.* Trådløse Trondheim, februar 2007.
http://www.tradlosetrondheim.no/sec.php?page=sec_wirelesstrondheim&la=no.

[Tsc06] H. Tschofenig. *The IETF Geopriv and Presence Architecture Focusing on Location Privacy.* W3C, juli 2006.
http://www.w3.org/2006/07/privacy-ws/papers/26-tschofening-geopriv/.

[Val07] R. Valdes. *How VoIP works.* How stuff works, mai 2007.
http://communication.howstuffworks.com/ip-telephony.htm/printable.

[Wik07a] Wikipedia. *Galileo positioning system.* Wikipedia, mai 2007.
http://en.wikipedia.org/wiki/Galileo_positioning_system.

[Wik07b] Wikipedia. *Geography Markup Language.* Wikipedia, mai 2007.
http://en.wikipedia.org/wiki/Geography_Markup_Language.

[Wik07c] Wikipedia. *Global Navigation Satellite System.* Wikipedia, mai 2007.
http://en.wikipedia.org/wiki/GNSS.

[Wik07d] Wikipedia. *GLONASS*. Wikipedia, mai 2007. http://en.wikipedia.org/wiki/GLONASS.

[Wik07e] Wikipedia. *GSM localization*. Wikipedia, mai 2007. http://en.wikipedia.org/wiki/GSM_localization.

Kapittel 7

Appendiks

Appendiks A : Korrespondanse med St. Olavs Hospital
Appendiks B : Rammeverk og verktøy benyttet i den praktiske delen
Appendiks C : SIP INVITE melding med sos-attributter
Appendiks D : Klassediagram for klient- og serversiden
Appendiks E : Skjermbilde av serversidens kartapplikasjon
Appendiks F : Målinger i Trådløse Trondheim

Appendiksene er sortert etter når de er referert i teksten.

A: Korrespondanse med St. Olavs Hospital

For å finne ut hvilke krav AMK-sentralen ved St. Olavs Hospital setter til nødanrop, har vi kontaktet dem via epost:

Vi er to studenter ved NTNU som skriver masteroppgave om posisjonsinnhenting for nødmeldetjenester i Trådløse Trondheim"med professor Steinar H. Andresen som veileder. Vi skal studere hvordan en klient som benytter VoIP kan finne sin egen lokasjon, og legge ved denne i anropet til AMK-sentralen, slik at AMK-sentralen med en gang ved hvor anropet originerer fra. Lokasjonen som blir overført vil bestå av enten koordinater (GPS) eller gateadresse. I denne anledning må vi sette opp diverse krav til systemet, for å evaluere forskjellige tekniske løsninger. Disse kravene hadde vi håpet dere kunne hjelpe oss med å fastsette :

1. *Feilmargin. Hvor mange meter feilmargin kan tolereres?*
   Dessverre kan vel dette ikke oppgis I rommet, dvs kan si kun hvor på kartet/geografien anropet kommer fra, ikke hvilken etasje. Derfor bør det vel være så liten feilmargin at en kan rope og få svar. Derfor maks 20 meter, kanskje.

2. *Tidsforsinkelse. Det vil ta lengre tid å sette opp ett anrop hvis man skal finne lokasjonen når man ringer. Hvor stor tidsforsinkelse kan tolereres?*
   Helst ingen, duppeditten som har VoIP bør hele tiden vite hvor den er. Når du er syk eller trenger hjelp raskt, er det vanskelig å starte med noe du ikke gjør til vanlig/daglig: Finne fram egen lokasjon i en slik situasjon tror jeg kan være vanskelig. Kan en ringe først og så etterpå sende lokasjon? Kontakten med 113 er viktigst, dernest lokasjon. Derfor bør duppeditten ha med som vedlegg lokasjon allerede ved kontakt med 113. Kun nødsentralene kan være de som kan avlese lokasjon. Derfor primært ingen tidsforsinkelse, sekundært så liten tidsforsinkelse som mulig.

3. *Har dere støtte for IP-telefoni (VoIP)? Hvis ikke, planer for fremtida?*
   Vi har ikke støtte for IP-telefoni, men ved anrop fra IP-telefon skal opprinnelsesmarkeringen følge dersom de ringer fra et fast punkt (krav fra Post og Teletilsynet).

4. *Hvilke løsninger har dere for å finne lokasjon til en som ringer fra mobiltelefon. Må dette oppgis av innringer, eller har dere tekniske løsninger som skaffer dette? Hvor nøyaktig er det isåfall?*
   Vi har ikke opprinnelsesmarkering fra mobiltelefoni. De løsningene som tilbys fra Telenor, NetCom og andre leverandører har ikke en nøyaktighetsgrad som vi er tjent med. Vi har mange radiobaser i vårt område uten sektorisiserte antenner slik anrop over mobiltelefonnettet vil ha alt for stor unøyaktighet til at vi kan stole på posisjonene som følger anropet.

Spørsmål 1 og 2 er besvart av Johan-Arnt Hegvik, medisinsk systemansvarlig.
Spørsmål 3 og 4 er besvart av TØ, teknisk systemansvarlig.
Korrespondansen har foregått med Kirsten Mo Haga, seksjonsleder ved Medisinsk nødmeldetjeneste AMK-LV-sentralen, St. Olavs Hospital.

B: Rammeverk og verktøy benyttet i den praktiske delen

Rammeverk

- Active Sync 4.0
- Microsoft .NET Framework 2.0
- Microsoft .NET Framework 2.0 SDK
- Microsoft .NET Compact Framework 2.0
- Microsoft Device Emulator 1.0
- Microsoft Windows SDK for Pocket PC 2002
- Microsoft Windows SDK for Smartphone 2002
- OpenNETCF Framework
- Smart Device Framework 2.1 Extensions for Visual Studio

Programmeringsverktøy

- Microsoft Visual Studio 2005 med støtte for Visual C# og Windows Mobile 5.0 Pocket PC

Simuleringsverktøy

- SJ Phone version 1.60 Build 289a, 12. juli 2005
- WireShark version 0.99.5 (SVN Rev 20677)

Klient/Terminal

- Fujistu Siemens Loox N95 Pocket PC med innebygd GPS
- Operativsystem : Windows Mobile 5.0

C: SIP INVITE melding med sos-attributter

```
2007-06-12 20:16:49.937 UDP 129.241.200.44:5060->LOCAL
INVITE sip:sos@129.241.209.203:5060 SIP/2.0
Record-Route: <sip:129.241.200.44;lr=on;ftag=230821822905>
To: <sip:sos@callme.item.ntnu.no:5060>
From: "fg"<sip:luke@callme.item.ntnu.no:5060>;tag=230821822905
Via: SIP/2.0/UDP 129.241.200.44;branch=z9hG4bK6f5a.c3a2d033.0
Via: SIP/2.0/UDP 127.0.0.1;received=129.241.209.98;rport=7000
Call-ID: 000020EA-2CC9-0000-E66C-000059200000@192.168.1.100
CSeq: 1 INVITE
Contact: <sip:luke@192.168.1.100:7000>
Max-Forwards: 69
User-Agent: SJphone/1.60.303c (SJ Labs)
Content-Length: 260
Content-Type: application/sdp
P-hint: usrloc applied

v=0
o=- 3390668204 3390668204 IN IP4 127.0.0.1
s=SJphone
c=IN IP4 127.0.0.1
t=0 0
a=direction:active
m=audio 49160 RTP/AVP 8 0 3 101
a=rtpmap:8 PCMA/8000
a=rtpmap:0 PCMU/8000
a=rtpmap:3 GSM/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-11,16
a=soscoord:569477.0 7034368.0
a=sosformat:UTM
a=sossource:GeoPos
a=sosmac:00:0B:85:89:B2:AE
a=sosnapmac:00:30:05:B6:18:AF
a=sosdelay:00:00:05
```

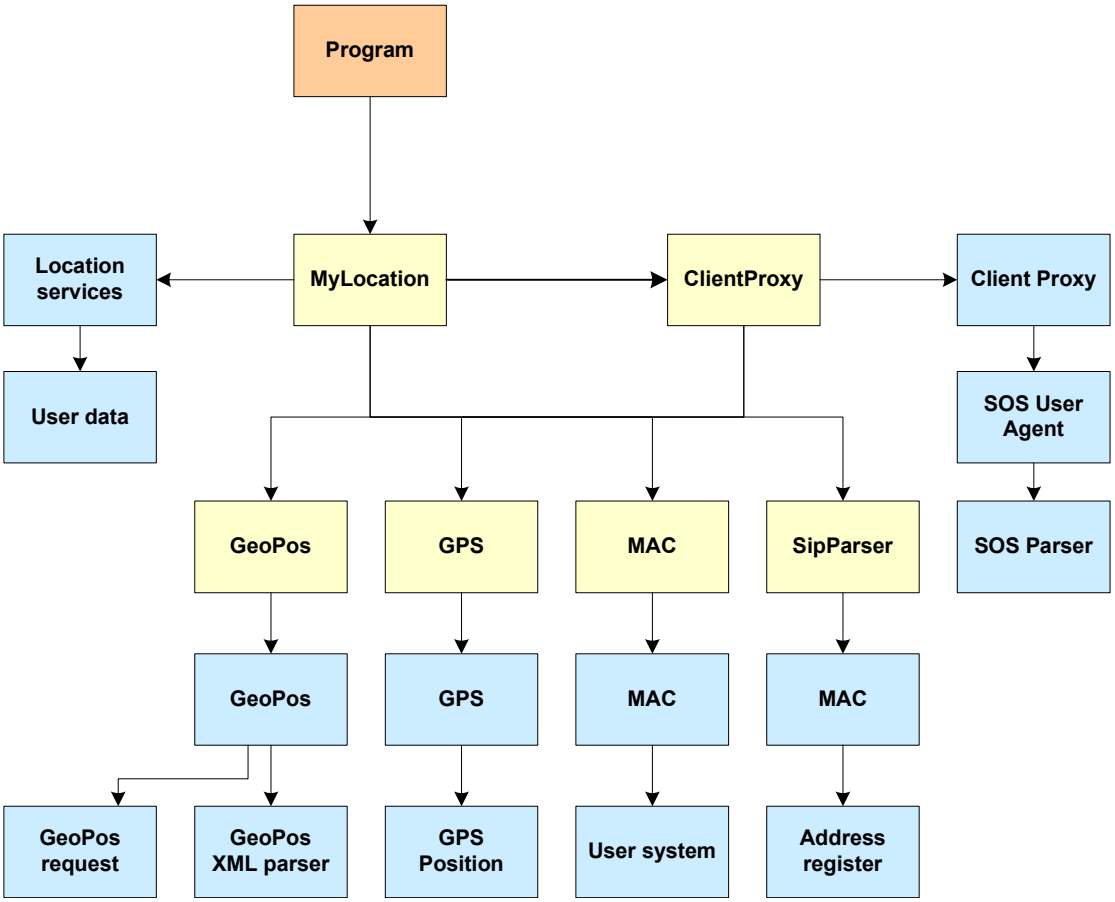
Figur 7.1: SIP INVITE-melding med sos-attributter slik nødsentralen mottar den. sos-attributtene er uthevet med fet tekst. sosdelay kommer i tillegg til sos-attributtene beskrevet i kapittel 4.2.1, og viser hvor lang tid det tok å anskaffe lokasjonen.

D: Klassediagram for klient- og serversiden

Dette appendikset inneholder to klassediagram for funksjonalitet på klient- og serversiden. På klientsiden blir funksjonaliteten implementert som en plug-in løsning for VoIP-applikasjonen i terminalen. På serversiden er funksjonaliteten implementert som en applikasjon (kalt sniffer), som fungerer uavhengig av terminal.

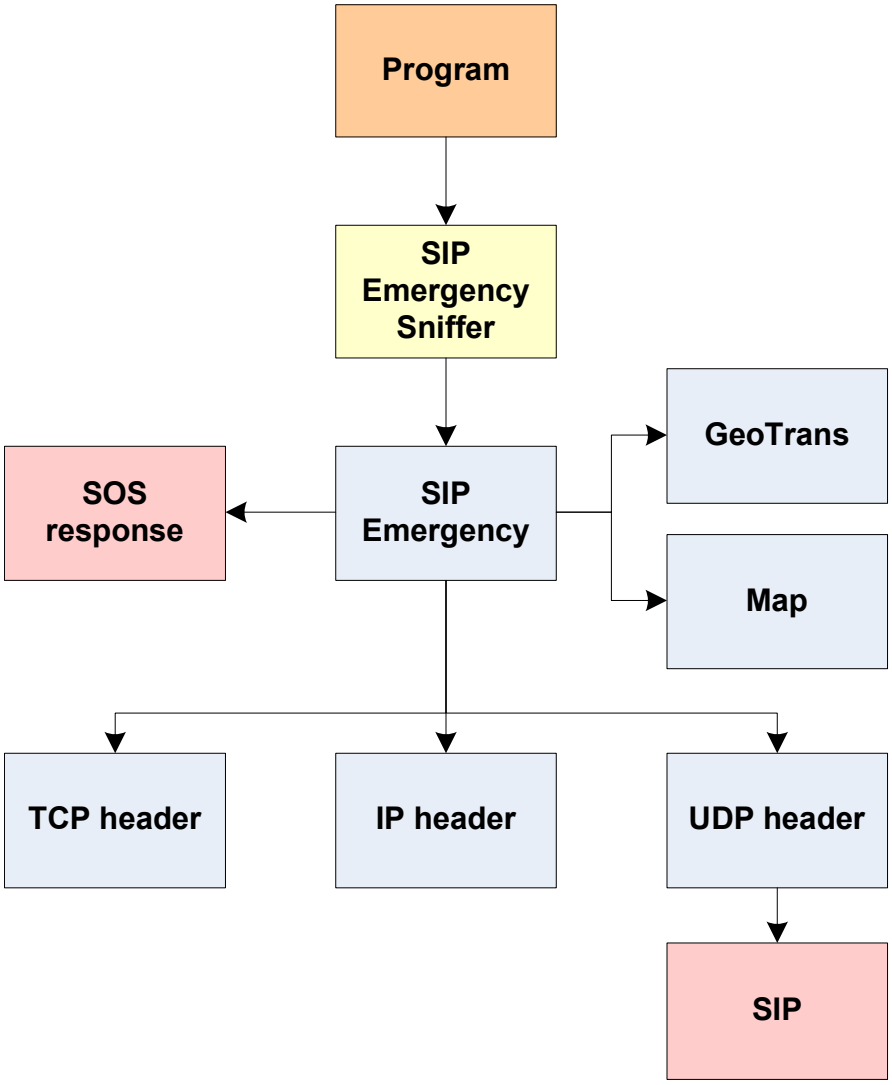
Implementeringen er modulbasert, det vil si at hvert bibliotek (de gule boksene) kan fungere uavhengig av de andre bibliotekene og på egen hånd. Dette muliggjør gjenbruk av bibliotekene. Pilene i klassediagrammene viser hvordan bibliotekene kommuniserer.

Klassediagram for klientsiden (plug-in løsning)



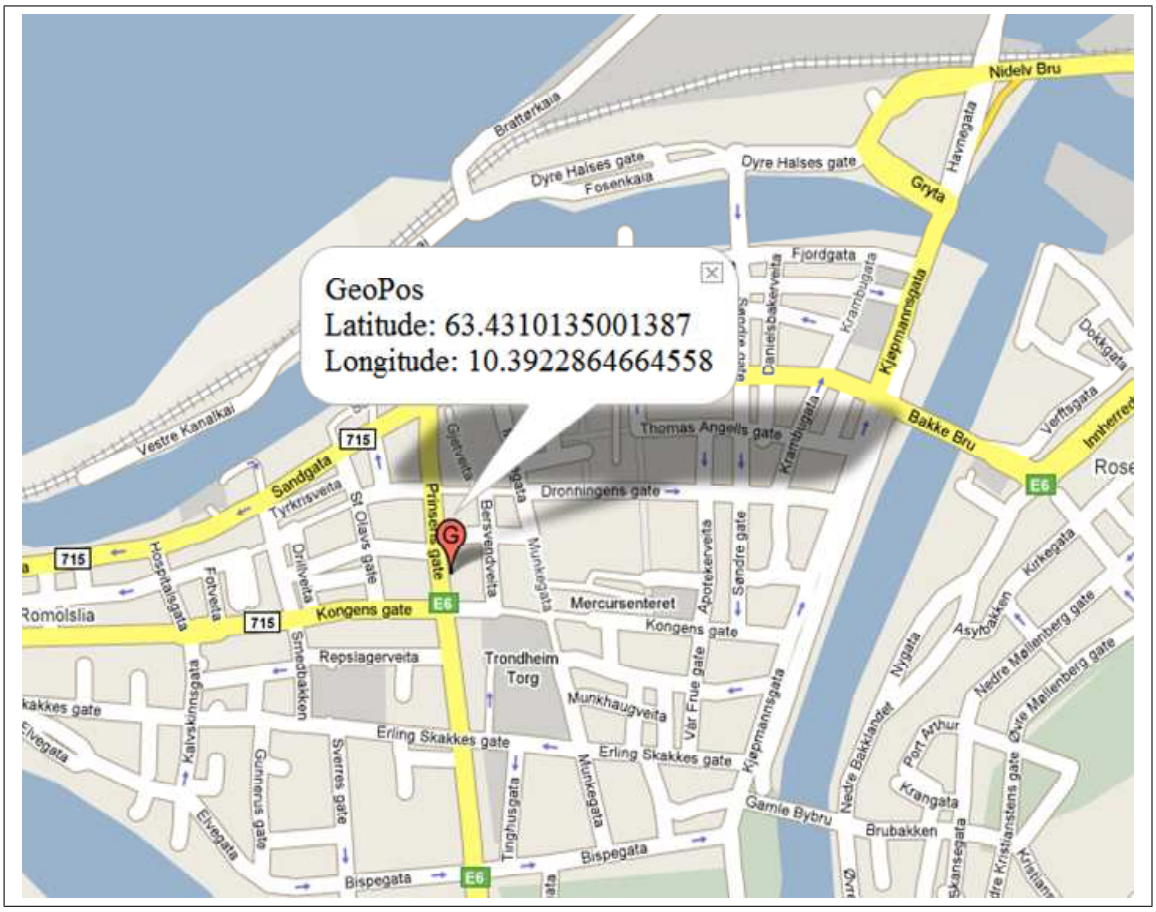
Figur 7.2: Klassediagram for klientsiden. Gule bokser er egne bibliotek, kalt solutions i C#, mens de lyseblå boksene representerer klasser. Programboksen er der programmet starter. GPS-biblioteket inneholder flere klasser som vi har valgt å ikke illustrere i figuren. Dette biblioteket er et omfattende ferdigbibliotek fra en annen kilde, og vi har derfor bare inkludert de klassene vi har direkte kontakt med.

Klassediagram for serversiden (nødsentral/PSAP)



Figur 7.3: Klassediagram for serversiden. Gule bokser er egne bibliotek, kalt solutions i C#, mens de lyseblå boksene representerer klasser. De rosa boksene er ikke klassen, men strukturer som representerer hvordan en SIP-melding og en SOS-melding skal se ut. Programboksen er der programmet starter.

E: Skjermbilde av serversidens kartapplikasjon



Figur 7.4: Skjermbilde av serversideapplikasjonens kartfunksjonalitet ved innkommende nødanrop. Man ser koordinatene og lokasjonskilden som er benyttet.

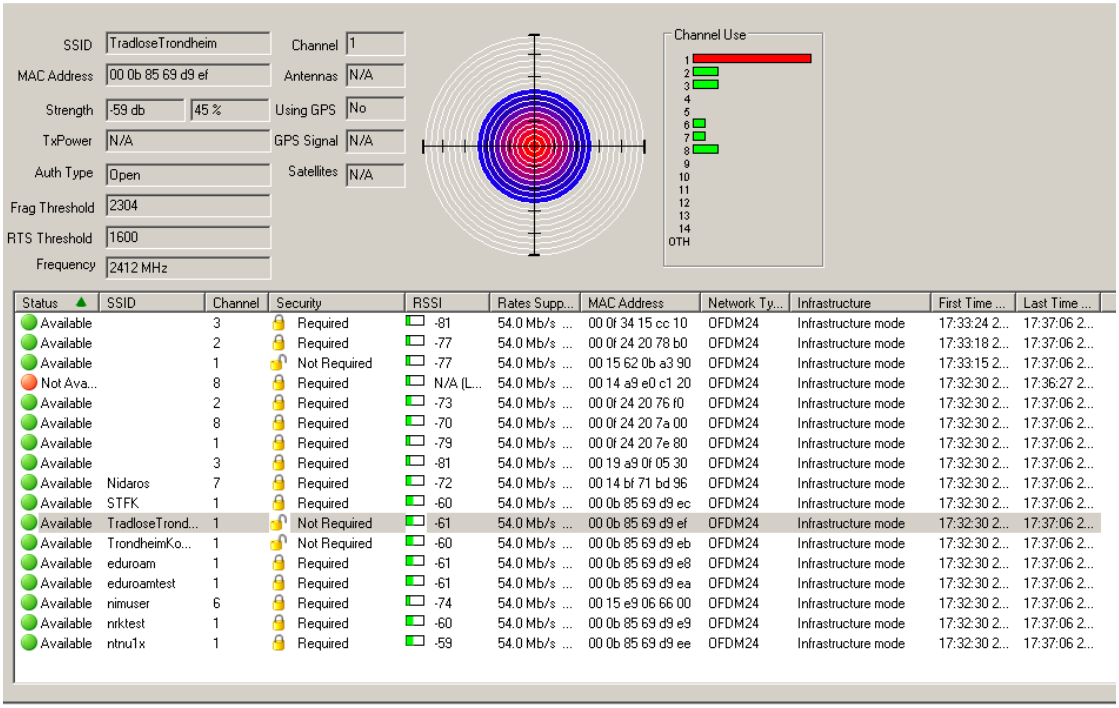
F: Målinger i Trådløse Trondheim

Forklaring

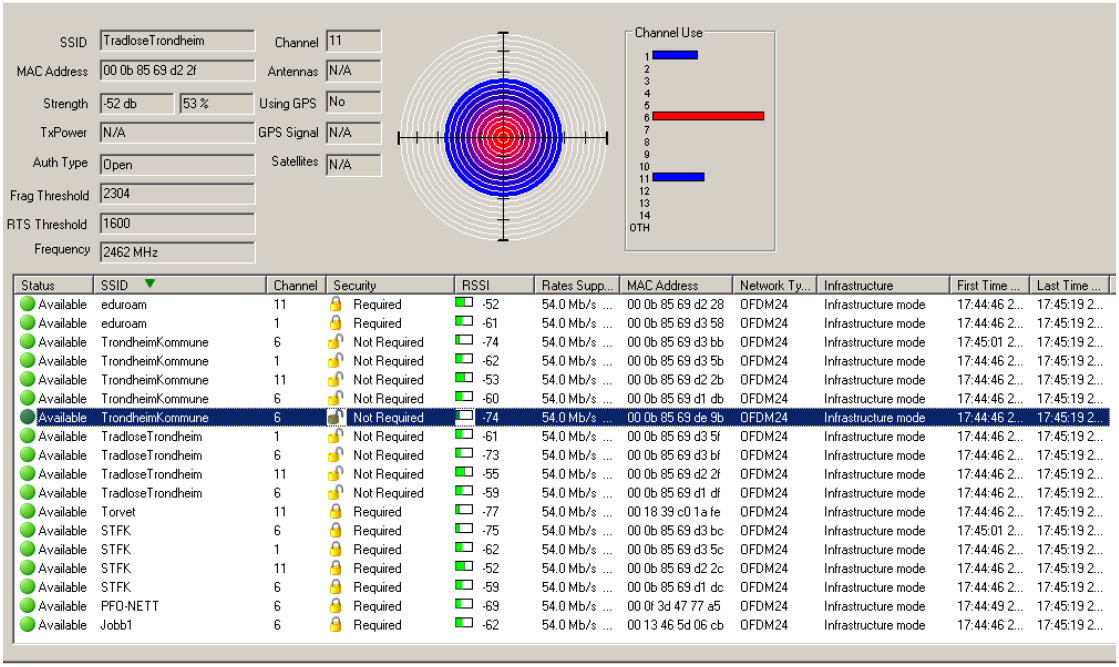
- Målinger av antall aksesspunkt med SSID lik "Tradlose Trondheim" ved en gitt lokasjon.
- Målinger av akesesspunktenes signalstyrke.

Verktøy

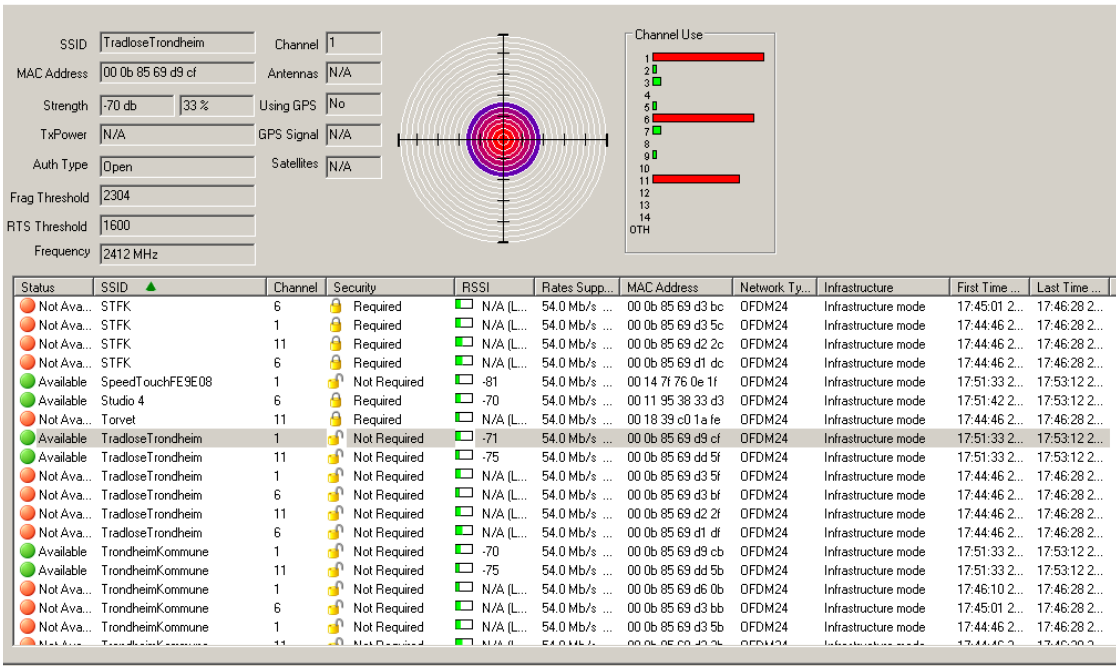
- Programvare: PassMark WirelessMon v2.0
- Maskinvare: Intel(R) PRO/Wireless 2200BG Network Connection



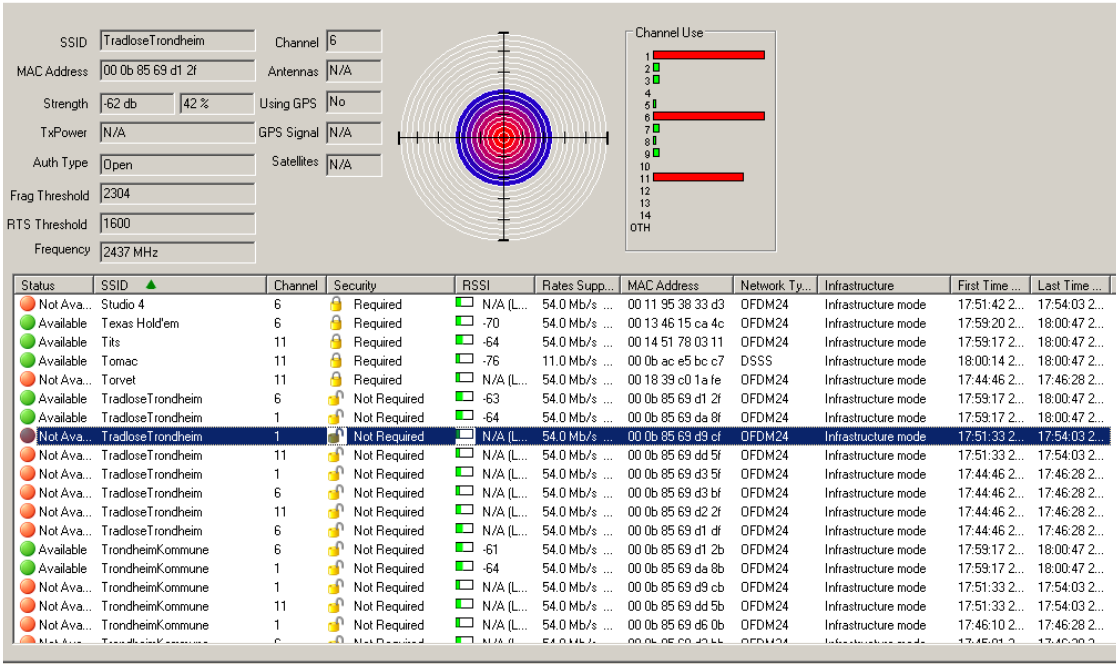
Figur 7.5: Trondheim Katedralskole (videregående skole) - 1 aksesspunkt og 45% signalstyrke



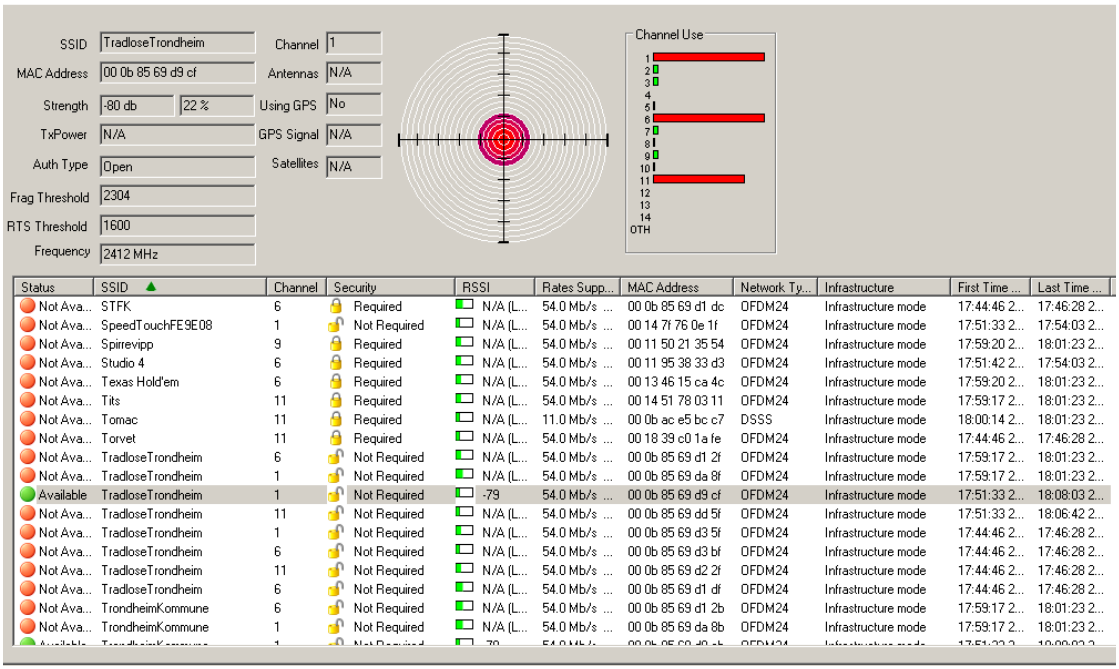
Figur 7.6: Trondheim torg - 4 aksesspunkt og 53% signalstyrke



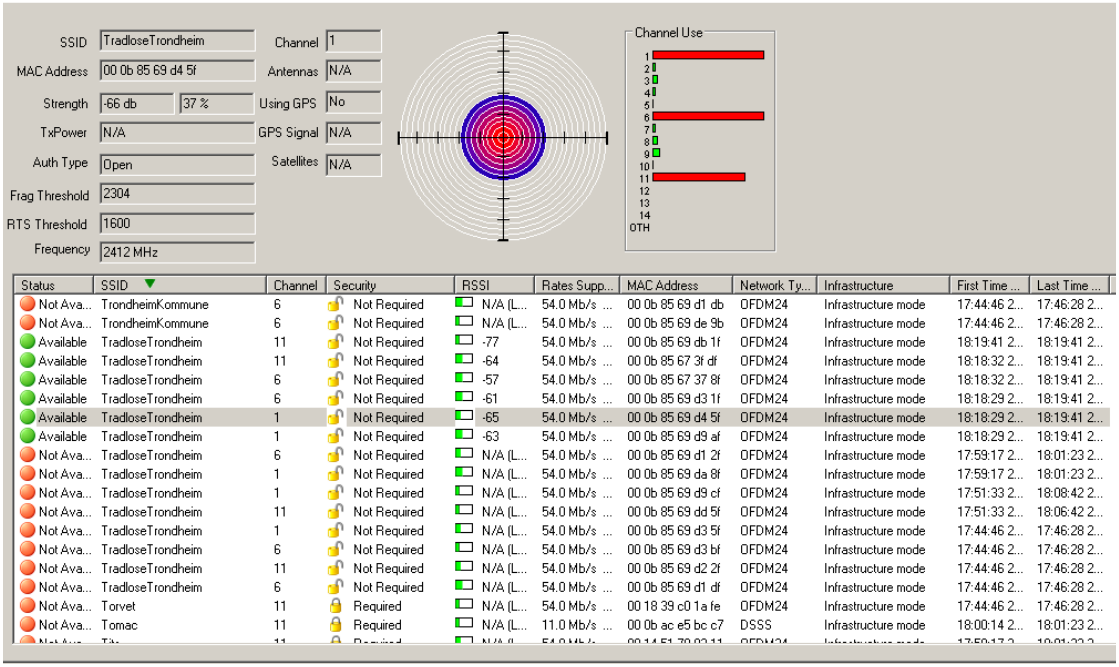
Figur 7.7: Kjøpmannsgata 54, Peppes Pizza - 2 aksesspunkt og 33% signalstyrke



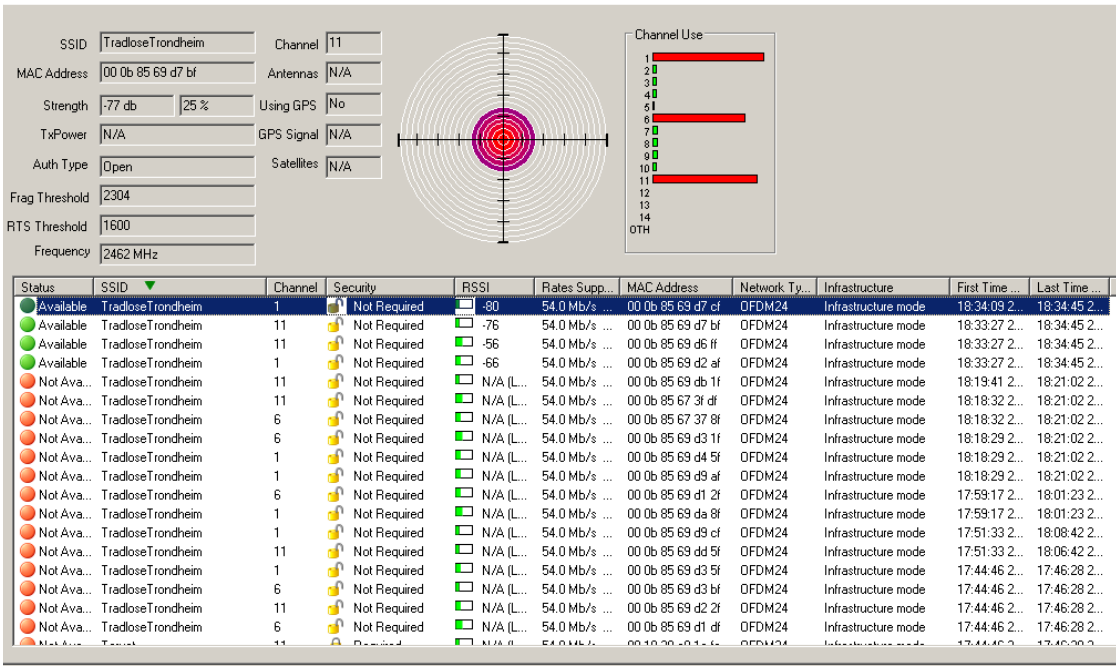
Figur 7.8: Nedre Bakklandet 3, Dromedar Kaffebar - 2 aksesspunkt og 42% signalstyrke



Figur 7.9: Nygata 12 (innendørs) - 1 aksesspunkt og 22% signalstyrke



Figur 7.10: Solsiden, Choco Boco - 6 aksesspunkt og 37% signalstyrke



Figur 7.11: Fjordgata 68, KPMG - 4 aksesspunkt og 25% signalstyrke