FFI-RAPPORT

16/01643

Nettverksarkitektur for heterogene mobile taktiske kommunikasjonsnettverk

–

Lars Landmark
Erlend Larsen
Mariann Hauge
Øivind Kure

Nettverksarkitektur for heterogene mobile taktiske kommunikasjonsnettverk

Lars Landmark
Erlend Larsen
Mariann Hauge
Øivind Kure

Forsvarets forskningsinstitutt (FFI) 15. desember 2016

Emneord
Kommunikasjonsnettverk
Mobilkommunikasjon
Radiokommunikasjon

FFI-rapport
FFI-RAPPORT 16/01643

Prosjektnummer
1249

ISBN
P: 978-82-464-2806-2
E: 978-82-464-2807-9

Godkjent av
Jan Erik Voldhaug, *forskningsleder*
Anders Eggen, a*vdelingssjef*

Sammendrag

Fremtidige militære kommunikasjonsnettverk vil trolig i større grad bestå av flere ulike typer radionettverk med ulike egenskaper. Sammenkobling av disse ulike radionettverkene muliggjør bedre utnyttelse og økt robusthet. I senere tid er det foretatt flere initiativ hvor enkeltsystemer slik som Satellite On The Move (SOTM) og Long Term Evolution (LTE) er testet for å gi økt kapasitet til Forsvaret. Disse nettverkene med flere vil være viktige, og vil ha sine fordeler innen hvert sitt enkeltområde i Forsvaret. En konsekvens av slike initiativ er at det i fremtidige operasjoner trolig vil bli mange forskjellige radionettverk for å dekke forskjellige behov. Behov kan være slik som lang rekkevidde, kort tidsforsinkelse, høy kapasitet, og interoperabilitet med andre nasjonale enheter eller nasjoner. Det er derfor ønskelig og viktig at ulike nettverk kan kobles sammen til et felles nettverk. Et sammenkoblet nett som består av forskjellige radioteknologier vil kunne gi tilgjengelighet over avstand, øke den totale tilgjengelige kapasiteten og gjøre kommunikasjonen mer robust mot både vanskelig terreng og jammeforsøk.

Prosjektet «Nettverksarkitektur for heterogene mobile taktiske nettverk» har utarbeidet en metode som møter utfordringene ved sammenkobling av militære radionettverk. Forsvaret har, og vil også i fremtiden operere radionettverk med store ulikheter. Eksempler på ulikhet kan være forskjell i datarate fra noen få kilobits per sekund (kbps) til gigabit per sekund (Gbps) eller rekkeviddeforskjeller fra noen få hundre meter til titalls kilometer. En utfordring er å få til riktig avveiing mellom signaleringstrafikken som må gå i disse nettverkene for å opprettholde riktig bilde av topologien til nettverket, og gjenværende kapasitet til radioteknologiene i det sammenkoblede nettverket. Et viktig krav til metoden prosjektet har utarbeidet var at radionettverk med lav kapasitet også skulle kunne være en del av det sammenkoplede felles nettverket, da disse i dag er en av de viktigste radioteknologiene for landstyrker. Radionettverk med lav kapasitet har lang rekkevidde og vil i mange sammenhenger bli brukt som bindeledd mellom nettverk med høyere kapasitet. Et annet krav til metoden var å støtte styring av datatrafikken i nettverket med hensyn på tilgjengelig kapasitet og kvalitet på de forskjellige veiene gjennom nettverket (traffic management). Det er også lagt vekt på muligheten for styring av trafikk basert på operasjonelle behov. Metoden støtter mulighet for å kunne omprioritere bruken av nettverket underveis i en operasjon.

Denne rapporten gir en overordnet beskrivelse av fordelene Forsvaret vil ha av å sammenkoble nettverk. Med sammenkoblede nett vil Forsvaret imøtekomme fremtidige behov for robust samhandling over mobile nettverk. Vi skisserer et rammeverk for en søketeknikk som kan skreddersys til å finne veier i nettverket basert på operasjonelle behov og dataflytens krav til tjenestekvalitet. Metoden har en viktig egenskap i å kunne styre mye av signaleringstrafikken vekk fra nettverk med lav kapasitet og tillater dermed at disse nettverkene kan være en del av det sammenkoblede nettverket.

Summary

Future military communication networks will probably consist of several different types of radio networks with different properties. By linking various radio networks, we will enable better utilization and increase the network robustness. More recently, there have been several initiatives in which individual systems, such as Satellite On The Move (SOTM) and Long Term Evolution (LTE), have been tested, in order to provide increased capacity. The individual networks will be important and have their advantages in their individual areas. One consequence of these initiatives is that future military operations are likely to consist of many different radio networks in order to meet the different needs. Different needs can be long range, short latency, high capacity, and interoperability with other national units or nations. It is therefore desirable and important that different networks can be connected to form a common network. An interconnected network consisting of different radio technologies will be able to provide availability across distance, increasing the total available capacity and enable robust communications against both difficult terrain and jamming attempts.

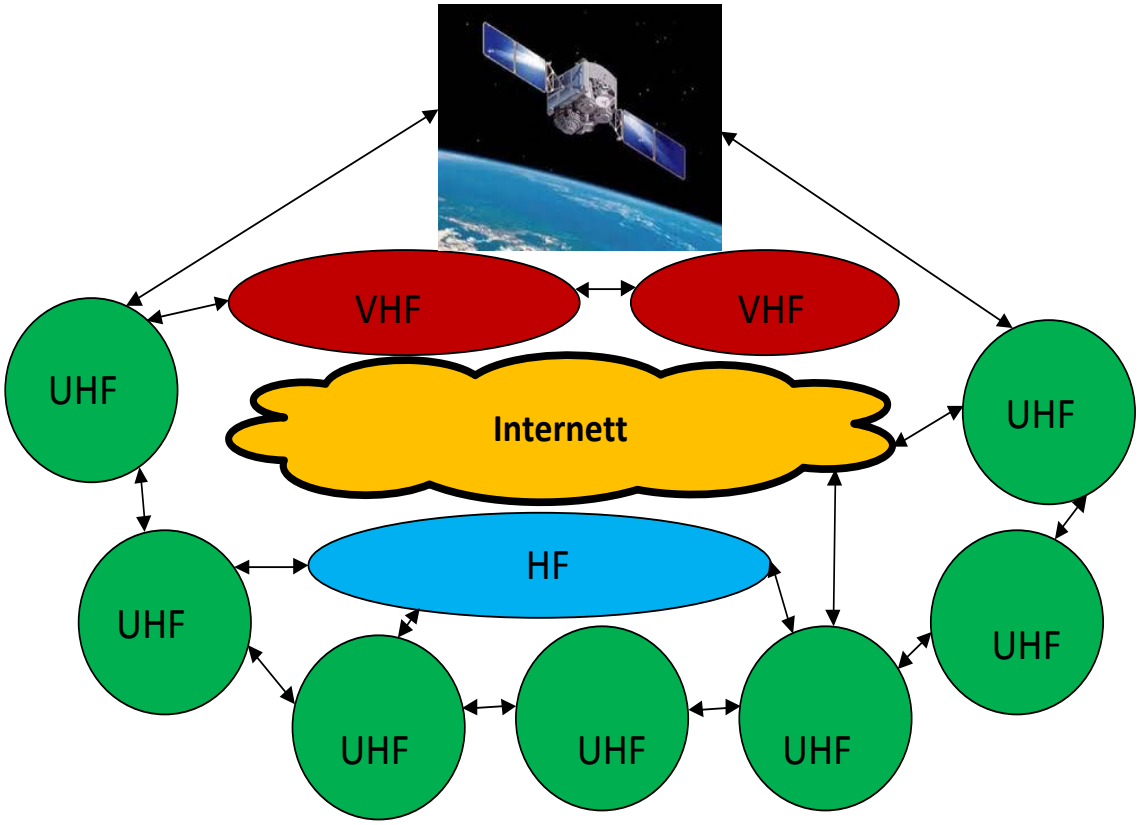
Within the project «Nettverksarkitektur for heterogene mobile taktiske nettverk» a method has been developed that meets the challenges of linking military radio networks. Present and future military communication radio networks will operate radios with disparities, both in terms of mobility and data rate. The inequality may consist of differences in data rate from a few kilobits per second (kbps) to gigabit per second (Gbps) or differences in range from a few hundred meters to tenths of kilometers. A major challenge is the tradeoff between the amount of signaling traffic required to maintain an accurate picture of the network topology, and the remaining available capacity of the different radio technologies in the interconnected network. An important requirement of this project has been to include low capacity radio networks in the common network, since they are one of the main radio technologies for land forces and will often act as a bridging point between networks with higher capacities. Another requirement was to support the ability to select traffic paths depending on application requirements and available network capacity (traffic management). The possibility of controlling traffic based on operational needs was also emphasized. The method supports the ability to re-prioritize the use of the network resources during an operation, and block and filter traffic based on network policing.

This report provides a general description of the benefits that the Norwegian defense can have by interconnecting networks to meet future needs for robust interactions over mobile networks. It outlines a search technique that can be tailored to find network routes based on the requirements of the military operation and its data applications. The method is able to offload signaling traffic from very low capacity networks and can thus allow these networks to be part of the interconnected network.

Innhold

1 Innledning

Bredbåndsradioer blir viktige i Forsvarets mobile taktiske nett som en del av oppgradering av nye kampvogner (Kampvognprosjektet)[21]. Det er også andre initiativ for å gi mobile styrker høyere datakapasitet. FFI har blant annet gjort studier på og eksperimentert med bruk av mobil satellittkommunikasjon (Satellite On The Move (SOTM)) [1], som har fått mye interesse i Forsvaret. Studier på sivile teknologier, for eksempel på mobilkommunikasjonsteknologien Long Term Evolution (LTE) i mobile og deployerte militære nettverk, er også noe som blir diskutert i Forsvaret. Interessen for å løfte nettverkselementer opp i luften er også en trend som trolig kommer til å få mer fokus fremover.



Figur 1.1 Nettverk av nettverk. Dette arbeidet ser på hvordan kommunikasjonsnettverk med ulik teknologi kan kobles sammen og problemområder knyttet til dette. Det er lagt spesielt vekt på inkludering av radionettverk med lav datarate og trafikkstyring.

I tillegg til disse bredbåndsinitiativene vil det fortsatt være utstrakt bruk av radioer med lav datarate, slik som Multi-Rolle Radio eller NATO Narrowband Waveform (NBWF(STANAG 5630-5633)). En viktig faktor for disse radiosystemene er rekkevidde. Radiosystemer med lav datarate gir normalt lengre rekkevidde og er på denne måten en viktig komponent for tilgjengelighet. Kommunikasjon på HF-radio er også forventet å ha en rolle i uoverskuelig

fremtid. Konsekvensen av alle disse initiativene er at det blir mange forskjellige radionettverk med varierende ytelse i en operasjon. Det er ønskelig og viktig at disse nettverkene kan kobles sammen. Sammenkoblede nett vil kunne øke den totale tilgjengelige kapasiteten og gjøre kommunikasjonen mer robust.

Behovet for gjennomgående kommunikasjon i Forsvaret vil trolig øke i fremtiden. Flere av Forsvarets tjenester og plattformer vil dra nytte av økt informasjonsdeling. FISBasis Taktisk med sine tjenester er et eksempel på en slik plattform med behov for kommunikasjonsnettverk. Fremtidige mobile plattformer med kun lav-datarate kommunikasjonslinjer vil ha sensorer. Ser vi dette i sammenheng med nettverksbasert forsvar (NbF), så viser det vei for at man må kunne legge til rette for gjennomgående kommunikasjon i hele nettverksstrukturen, fra mobile nett via deployerte nett til stasjonære nett. Arbeid for å få til god utveksling av etterretning og overvåking (Joint Intelligence, Surveillance and Reconnaissance (JISR)) vil også sette store krav til gjennomgående fleksibel kommunikasjon helt ut til mobile plattformer.

Kommunikasjonsnettverkene som binder bredbåndsnettene sammen, vil i varierende grad støtte høykapasitetsoverføringer. Fremtidige militære nett vil dra fordel av å kunne knyttes sammen uavhengig av nettegenskaper. Det blir dermed et økt behov for å styre nettverkstrafikken, både tale og data, slik at man kan sikre nødvendig tjenestekvalitet og at nettverkene ikke utsettes for høyere trafikkbelastning enn de kan tåle. Slik styring vil også kunne prioritere stridskritisk trafikk framfor mindre kritisk trafikk.

I FFI-prosjektet *Nettverksarkitektur for heterogene mobile taktiske nettverk* har vi designet og bygd en ruteprotokolldemonstrator som kan koble sammen ulike radionettverk. Det er tatt spesielt hensyn til å inkludere radionett med lav datarate. Demonstratoren er godt studert i nettverkssimulator og testet i en enkel testbed for å vise konseptet. Løsningen tillater styring av trafikk med hensyn på et regelsett som definerer nettverksbruken.

Arbeidet har vært delt i tre oppgaver:

- Første del har sett nærmere på hvordan man kan koble samme nettverkene i en operasjon på IP-nivå samtidig som lavkapasitetsnettverk/-linker blir beskyttet mot kontrolltrafikk.

- Andre del har tatt for seg regelsettet for styring av datatrafikken i nettverket. Her er det lagt inn metoder for enkelt å styre hvilke data som får lov til å bruke hvilke nettverksressurser og til hvilket tidspunkt.

- Tredje del har rettet seg mot å gi datastrømmer etterspurt tjenestekvalitet (QoS).

Designet gir frihet til å styre trafikk på mange måter. Styrken ved designet ligger i kombinasjonen av et skille mellom operatør og etterspurt ressurs som ligner på Integrated Service (IntServ) [2], og at vi i tillegg søker nettet etter ledig ressurs. Søk etter nettverksressurser kan bero på behov for datarate eller for eksempel ende til ende tidsforsinkelse. Andre behov kan være bruk av foretrukne radionettverk, eller motsatt,

radionettverk som ikke kan brukes basert på tillit eller operasjonelle behov/krav. Styrken i vårt design er mulighet for tilpasset søk.

Resten av rapporten er organisert som følger: Kapittel 2 gir en innføring i bakgrunnen for hvilke problemer som er adressert og relatert arbeid. Kapittel 3 gir en oversikt over metoden som er valgt for å koble sammen nettverk med ulike egenskaper. Kapittel 4 beskriver oppsettet av test hvor vi har brukt software-rutere og militære bredbåndsradioer. Siste kapittel oppsummerer arbeidet.

2 Bakgrunn

Dette kapittelet beskriver motivasjon, bakgrunn og relaterte løsninger for hvordan nettverk med ulike egenskaper kan knyttes sammen.

I første delkapittel introduserer vi utfordringer ved sammenkobling av ulike radionettverk. Forskjellen mellom ulike typer radionettverk ligger i datarate og rekkevidde. Løsninger for disse problemene er implementert og testet i vårt forslag. I delkapittel 2.2 ser vi på fordeler ved å koble sammen ulike radionettverk. I delkapittel 2.3 ser vi på teknologier som eksisterer i dag og problemene med å sammenkoble mobile heterogene radionettverk.

2.1 Utfordringer med å koble sammen mobile heterogene radionettverk

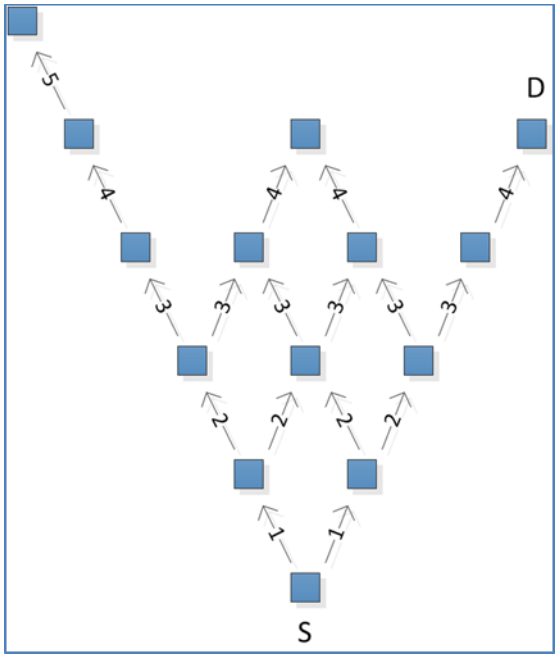
I dag er metoden for å etablere et datanettverk i all hovedsak basert på proaktive ruteprotokoller. Det vil si at signaleringspakker blir regelmessig sendt mellom rutere for å finne nye rutere og deres linker, og for å oppdage brudd på etablerte linkforbindelser. For at alle rutere i et nettverk skal kunne opprette nettverksforbindelser, må de ha en felles sanntids oversikt over tilgjengelige linker mellom kommuniserende enheter (nettverkstopologi). Dette fungerer bra for faste installasjoner og nettverk hvor det er lite endringer.

Ved sammenkobling av ulike linkkvaliteter (datarate og eller rekkevidde) øker sannsynligheten for ulik topologiforståelse, med økt forekomst av ugyldige ruter som resultat. Brukeren opplever dette som et brudd i nettverksforbindelsen. I [3] ble noder utstyrt med en eller to radioer. Egenskapene til radioene i [3] var ulike i form av rekkevidde og datarate. Radioen med høy datarate hadde kort rekkevidde, mens radioen med lav datarate hadde lang rekkevidde. Studiet viste at signaleringspakkene i heterogene nett propagerer med ulik tidsforsinkelse, som igjen fører til ulikt syn på nettverkstopologien. Ulikt syn på topologi fører til at en ruter med økt sannsynlighet kalkulerer ulike stier, med ruteloop som resultat. Teknikker for avverging og håndtering av ruteloops ble videre analysert i [4].

En annen metode som ofte blir brukt for etablering av ruter i trådløse nett, er reaktiv ruting med bruk av breddesøk etter en rute (se figur 2.1). Reaktiv ruting har, i motsetning til proaktiv ruting, ingen rute tilgjengelig før det er et behov. Denne metoden sender ingen regelmessig kontrolltrafikk for å ha et tidsriktig bilde av nettet. Søk etter en rute starter når en ruter får en pakke med ukjent rute. Fordelen med breddesøk er at den ikke belaster nettet unødig med signaleringstrafikk ved lav trafikk, men viktigst er at den har et tidsriktig bilde av nettet, ettersom rutene etableres ved behov.

En ruter som har trafikk å sende, vil starte et søk etter rute til mottakeren. En søkepakke blir sendt ut til alle naboer fra kilde. Hver nabo sender igjen til alle sine naboer. Mottakeren vil så sende svar tilbake til søker langs ruten som søkepakken brukte. En rute i begge retninger etableres gjennom nettet, basert på korteste vei, eller ifølge annet krav til oppsett av rute, som for eksempel datarate. Problemet med denne metoden er at alle nett/linker belastes for alle søk.

Lavkapasitetsnett vil måtte prosessere alle søkepakker og dermed legge unødig beslag på ressurser i nettet. Studie utført i [5] så på metoder for kommunikasjon i et nett med ulike radioegenskaper ved bruk av breddesøk. Metoden som viste seg best egnet, var å forsinke signaleringstrafikk basert på radioegenskaper og trafikkbelastning.



Figur 2.1 Bredde først-søk. Tallene indikerer transmisjonsrekkefølge.

Mobile og deployerte nettverk i militær sammenheng har kapasitet fra kbps til Gbps. Lavkapasitets-radionettverk bruker tradisjonelt lave frekvenser, mens høykapasitetsnettverk bruker høyere frekvenser. Lave frekvenser har lengre rekkevidde enn høyere frekvenser ved samme utgangseffekt. Som tommelfingerregel er det et inverst forhold mellom rekkevidde og datarate. Lang rekkevidde gir lav datarate og omvendt.

Ulike nett har forskjellige endringsrater for nettverkstopologien og krever dermed ulike oppdateringsfrekvenser på signaleringspakker basert på radio rekkevidde og mobilitet. Ved lik mobilitet vil høykapasitetsnett typisk ha lavere linklevetid enn lavkapasitetsnett og dermed gjøre krav på høyere signaleringstrafikk. Topologiendringer i høykapasitetsnett må derfor både aggregeres og forsinkes i tid for å kunne spres over nett med lavere kapasiteter. I tilfeller med stor endringsrate og mange linker, vil lavkapasitetsnettverk ha redusert kapasitet til å bringe informasjon om endringer/variasjoner i andre nett.

2.2 Fordeler med heterogene kommunikasjonsnettverk

Radionettverk med ulike egenskaper blir ofte referert til som heterogene kommunikasjonsnettverk. Ulike egenskaper kan dekke områder som, men ikke begrenset til, protokoller, teknologi eller frekvenser som gir ulik radiooppførsel. I vårt arbeid har vi definert et heterogent nettverk som et nettverk bestående av ulike mindre radionettverk som har ulike radioegenskaper. Ulikheten ligger i, men er ikke begrenset, til ulik rekkevidde og datarate. Metoden vår kan brukes ned på linknivå internt i et nettverk, eller for sammenknytting av større nettverk. Hovedbruksområdet er hvor noen linker/nettverk ikke tillater regelmessig eller stor signaleringstrafikk.

En radioteknologi og dens nettverksfunksjonalitet er ofte anskaffet for en spesifikk oppgave. Fordelen med å bruke dedikerte radionettverk til en spesifikk oppgave er forutsigbarheten, det være seg tilgjengelig kapasitet, oppførsel med mere. Den største svakheten er kostnad og robusthet sett i sammenheng med utnyttelsesgraden. Mange radiosystemer er bygget med robusthet for å kunne motstå jamming og ha alternative veier hvis en link går ned. Derimot, hvis nettverket blir jammet, så vil kommunikasjonen i dette nettet stoppe opp. Ulik radioteknologi kan utsette kommunikasjons brudd, eller i mange tilfeller opprettholde kommunikasjon. Tilgjengelighet til flere ulike radionettverk vil øke robustheten når eksterne hendelser slik som for eksempel jamming eller ugunstig topografi fører til at primærnettverket ikke kan brukes. Fordelene med å koble sammen forskjellige radioteknologier til et felles heterogent nett er således bedre utnyttelse av tilgjengelig kapasitet og mer robust kommunikasjon, siden vi har flere alternativer veier.

Når mobile nettverk blir koblet sammen for å oppnå bedre utnyttelse av ressurser og mer robust kommunikasjon, er det viktig å sikre at dette skjer på en slik måte at nødvendig kvalitet på primærtjenesten eller oppgaven som nettverket skal støtte, blir opprettholdt. Anskaffet netteknologi er i mange tilfeller tilpasset tjenestens spesielle behov, slik som krav til forsinkelse, variasjon i forsinkelse («jitter») og tilgjengelig ressurser. Ved å knytte sammen nett vil det være viktig å sørge for at de allerede anskaffede kommunikasjonsnettverk med sine tjenester får tilgang til sin ressurs ved normal bruk. Når det er sagt, vil spesielle hendelser under en operasjon kunne føre til behov for omprioritert bruk av nettverksressursen. I et felles heterogent nett vil dette være fullt mulig.

Ulike nett har forskjellige metoder for oppbygning av ruter og trafikkstyring. Ofte er den valgte metoden i et produkt optimalisert for den tiltenkte oppgaven (trafikkmønster) og for radioomgivelsene. En felles metode for rute- og trafikkstyring for alle nettverk med ulike omgivelser og trafikkmønstre vil således redusere fleksibiliteten og i mange tilfeller ytelsen. Det vil derfor være fordelaktig om sammenkobling av ulike nett ikke krever endring i trafikkstyring innad i hvert nett, men at hvert nett bevarer sin optimaliserte trafikkhåndtering.

Utfra de nevnte utfordringene ble det i prosjektet utformet et grunnleggende design for hvordan koble sammen ulike radionettverk. Designet er laget for å løse utfordringer identifisert i eget tidligere arbeid ved sammenkoblinger av linker/nettverk av ulik kapasiteter (ruteloop [3][4],

CoNSIS [6][7] og breddesøk [5]) og kjente utfordringer fra annen internasjonal forskning (for eksempel BGP problemer nevnt i [10]). Løsningen ble basert på dybdesøk med hint (en beskrivelse av metoden er gitt i kapittel 3). Metoden er basert på arbeid med å koble nett sammen i det faste Internett [10]. Metoden bygger på ideen om at autonome nett på Internett etablerer en eller flere pathlet(s). Oppgaven til en pathlet er å annonsere egenskapen og policy regler til det autonome nettet. Pathleten blir deretter annonsert til alle autonome nett på Internett. Resultatet er at alle kantrutere i et autonomt system selv kan bestemme hvilke autonome nett kilden vil bruke for å nå en bestemt destinasjon. I motsetning til vårt arbeid blir pathlet-informasjon distribuert ut til alle autonome nettverk. I vårt arbeid blir denne informasjonen ikke delt, derav oppnår vi en sterk reduksjon i signalering. Siden vi ikke har full oversikt over hele nettet til enhver tid, bruker vi ikke source-based ruting. Source-based ruting innebærer at hver datapakke innehar stien den skal gå, det vil si hvilke autonome nett den skal bruke for å nå sin destinasjon.

2.3 Relatert arbeid for sammenkobling av ulike radionettverk

I dag brukes Border Gateway Protocol (BGP) [9] for sammenkobling av nett på Internett. BGP gjør bruk av to metoder som bestemmer utveksling av informasjon: Internal BGP (iBGP) og External BGP (eBGP) for kommunikasjon med interne og eksterne nettverk. Det er flere kjente problemstillinger med BGP som gjør denne protokollen uegnet for sammenknytning av forskjellige mobile nettverk. iBGP-noder trenger å kommunisere seg i mellom i full mesh (alle til alle) for å unngå rutelooper. Denne metoden krever høy signalering i dynamiske miljøer. I [10] ble det påpekt at BGP har problemer med å etablere flere veier mot en destinasjon samtidig som den skal tilfredsstille policy satt av hvert enkelt nett. Multiple veier med bruk av policy for trafikkstyring er en av de store fordelene med sammenkobling av ulike trådløse nett. I [11][12] ble problemene rundt mobilitet og BGP vist. BGP er en distance vector protokol, som er kjent for å ha problemer med konvergeringstid. Med konvergeringstid menes tiden det tar før alle deler det samme bildet av kommunikasjonsnettverket.

BGP er designet for sammenkobling av autonome systemer. Den støtter et utstrakt regelsett eller policy for trafikkstyring mellom autonome systemer eller mellom sub-autonome systemer. BGP har imidlertid redusert eller ingen støtte for policy per flyt, i form av datastrøm mellom to applikasjoner, som trolig vil være et økende behov i fremtidige militære kommunikasjonsnettverk.

Sammenkobling av nett med ulike egenskaper er blitt utprøvd i det internasjonale samarbeidsprosjektet Coalition Network for Secure Information Sharing (CoNSIS) [6][7], der FFI var en av partnerne. I CoNSIS ble fire forskjellige mobile nettverk fra to forskjellige nasjoner koblet sammen. Metoden for sammenkobling var basert på proaktiv ruting ved hjelp av multitopologi OSPF (MT-OSPF) [8]. MT-OSPF er en kjent metode og noe støttet i nettverksutstyr levert av de store ruterleverandørene. Løsningen har mange gode egenskaper og er godt egnet i heterogene nettverk som ikke har nettverkssegment med smalbåndsradioer med

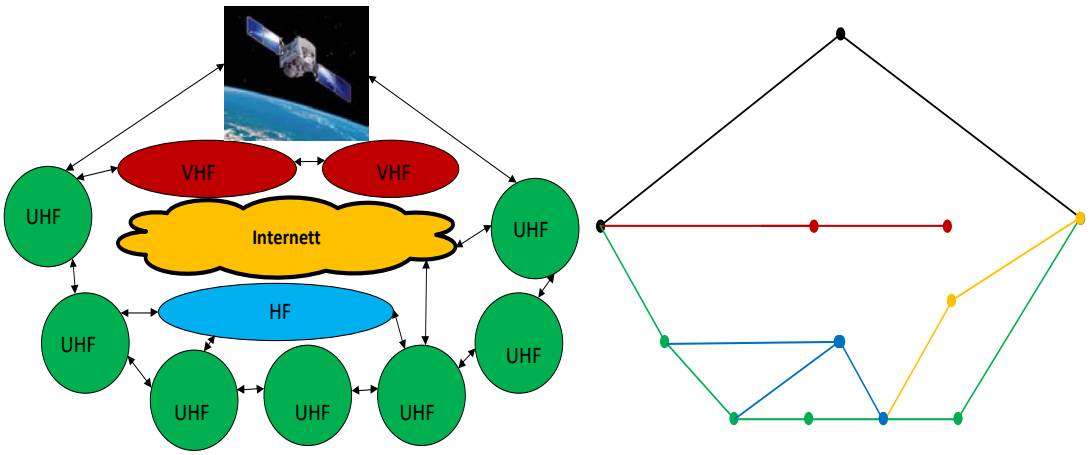
liten kapasitet. Ved sammenkobling av mange radionett, inkludering av lavkapasitetsnett eller økt mobilitet vil problemstillingen som nevnt i [3][4] oppstå grunnet bruk av proaktiv ruting.

3 Beskrivelse av ruteprotokollen

I dette kapittelet beskriver vi en metode for hvordan ulike nettverk kan kobles sammen og for styring av datatrafikk mellom radionettverkene. I delkapittel 3.1 gir vi en overordnet introduksjon til designet bak metoden, mens vi i delkapittel 3.2 går mer i detalj når det gjelder meldingsutveksling for metoden. I delkapittel 3.3 beskriver vi hvordan ruteinformasjon utveksles med hensyn på redusert signalering. Delkapittel 3.4 tar for seg hvordan datatrafikk blir styrt ved hjelp av regelsett eller policy. I siste delkapittel ser vi på hvordan tjenestekvalitet er løst i et kommunikasjonsnett bestående av mange, men ulike radionettverk.

3.1 Design av sammenkobling av ulike radionettverk

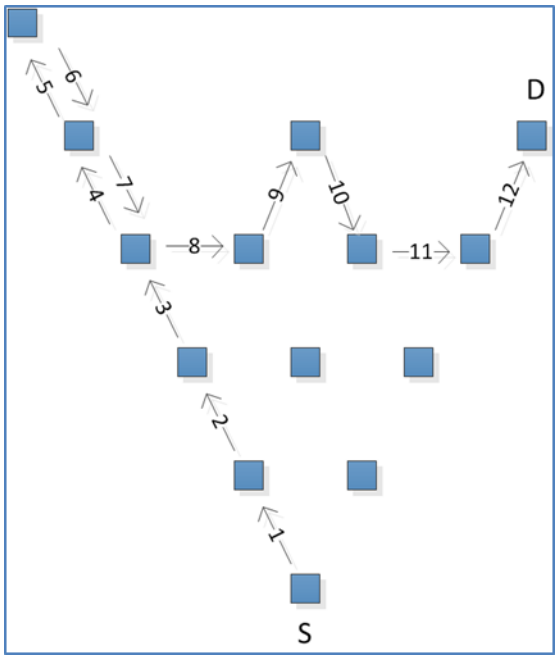
Prosjektet har utviklet en ruteprotokoll som har fått navnet «Depth-First Search Protocol» (DFSP). Metoden vil søke etter destinasjon over ett eller flere nettverk med ulik egenskaper (se figur 3.1). Prinsippet for søk etter en destinasjon er *dybde først*. Det betyr at den sender et søk én vei og forsøker å komme frem til destinasjonen langs denne veien. Dersom den kommer til en node som ikke har nye veier å søke over, går den tilbake til forrige node og søker videre derfra. Hver node tar beslutning om hvilken vei søket skal gå, enten basert på tidligere erfaring/hint som har til hensikt å redusere søketiden/signaleringen, gitte preferanser for neste hopp, eller bare tilfeldighet.



Figur 3.1 Nettverk av ulike radionettverk og tilhørende virtuelle linknettverk hvor søk etter destinasjon kan forekomme.

Rapporten fokuserer på dybde først-søking etter destinasjon. Det kan derfor være oppklarende å forklare dybde først-søk. I figur 2.1 ble bredde først-søk forklart. Kjennetegnet til breddesøk er at en kilde sender søkepakker over alle grensesnitt samtidig. Hver ruter som mottar søkepakker som ikke er destinasjon eller kjenner en rute til destinasjon, vil videresendes på samme måte. Prosessen gjentas gjennom hele nettverket. Med mindre man har lagt begrensninger på antall videresendinger i form av for eksempel ring search, vil søkepakkene bevege seg over alle grensesnitt i hele nettverket. Metoden vil derfor legge beslag på mye ressurser over radionettverk med lav datarate.

For å unngå å sende søkepakker over alle radionettverk har vi i denne løsningen valgt å søke sekvensielt gjennom nett ved hjelp av dybde først-søk (se figur 3.2). Et dybde først-søk sendes kun over ett grensesnitt av gangen. Man søker i dybden først, og returnerer nærmere kilden (S) kun når alle andre forsøk er prøvd. Fordelen med dybdesøk er at man kan unngå å belaste hele nettverket for hvert søk.

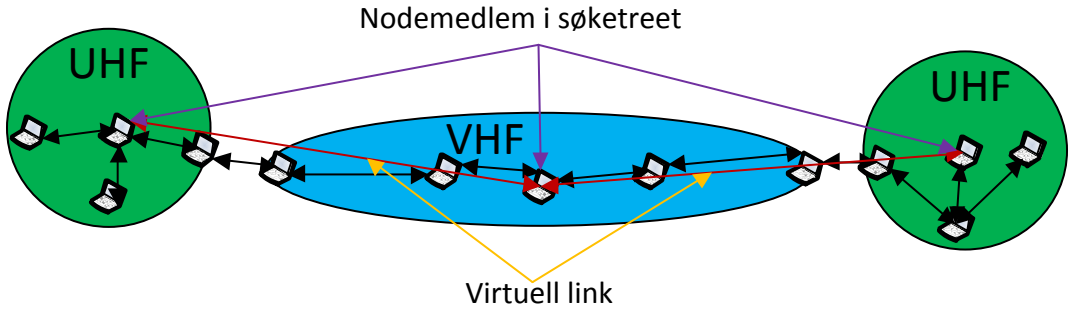


Figur 3.2 Dybde først-søk. Tallene indikerer transmisjonsrekkefølge.

Metoden muliggjør enkel styring av hvilke nettverk et bestemt søk skal tillates å gå over. Et søk kan settes til å prøve ut bestemte teknologier, fordelaktige nettverk eller annet. Et dybdesøk er heller ikke avhengig av at alle rutere i nettverket skal bære samme tidsriktige informasjon om nettverkstopologien slik som i proaktiv ruting. Fordelene med dybdesøk er således redusert signaleringstrafikk samt enkel trafikkstyring.

Ulempen med dybdesøk er forlenget tid for etablering av forbindelser og en risiko for å velge en rute som ikke nødvendigvis er den beste, men god nok. Lengre tid brukes dersom nettverket er stort og søket går i feil retning i forhold til beliggenheten til destinasjonen (D). Den andre

ulempen er at den beste veien ikke nødvendigvis blir funnet, og således legger unødvendig beslag på nettverksressurser. Unødig nettverksressurser benyttes på grunn av for eksempel lengre vei mellom avsender og mottaker. Disse ulempene er en konsekvens av kravet til redusert signalering over radionettverk med lav kapasitet.



Figur 3.3 Nett av nett. En eller flere noder i hvert nett kan være med i det virtuelle søkbare treet.

Hvert nett bygger veier i form av virtuelle linker som benyttes for søk etter destinasjon (figur 3.3). Veiene mellom ruterne blir assosiert med visse egenskaper og regler (policy) for tillatt trafikk. Veien til en naboruter blir IKKE annonsert til andre nett, med mindre noe annet er ønskelig. Det er for å spare på nettverksressurser. Gitt tilstrekkelig ressurser kan veiene likevel annonseres innenfor et begrenset område, eller til hele nettet. Veiene over hvert nett vil på denne måten etablere et virtuelt nettverkslag som brukes for søk etter destinasjon. Kravet for individuelle nett er at hvert nett har minimum én ruter som er deltaker i det virtuelle nettverkslaget. Rutingen innad i hvert nett er ikke endret. Hvert nett bygger således sine egne ruter gjennom sine egne nett.

Plassering av rutere i et nett er ikke bestemt, men har mange frihetsgrader. Det kan være en eller flere rutere i hvert nett basert på behov eller begrensninger. Et eksempel på behov kan være redusert signalering på bekostning av potensielt lengre veier, derav kun én ruter i hvert nett. En annen begrensing kan være plassering av rutere på nettkantene fordi lite eller ingen ruteinformasjon blir delt mellom nettene. For å se begge nettene må trafikk sendes til en ruter med et bein i begge nett.

I vår metode har hver ruter et regelsett eller en policy som dikterer hvordan et søk skal behandles. Et eksempel på en regel kan være at nettverk A ikke er tillatt over nettverket som denne ruteren står i. Resultatet er at et søk med kildeadresse A blir stoppet og returnert til forrige ruter.

Det er ikke gjort krav på at alle i hele nettet skal vite om alle rutere sitt regelsett. Løsningen vil imidlertid finne en vei som imøtekommer en kildes forespurte ressurs samtidig som hver enkelt nettoperatør er gitt full frihet til å sette regelsett som måtte passe. Regelsettet kan endres individuelt, basert på hver enkelt netteiers ønsker. Det er enkelt å endre regelsettet underveis i en operasjon for å tilpasse nettverksbruken til endringer i operasjonen. Løsningen vil derfor

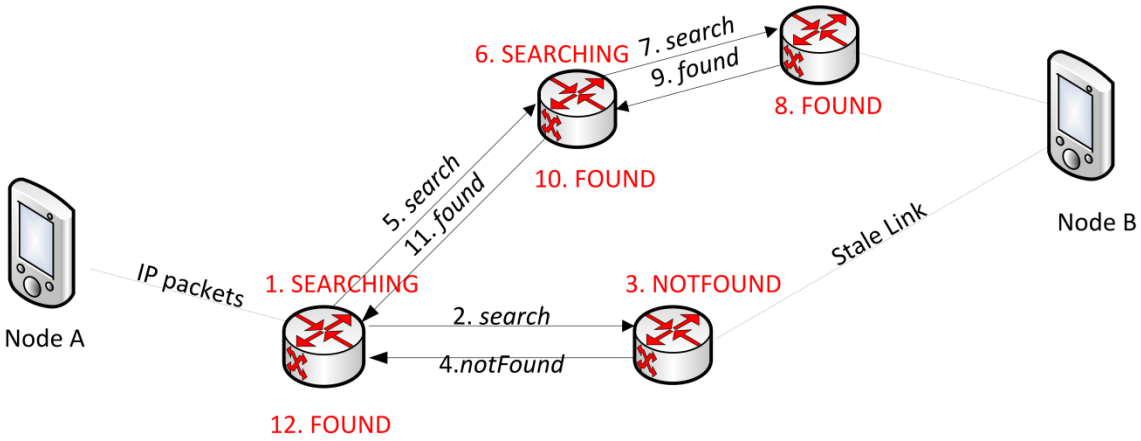
kunne bidra til fleksibel trafikkstyring i Forsvarets mobile og deployerte nett, hvor flere nett er koblet sammen for bedre og, ikke minst, mer robust kommunikasjon.

For å redusere oppkoblingstiden har vi brukt forskjellige hint. Hint er brukt for å hjelpe søket å gå i riktig retning. Hver ruter har en hint-database som bygges opp ved hjelp av informasjon fra tidligere søk og fra annen trafikk som går i nettet. Kildene til hint kan være mange. For eksempel vil det i Forsvarets mobile nettverk ofte gå trafikk for å bygge situasjonsforståelse. Denne type informasjon vil ofte flyte mellom de fleste enheter, og i mange sammenhenger vil den kunne gi verdifull informasjon om nettverkstopologien som kan utnyttes til trafikkstyring.

En annen metode er å bruke underliggende protokollers topologi-informasjon som hint for forbedret søk mot destinasjonen. Hint lages fra trafikk prosessert av en ruter. Et typisk hint vil være et tidligere søk som ikke kom fram til neste hopps-ruter. Det kan være flere årsaker til at den ikke kom frem, for eksempel at trafikktypen ikke var tillatt i nettverket, for lite ressurser, eller at nabonettet er midlertidig stengt for all transitt-trafikk. Uansett grunnen til at søket stoppet, vil det bli sendt tilbake til forrige søkenode. Denne noden vil så søke videre en annen vei. Senere søk vil således dra nytte av erfaringer fra tidligere søk.

Pakker som ankommer en node i det virtuelle nettet, må kunne lagre trafikken inntil en rute er funnet. Noder i autonome nett uten kjent ruteoppslag til en bestemt destinasjon vil derfor sende trafikken til en gateway som er medlem i det virtuelle nettverkslaget. Trafikken blir så lagret temporært i gatewayen. Videre vil det virtuelle nettverket brukes til å søke opp nettverket som har mottakeren i sitt adresserom. Mottakernettverkets gateway vil så sende en melding tilbake til avsendernettverkets gateway om at destinasjonen er funnet. Den lagrede trafikken og påfølgende trafikk kan deretter flyte til mottaker-gatewayen. Ved ankomst ved mottaker-gatewayen vil trafikken bli rutet videre ved hjelp av mottakernettverkets interne ruting.

3.2 Meldingsutveksling i dybde først-søk-protokoll (DFSP)



Figur 3.4 Prosesseringen av dybde først-søk. Node A sender trafikk til node B, hvor nærmeste ruter til node A initierer søk mot node B (1). Søket initieres med søkepakke (2).

Dybdesøk fungerer ved å søke sekvensielt. Figur 3.4 viser hvordan et søk etter node B fra node A foregår. Node A har ingen rute og sender derfor til nærmeste ruter som er medlem i det virtuelle pathlet-nettverket. Denne ruteren initierer et søk etter node B og setter status for søket til SEARCHING (1). En generert søkepakke (SEARCH) sendes ut over et av ruterens nettverksgrensesnitt mot en annen virtuell pathlet-ruter (2). I (3) blir søket mottatt av ruteren, men denne klarer ikke å sende pakken videre til node B grunnet link nede og setter derfor statusen for søket til NOTFOUND, samtidig som en melding blir sendt tilbake med status NOTFOUND (4). Søket har nå returnert til start og prøver seg mot neste nabo (5). Denne noden setter status for søket til SEARCHING (6) og sender søket videre til neste node (7). I (8) ankommer søket til en ruter som har rute til node B og denne setter status til FOUND. FOUND melding sendes så tilbake mot initierende ruter (9). Noden som mottar pakken, endrer status fra SEARCHING til FOUND (10) og sender beskjeden videre til initierende node (11). Initierende node setter søket til FOUND (12) samtidig som lagrede pakker blir sendt mot node B.

3.3 Besøkte noder og utveksling av rutetabeller

I forrige avsnitt ble dybdesøk kort beskrevet. I dette avsnittet vil vi forklare hvordan hint basert på SEARCH-pakker blir utvekslet og bygget. SEARCH-pakker er de som benyttes for søk etter destinasjon, mens NOTFOUND benyttes når en ruter ikke har flere muligheter for søk, og dermed sender beskjed tilbake om at den har gått tom for søkemuligheter. Hver SEARCH-pakke inneholder informasjon fra siste naboruter. Informasjonen som bæres, er hvilke noder som er besøkt i søket og i hvilken rekkefølge. Rutere som da mottar et søk vil dra nytte av denne informasjonen for senere søk. De besøkte nodene er gode kandidater for kommende søk fordi de nylig har samarbeidet om søk.

SEARCH-pakker inneholder rutetabellen til forrige naboruter. Hver node sender altså med sin egen rutetabell til nærmeste nabo. Denne metoden deler mange likheter med BGP [9] og RIP [13]. BGP blir brukt i Internett for sammenknytning av autonome nett. BGP har mulighet til å sende hele eller deler av sin egen rutetabell til sin neste nabo. Filtreringen av ruteinformasjon er basert på regelsettet (policy) til hver ruter. I likhet med BGP kan vår protokoll filtrere informasjon. Et nettelement har således full frihet til å velge hvilke ruteinformasjon den ønsker å dele med sine naborutere. En implementasjon kan være, i likhet med iBGP, utstrakt deling av ruteinformasjon mellom rutere innad i ett og samme nett. Imidlertid vil ruteinformasjon bli kjørt gjennom en filtreringsprosess mellom autonome nett i likhet med eBGP. Hvilken ruteinformasjon som blir utvekslet og hvilken som blir filtrert bort, beror på hvert enkelt netts regelsett (policy).

3.4 Policy

Policy betegnes ofte som et sett med regler for hvordan trafikk skal håndteres. I dette arbeidet har vi brukt policy til trafikkstyring i forbindelse med håndtering av trafikk inn og ut av hvert radionettverk, eller over en link. Det vil være naturlig at det lages policy for hvordan et operasjonsnettverk skal brukes som en del av planleggingen av en operasjon. Det er også ønskelig å kunne endre disse reglene underveis i en operasjon for å kunne omprioritere bruken av nettverksressurser, eller for å kunne håndtere uforutsette behov. Løsningen vår tillater endring av regler etter skiftende operative behov.

Utgangspunktet for policy-regelsettet i dette arbeidet er en enighet mellom alle netteiere om et globalt sett av regler. Settet er kjent av alle nett, men hver netteier velger hvilke regler de til enhver tid har implementert eller benytter. Arkitekturen er ikke avhengig av en enighet mellom netteiere for søket, men informasjonsutveksling for oppbygging av hint vil da gå mye enklere. Et eksempel er når et søk blir stoppet på grunn av at forrige nett ikke har lov til å sende lavprioritetstrafikk over neste nett. En tilbakemelding fra forrige node ved hjelp av NOTFOUND bekrefter at den ikke kan søke videre. Søket vil således gå videre uten nødvendigvis å vite årsak. For oppbygging av hint er det gunstig med utveksling av årsak for returnering av søk. Årsaken blir så lagret i hintdatabasen og gjenbrukt ved senere søk.

Arkitekturen gir mulighet for å isolere nett og bestemme hvilken trafikk som får gå gjennom hvilket nettverk til hvilken tid. Muligheten til å isolere nett kan være nødvendig i situasjoner hvor all annen enn tiltenkt trafikk for nettet må blokkeres, nett som har blitt kompromittert, med mere. Utveksling av rutetabeller er basert på regelsettet til individuelle nett. En ruter kan velge å distribuere hele, deler av eller ingenting av ruteinformasjonen til sin neste naboruter.

Rutingsprotokollen støtter i dag distribuert policykontroll av trafikk basert på kilde, destinasjon eller Type Of Service (TOS) som er et felt i IP-header som kan brukes til å identifisere trafikk-klasse eller type. IP *TOS* blir regulert av STANAG 4711 i NATO-sammenheng, men denne er i skrivende stund ennå ikke ratifisert. IP (kilde, TOS, Destinasjon) vil kunne entydig identifisere kilde, destinasjon samt type trafikk. Den vil ikke kunne skille mellom trafikkflyter innenfor

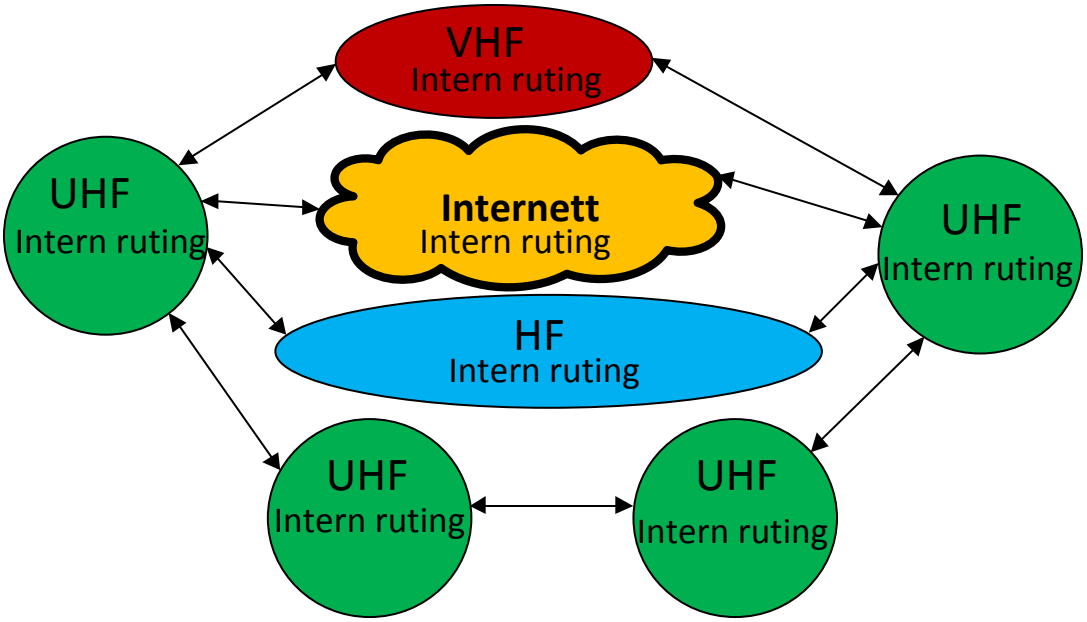
samme trafikktype mellom samme kilde og destinasjon. Utvidelsen med å skille flyter innen samme trafikk-klasse er ikke implementert, men kan utvides med for eksempel transportprotokoll-portnummer.

En fordel med reaktive ruteoppsett er at nettoperatør på et hvilket som helst tidspunkt kan endre sitt eget netts regelsett. Endringen er ikke assosiert med krav om å informere resten av nettet, i motsetning til proaktiv ruting som trenger informasjon for å kunne tilpasse seg ny videresending. En grunn til å endre regelsettet kan være at nettet, innenfor et tidsrom, kun skal brukes kun til sin «primære oppgave».

3.5 Tjenestekvalitet i kommunikasjonsnettverk bestående av ulike radionettverk

Ressursallokering blir brukt for å reservere ressurser i et nett til spesifikk trafikk. På denne måten får man en større forutsigbarhet for at viktig datatrafikk kommer frem. I skrivende stund er det i hovedsak to metoder for håndtering av tjenestekvalitet, Differentiated Services (DiffServ) [14] og Integrated Services (Intserv) [2]15]. I DiffServ er trafikken delt opp i klasser hvor klassene blir behandlet ulikt av nettverket. Graden av ulikhet beror på ønske om differensiering av hver klasse. DiffServ skalerer veldig godt, samtidig som den klarer å utnytte ressursene i nettet godt. Derimot støtter DiffServ ikke QoS per flyt, altså trafikk mellom to applikasjoner. I vårt arbeid og nettene vi adresserer, vil mange av trafikkflytene ha behov for flytkontroll. IntServ gir trafikkontroll på flytnivå, men trenger informasjon om ønsket behandling i nettet fra tilhørende applikasjon. Ønsket blir behandlet av hver ruter, hvor den enten blir avslått eller godtatt.

I det utarbeidede designet blir nett koblet sammen ved hjelp av rutere i et virtuelt nett (figur 3.3). Det vil si at ikke alle rutere i et spesifikt autonomt nett nødvendigvis er medlem i det søkbare virtuelle nettet. Problemet med et virtuelt nett er at vi ikke har direkte tilgang til hvert enkelt netts ressurser. Vi har heller ikke nødvendigvis tilgang til å reservere ressurser i hvert enkelt nett, siden hvert enkelt nett kjører sin egen interne ruteprotokoll (figur 3.5). Vi kan imidlertid reservere en delmengde av estimert tilgjengelig ressurser mellom de virtuelle nodene på de virtuelle nodene. Estimering kan gjennomføres ved hjelp av testtrafikk for å få et bilde av tilgjengelige ressurser. I dette arbeidet antar vi at vi kjenner til nettverksressursene, og at ressursene ble statisk satt. I et ekte deployert eller mobil nett vil estimering av ressurser være påkrevd. En ressurs kan estimeres ved hjelp a flere metoder. En metode er å kjøre aktiv ressursmåling, en annen metode er passiv ressursmåling, en tredje metode er grov estimat basert på link/nettverkskapasitet.



Figur 3.5 *Figuren illustrerer et eksempel på sammenkopling av nettverk med ulik teknologi. Hvert lokale radionettverk kjører sin egen ruteprotokoll som er optimalisert for sitt eget miljø. Vår protokoll har nødvendigvis ikke tilgang til hvert lokale nett sin informasjon om tilgjengelig kapasitet, eller mulighet for å reservere ressurser i et lokalt nett.*

I vårt testoppsett ble hver virtuelle ruter tildelt en statisk ressurs per grensesnitt. Hvis ledige ressurser og policy-regelsettet er oppfylt, vil søket fortsette mot destinasjon. Hvis ressursen derimot ikke er tilgjengelig, blir søket stoppet og returnert til forrige søkenode. Hver allokert ressurs er bundet til en flyt som identifiseres med *(kilde,TOS,destinasjon)*.

3.6 Oppdagelse av nye naboer

Hver ruter i det søkbare virtuelle nettverket må assosieres med en eller flere naborutere som også er medlem i det søkbare virtuelle nettverket. Naboer må derfor oppdages og registreres. I skrivende stund er [17] en mye brukt metode for å oppdage nabonoder.

I vårt arbeid kan avstanden mellom naborutere være alt fra én fysisk link til flere fysiske linker over flere nettverk. I den grad avstanden er mer enn en fysisk link, må ruteren søkes opp. Tradisjonelt brukes en nabo-oppdagelsesprotokoll («Neighbour Discovery») som foretar søket. Søket vil typisk gå med en gitt multicast-adresse. Dagens protokoller har ingen fullgod løsning for oppdagelse av rutere med avstand over flere nettverk. En alternativ løsning kan være basert på Multicast Source Discovery Protocol (MSDP) [18].

I vår implementasjon ble hver nabo statisk konfigurert. Dette gir den fordelen at vi slipper å søke opp naboer på bekostning av mobilitet av nett. Statisk konfigurasjon gir ikke mulighet for

at en nabos nett flytter seg og danner naboskap mot et annet nett uten manuell endring av naboskap.

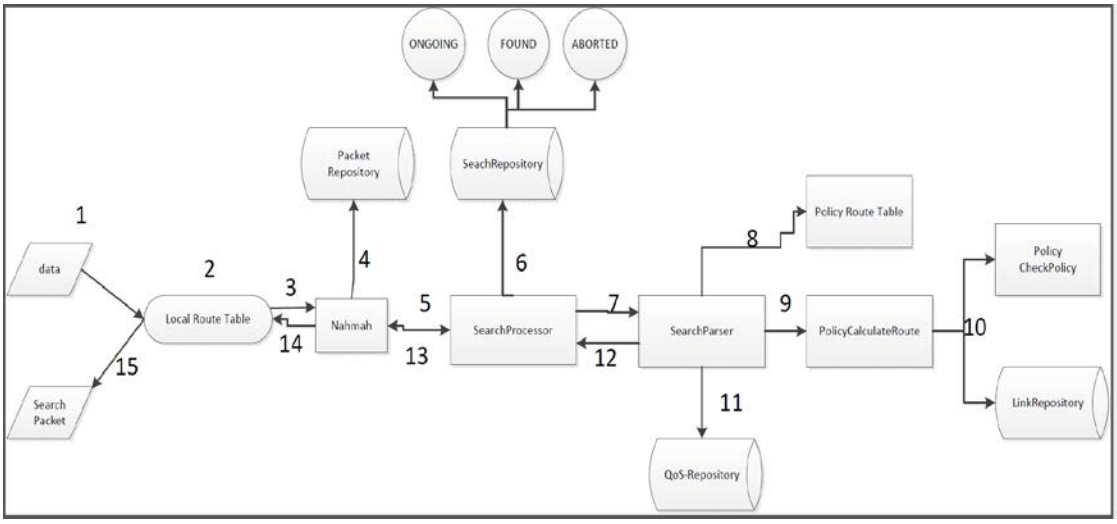
4 Utvikling av kode og testbed

Utvikling og test av løsningen har i all hovedsak foregått i simulator, men koden er skrevet for enkelt å kunne flyttes fra et system til et annet system, slik at løsningen også skal kunne brukes i en testbed. Ofte blir utviklingskode skrevet med bruk av biblioteker gitt av utviklingsmiljøet. Vi ønsket en kodebase som kunne flyttes mellom systemer i stedet for å være bundet til ett spesifikt system. Koden ble derfor skrevet som en modul, med grensesnitt inn mot nye potensielle systemer. Et eksempel på slike grensesnitt kan være tidsbrytere («timere»), utsending av pakker, mottak av pakker med mere. Systemet, enten det er Linux eller Windows, må støtte disse grensesnittene. Vi valgte å kjøre vår kode i en nettverksimulator og en software-ruter på linux, og måtte således implementere grensesnittspesifikke funksjoner for begge systemene, mens hovedmodulen forble uendret.

Hoveddelen av funksjonaliteten ble utviklet i network simulator 3 (ns-3) [19]. ns-3 gir gode muligheter til å isolere et problem, for så å prøve ut løsninger innenfor dette spesifikke problemområdet. Videre gir simulatoren også mulighet til å simulere nettverk med både fast, så vel som trådløs infrastruktur, med og uten mobilitet. Hoved funksjonalitet og ytelsen til metoden ble publisert på den årlige internasjonale militære kommunikasjonskonferansen «MilCom» [20].

Ettersom løsningen er bygget og implementert for å kjøre uavhengig av plattform, har vi hatt mulighet til å teste implementasjonen på software-rutere, slik som «Click modular router» (heretter Click) [16]. Clik er en åpen kildekode-ruter. Den er konfigurerbar, svært fleksibel og enkel å utvide for ny funksjonalitet. Konfigurasjonen til Click er en rettet graf med elementer på punktene langs kantene av grafen. Grafen danner således en sti som trafikken går igjennom fra den mottas/genereres til den forlater ruteren. Vanligvis er ett element ansvarlig for å motta pakker fra luft/kabel og skyve den opp til neste element.

Vår DFSP implementasjon er kompilert inn i Click som et element ved hjelp av push. Push vil si at pakkene blir filtrert og dyttet opp til vårt Clik interface-element med navnet NAHMAH (figur 4.1).

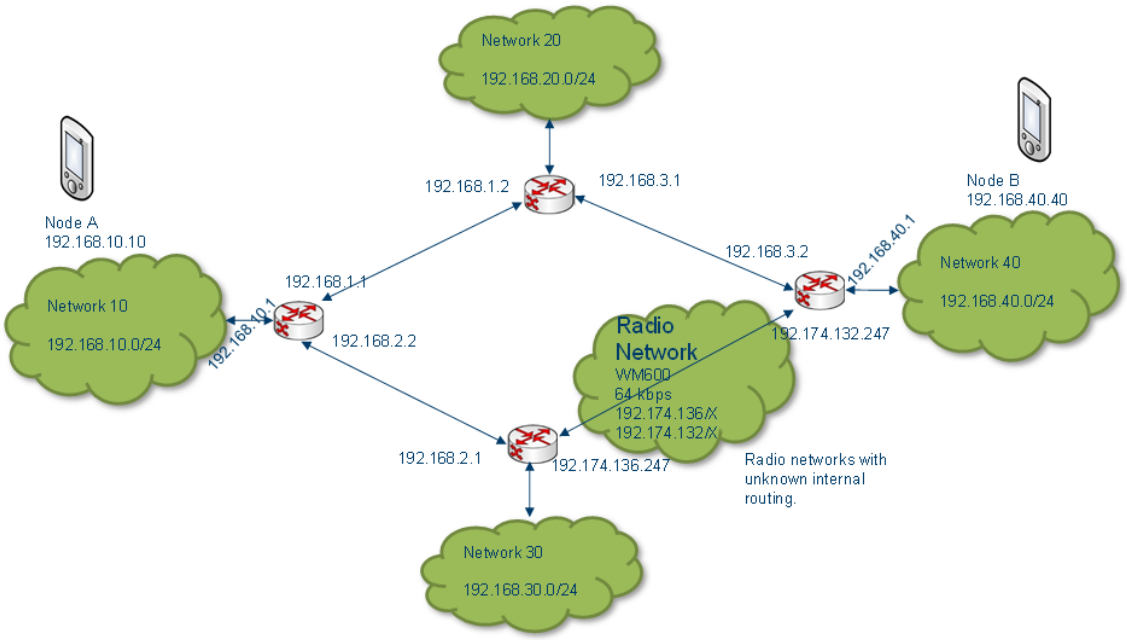


Figur 4.1 Skjematisk oversikt over søkepakke-prosessering internt i vår søkealgoritme.

Figur 4.1 illustrerer kontrollflyten internt i click modular software router. Data eller søkepakker ankommer lokal rutetabell. Ved mangel av ruteinnslag for data eller søkepakker, så sendes pakkene videre til NAHMAH. NAHMAH vil så kalle på vår selvstendig kodebase som håndterer initiering av et søk eller prosessering av søkepakker.

Datapakke mottatt over Nahmah port blir videresendt til searchprocessor. Selve boksen Nahmah i figur 4.1 implementerer således system-grensesnitt for vår kode og benytter systemspesifikt bibliotek. Resten av boksene opererer uavhengig av systemspesifikke biblioteker.

4.1 Click testbed



Figur 4.2 Testbed for kjøring av søk. Fire rutere er med i det virtuelle nettet som binder sammen alle nett.

Figur 4.2 viser topologien for testoppsettet. Node A og node B er to endebrukere som både sender og mottar trafikk. Disse har ingen rute for å nå hverandre, men hver har en standardrute til nærmeste virtuelle ruter. Nærmeste virtuelle ruter blir nådd ved hjelp av intern ruting i hvert enkelt nett. Nærmeste virtuelle ruter blir derfor en gateway. I vår test er node A koblet på nettverket 192.168.10.0/24. All trafikk uten ruteoppslag sendes til 192.168.10.1, som igjen er den nærmeste ruteren i det virtuelle nettverket. Denne ruteren har ikke nødvendigvis et ruteoppslag, men må søke opp en rute. Pakke-trafikk lagres midlertidig på denne ruteren under søkeperioden, men bare for IP-pakker med kildeadresser innenfor nettverket 192.168.10.0/24 som er gitt av dens nettverks-policy. Begge neste hopp lenker har lik kapasitet, og i starten er det ingen hint tilgjengelig. Nexthop velges i vår implementasjon tilfeldig mellom nabonodene ved mangel på hint.

Nettet mellom 192.174.136.247 og 192.174.132.247 består av Kongsberg WM600 radioer. Den virtuelle linken går over to radionett med forskjellige nettmasker. Radionettverkene er isolerte og kjenner ikke til hverandres nettmasker, og har derfor ingen mulighet til å videresende trafikk for det andre radionettet internt. For å løse dette problemet ble tunnel brukt. Det ble sendt trafikk i begge retninger mellom node A og node B. Robustheten ble sjekket ved hjelp av påført linkbrudd. Testen viste at linkbrudd ble detektert og ny sti ble funnet. Policy ble også sjekket ved hjelp av nektelse av et utvalg av IP-adresser, det være seg mellomliggende noder, kilde- eller destinasjonsadresser.

Ressursreservering er implementert basert på IntServ-prinsippet [2][15]. Vi har muligheter for reservasjon på flytnivå. Forespørselen blir sendt, og dersom det er ledige ressurser blir forespørselen sendt videre.

5 Oppsummering

I dette arbeidet har vi presentert DFSP, en ruteprotokoll som møter noen av utfordringene ved sammenkobling av militære radionettverk som det ikke finnes gode løsninger for i dag. Den er basert på dybde-først søkeprinsippet. Dette har til hensikt å beskytte lavkapasitetsnettverk fra både uønsket signaleringstrafikk og datatrafikk i et heterogent nettverk av mange nettverk, men samtidig kunne integrere også disse nettverkene i et større felles nettverk for en operasjon.

Fremtidige militære nett vil måtte støtte heterogenitet for å imøtekomme behovet for økt robusthet, datarate med mer. Et felles heterogent nett vil trenge mekanismer for styring av trafikk og mulighet til å kunne sette forskjellig policy for bruken av nettverket. DFSP adresserer mange av de påpekte utfordringene, samtidig som den har løsninger for problemene påpekt med BGP, og velkjente proaktive og reaktive ruteprotokoller. DFSP kan tilby flere veier til en destinasjon med forskjellig tjenestekvalitet, i henhold til gjeldende nettverks policy, samtidig som den gir netteier full mulighet til å blokkere for eksempel for spesifikke trafikktyper eller trafikk fra andre nasjoner, uten å informere resten av nettverkene i det store nettverket.

DFSP er assosiert med økt sannsynlighet for økt søketid og med risiko for å finne en sub-optimal sti mellom kommuniserende parter. Disse problemene er redusert ved hjelp av rutehint. Hint vil også redusere signaleringstrafikk. Erfaringsresultater fra tidligere søk samles inn og brukes i senere søk.

Policy er implementert for bedre kontroll over både signalering og datatrafikk. Hver naborelasjon er konfigurert med et regelsett basert på netteiers ønske. Regelsettet kan endres uten å informere resten av nettet. Som en konsekvens videresendes søk bare over linker som samsvarer med implementert regelsett.

Protokollen støtter også tilgangskontroll (admission control) samt ressursreservasjon. Når ressursreservasjon er brukt, vil verken signaltrafikk eller datatrafikk bli videresendt over nettverk uten tilstrekkelige ressurser. Søk blir således stoppet, enten ved mangel på ressurs eller ved brudd på lokal policy. I et heterogent nettverk, som i utgangspunktet tillater at all trafikk bruker denne fellesressursen, er det helt nødvendig å innføre tilgangskontroll og ressursreservasjon, samt støtte for QoS rolleprioritering og policy for hvordan nettverket skal brukes.

I vårt eksempel skiller vi trafikken ved (kilde, Type Of Service, destinasjon), men vi kunne også skilt trafikk basert på for eksempel protokolltype eller andre parametere. Hvilke parametere som blir brukt for å identifisere flyter, er mindre viktig, så lenge det gjøres entydig. Ideen er å sikre at nettverkene sender trafikk som forutsatt.

Utviklingen av DFSP har nådd en midlertidig slutt med avslutning av FFI-prosjekt 1249. Videre arbeid bør fokusere på, i prioritert rekkefølge:

- Å identifisere gode nettverksnoder som bør delta i det virtuelle nettverkslaget som kjører DFSP
- Å utforske mekanismer for kapasitetsmålinger over heterogene nett for å unngå overbelastning av nettverket
- Å prøve protokollen ut i et større heterogent nettverk
- Å utvikle adaptiv tidskontroll (timere) for tilpassing av trafikk og nettkapasitet. Så langt er timere statisk implementert, noe som innebærer at tidsstatus for flyter/rute/ressurs/regelsett kan slettes uten at det er meningen.

Referanser

[1] V. Arneson, E. Larsen, J. Sander, T.M. Olsen Mjelde, L.E. Bråten, Ø.Olsen, «Satellite Communication on the move- Measurements at high altitude», FFI rapport 15/00552, BEGRENSET

[2] R. Braden, L. Zhang, S. Berson, S. Herzog, S. Jamin, «Resource ReSerVation Protocol (RSVP)", RFC 2205

[3] L. Landmark, K. Øvsthus, Ø. Kure,"Routing Trade-offs in Sparse and Mobile Heterogeneous Multi-Radio Ad Hoc Networks", in proceedings MILCOM, San Jose, CA, USA, pp. 2229-2236, Nov. 2010.

[4] L. Landmark, M. Hauge, and O. Kure, "Routing Loops in Mobile Heterogeneous Ad Hoc Networks," *in proceedings MILCOM*, Nov. 2013, pp. 112-118.

[5] L. Landmark, Ø. Kure, Knut Øvsthus," Performance analysis of the AODV ad hoc routing protocol in a dual radio network", in proceedings WMuNeP'05, pages 106-112, 2005

[6] A. Eggen, M. Hauge, O. E. Hedenstad, K. Lund, A. Legaspi, H. Seifert, P. Sevenich and P. Simon, "Coalition Networks for Secure Information Sharing (CoNSIS)," (Invited paper) Military Communications Conference (MILCOM), San Diego, 2013.

[7] M. Hauge, J.E. Voldhaug, J. Sander, M.A. Brose, «Multi-Topology Routing – QoS functionality and results from CoNSIS field experiement», FFI rapport 13/00529

[8] P. Psenak, S. Mirtorabi, A. Roy, L. Nguyen, P. Pillay-Esnault, "Multi-Topology (MT) Routing in OSPF", RFC 4915

[9] Y. Rekhter, T. Li, and S. Hares, RFC 4271: A Border Gateway Protocol 4 (BGP-4), IETF Internet Standard, January 2006.

[10] P. B. Godfrey, I. Ganichev, S. Shenker, and I. Stoica, "Pathlet Routing," in Proceedings of the ACM SIGCOMM 2009 Conference on Data Communication, ser. SIGCOMM '09. New York, NY, USA: ACM, 2009, pp. 111–122.

[11] C.-K. Chau, J. Crowcroft, K.-W. Lee, and S. H. Wong, "Inter-domain Routing for Mobile Ad Hoc Networks," in Proceedings of the 3rd International Workshop on Mobility in the Evolving Internet Architecture, ser. MobiArch '08. New York, NY, USA: ACM, 2008, pp. 61–66.

[12] T. Gibbons, J. Van Hook, N. Wang, T. Shake, D. Street, and V. Ramachandran, "A Survey of Tactically Suitable Exterior Gateway Protocols," in Military Communications Conference, MILCOM 2013 - 2013 IEEE, Nov 2013, pp. 487–493

[13] G. Malkin, "RIP Version 2", RFC 2453

[14] K. Nichols, S. Blake, F. Baker, and D. Black, RFC 2474: Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers, IETF Internet Standard, December 1998.

[15] J. Wroclawski, RFC 2210: The Use of RSVP with IETF Integrated Services, IETF Standards Track, September 1997.

[16] The Click Modular Router Project. Sist besøkt 11.10.2016 [Online]. Available: http://www.read.cs.ucla.edu/click/

[17] T. Clausen, C. Dearlove, and J. Dean, "RFC 6130: Mobile Ad Hoc Network (MANET) Neighborhood Discovery Protocol (NHDP)," IETF Internet-Standard, MANET WG, April 2011.

[18] B. Fenner, D. Meyer," Multicast Source Discovery Protocol (MSDP)", RFC 3618

[19] Network Simulator 3 "ns3", https://www.nsnam.org/

[20] L. landmark, E. Larsen, M. Hauge, Ø. Kure, «Resilient internetwork routing over heterogeneous mobile military networks», Military Communications Conference, MILCOM 2015 - 2015

[21] https://forsvaret.no/aktuelt/forsvarets-nye-kampvognfamilie, Sist besøkt 11.10.2016 [Online]

Forkortelser

AODV	Ad hoc On-Demand Distance Vector
ARP	Address Resolution Protocol
BGP	Border Gateway Protocol
DFSP	Depth-First Search Protocol
DFS	Dybde-først søk
DiffServ	Differentiated Services
EBGP	External BGP
HF	High Frequency
IBGP	Internal BGP
IntServ	Integrated Services
JISR	Joint Intelligence, Surveillance and Reconnaissance
LTE	Long-Term Evolution
LPD	Low Probability of Detection
MANET	Mobile Ad Hoc Network
MIT	Massachusetts Institute of Technology
MRR	Multi-Rolle Radio
MSDP	Multicast Source Discovery Protocol
MT-OSPF	Multi Topology Open Shortest Path First
NbF	Nettverksbasert forsvar
NBWF	NarrowBand WaveForm
NHDP	Neighbor Host Discovery Protocol
OLSR	Optimized Link State Routing
OSPF	Open Shortest Path First
SOTM	Satcom On The Move
TOS	Type Of Service
UHF	Ultra High Frequency
VHF	Very High Frequency

About FFI

The Norwegian Defence Research Establishment (FFI) was founded 11th of April 1946. It is organised as an administrative agency subordinate to the Ministry of Defence.

FFI's MISSION

FFI is the prime institution responsible for defence related research in Norway. Its principal mission is to carry out research and development to meet the requirements of the Armed Forces. FFI has the role of chief adviser to the political and military leadership. In particular, the institute shall focus on aspects of the development in science and technology that can influence our security policy or defence planning.

FFI's VISION

FFI turns knowledge and ideas into an efficient defence.

FFI's CHARACTERISTICS

Creative, daring, broad-minded and responsible.

Om FFI

Forsvarets forskningsinstitutt ble etablert 11. april 1946. Instituttet er organisert som et forvaltningsorgan med særskilte fullmakter underlagt Forsvarsdepartementet.

FFIs FORMÅL

Forsvarets forskningsinstitutt er Forsvarets sentrale forskningsinstitusjon og har som formål å drive forskning og utvikling for Forsvarets behov. Videre er FFI rådgiver overfor Forsvarets strategiske ledelse. Spesielt skal instituttet følge opp trekk ved vitenskapelig og militærteknisk utvikling som kan påvirke forutsetningene for sikkerhetspolitikken eller forsvarsplanleggingen.

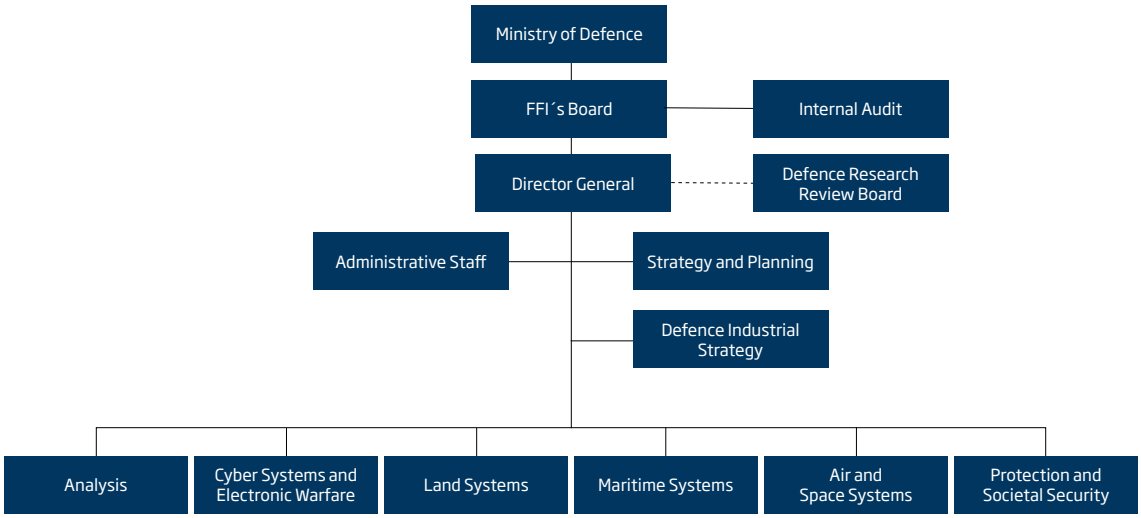
FFIs VISJON

FFI gjør kunnskap og ideer til et effektivt forsvar.

FFIs VERDIER

Skapende, drivende, vidsynt og ansvarlig.

FFI's organisation



Forsvarets forskningsinstitutt
Postboks 25
2027 Kjeller

Besøksadresse:
Instituttveien 20
2007 Kjeller

Telefon: 63 80 70 00
Telefaks: 63 80 71 15
Epost: ffi@ffi.no

Norwegian Defence Research Establishment (FFI)
P.O. Box 25
NO-2027 Kjeller

Office address:
Instituttveien 20
N-2007 Kjeller

Telephone: +47 63 80 70 00
Telefax: +47 63 80 71 15
Email: ffi@ffi.no

FFI Forsvarets forskningsinstitutt
Norwegian Defence Research Establishment