FFI-RAPPORT

19/00940

Information Centric Networking

– muligheter for mobile militære kommunikasjonsnettverk

Lars Landmark
Mariann Hauge
Erlend Larsen
Øivind Kure

Information Centric Networking – muligheter for mobile militære kommunikasjonsnettverk

Lars Landmark
Mariann Hauge
Erlend Larsen
Øivind Kure

Forsvarets forskningsinstitutt (FFI) 20. august 2019

Emneord
Kommunikasjonsnettverk
Mobilkommunikasjon
Radiokommunikasjon

FFI-rapport
19/00940

Prosjektnummer
1367

ISBN

P: 978-82-464-3190-1
E: 978-82-464-3191-8

Godkjennere

Jan Erik Voldhaug, *forskningsleder*

Dokumentet er elektronisk godkjent og har derfor ikke håndskreven signatur.

Sammendrag

Militære operasjoner i framtiden vil trolig stille strengere krav til kommunikasjonsnettverkene. Det vil bli et sterkere behov for samhandling på tvers av ulike typer enheter i tillegg til utveksling og innhenting av data fra et økende antall sensorer. Mobile militære kommunikasjonsnettverk må trolig kunne fungere under mer varierende og utfordrende omgivelser enn i dag. Det er en konsekvens av økende militære tidskrav som igjen krever evne til rask tilpasning til ny situasjon.

Internett og de fleste andre kommunikasjonsnettverk som benyttes i dag, inklusive de militære, er basert på Internet Protocol (IP). Med IP-baserte nettverk vil det være utfordrende å møte både dagens og framtidens behov innen samhandling, spesielt på gruppenivå, i trådløse kommunikasjonsnettverk. Trådløse nettverk har typisk langt lavere kapasitet og lavere stabilitet sammenlignet med trådbaserte nettverk.

IP kan sies å være en suksessfaktor for teknologiutviklingen innenfor kommunikasjonsnettverk. Men endringer i måten internett blir brukt på, fører til at det forskes på alternative nettverks arkitekturer. Information Centric Networking (ICN) er en nettverksarkitektur som får oppmerksomhet innenfor sivil og militær forskning og er på sikt en aktuell arvtaker etter IP.

Formålet med denne rapporten er å vurdere i hvilken grad ICN vil kunne bidra med å møte noen av utfordringene for framtidens mobile militære kommunikasjonsnettverk. Rapporten skisserer en forventet utvikling når det gjelder militære behov for informasjonsutveksling og peker på hvilke utfordringer IP-arkitekturen har. Videre beskriver vi ICN-arkitekturen og hvordan den kan møte disse utfordringene. ICN er en ung arkitektur og dermed mindre utforsket i mobile trådløse nettverk. Vurderingene i denne rapporten er derfor hovedsakelig basert på litteraturstudier, utforsking av åpen kildekode og bygging av en demonstrator, kombinert med FFIs erfaring med forskning på mobile militære kommunikasjonsnettverk.

Vi konkluderer med at ICN har egenskaper som potensielt kan forbedre effektiviteten og fleksibiliteten til militære kommunikasjonsnettverk sammenliknet med IP-arkitekturen. Arkitekturen er spesielt interessant for trådløse nettverk og nettverk hvor informasjons-utvekslingen er på gruppenivå. Selv om ICN-teknologien er for umoden til å tas i bruk på kort sikt, har den egenskaper som gjør den lovende for videre studier. Rapporten er ment å informere om den vitenskapelige og teknologiske utviklingen som vil kunne ha betydning for materiellanskaffelser for Forsvaret. Rapporten er skrevet spesielt for personell i forsvars-sektoren som arbeider med kommunikasjonsnettverk.

Summary

Future military operations will probably impose stringent requirements on the communication networks. There will be a stronger need for interaction across different types of units as well as exchange and collection of data from an increasing number of sensors. Future mobile military communication networks must probably operate under more diverse and challenging environments than today due to increasing military time requirements which in turn require the ability to quickly adapt to new situations.

The Internet and most other communication networks used today, including military networks, are based on the Internet Protocol (IP). With IP-based networks, it will be challenging to meet both present and future needs in interaction, especially at group level, in wireless communication networks. Wireless networks typically have much lower capacity and lower stability compared to wired networks.

While IP can be said to be a success factor for technology development in communications networks, changes in the way the Internet is used lead to research into alternative network architectures. Information Centric Networking (ICN) is a network architecture that receives attention in civil and military research and is, in the long term, a topical successor to IP.

The purpose of this report is to assess to what extent ICN will be able to help meet some of the challenges for future mobile military communication networks. The report outlines an expected development for military information exchange and points to challenges that the IP-architecture has in meeting these needs. The report furthermore describes the ICN-architecture and how it addresses these challenges. ICN is a young architecture and thus less explored in mobile wireless networks. The assessments made in this report are therefore based mainly on literature studies, exploration of open source code and the construction of a demonstrator combined with FFI's experience with research within mobile military communication networks.

We conclude that ICN has features that could potentially improve the efficiency and flexibility of military communications networks compared to the IP-architecture. The architecture is especially interesting for use in changing networks and networks where the information exchange is at group level. ICN-architecture is too immature to be able to be used in the short term, but the attractive properties make it necessary to study ICN further. This report is intended to inform about the scientific and technological developments that may be important for future material procurement for the Norwegian Armed Forces and is written specifically for personnel in the defense sector who work with communication networks.

Innhold

1 Innledning

> "Today we build, support, and use Internet applications and services on top of an extremely capable architecture not designed to support them. What if we had an architecture designed to support them?"
>
> Hentet fra: https://named-data.net/project/faq

Teknologi for å kommunisere har alltid vært under utvikling. Et godt eksempel er overgangen fra linjesvitsjet til Internett-basert telefoni. Telefoni var opprinnelig basert på en sammenhengende kobbervei mellom abonnentene. Denne teknologien ble videre utviklet til en linjesvitsjet teknologi hvor veien mellom abonnentene ble satt opp automatisk. Etterhvert meldte behovet seg for også å støtte andre tjenester enn kun tale. Pakkesvitsjet teknologi ga bedre støtte for nye tjenester med bedre ressursutnyttelse. Overgangen fra linjesvitsjet til pakkesvitsjet nettverk kom som en konsekvens av behov for å overføre pakker med informasjon, snarere enn en strøm av tale.

Dagens fokus er ikke lengre å overføre informasjon mellom to endesystemer, men heller å finne og hente informasjon. Det å bruke datapakker for overføring er ikke et mål i seg selv, men kun et verktøy for å dekke et kommunikasjonsbehov. IP-protokollene er derfor ikke nødvendigvis den mest effektive metoden for å imøtekomme fremtidens kommunikasjonsbehov.

1.1 Noen militære trender med innvirkning på informasjonsutveksling

Forsvaret deler mange felles trekk med det sivile når det gjelder behov for informasjonsutveksling. Ser vi på trender innen militær utvikling og kommunikasjon er det noen som peker seg ut mer enn andre slik vi ser det. Eksempler på trender er økt innhenting og fordeling av sensor-informasjon for bedre situasjonsforståelse, økt kommunikasjon til og mellom autonome systemer, økt kommunikasjon til og mellom våpensystemer og økt oppmerksomhet rundt tillit til mottatt informasjonen. Dette er noen få overordnede eksempler på trender som har sine ulike, men unike behov.

Sensorinformasjon vil variere mye med ulike typer sensorer, men vil potensielt kreve vesentlig datarate fra nettverket. Sensorinformasjonen vil være etterspurt av ulike analysesystemer, beslutningsstøttesystemer og autonome systemer. Informasjonen for å understøtte god situasjonsforståelse vil gå ut til flere mottakere. Gode distribusjonssystemer vil derfor være ressursbesparende. Styring av ett eller flere våpensystemer vil trolig i større grad foregå over lengre avstander, og vil ha behov for pålitelig kommunikasjon mellom beslutningstaker og våpensystemer. Informasjonsmottaker må ha tiltro til at mottatt informasjon er blitt produsert av rettmessig produsent og videre ikke har blitt endret på veien mellom produsent og mottaker.

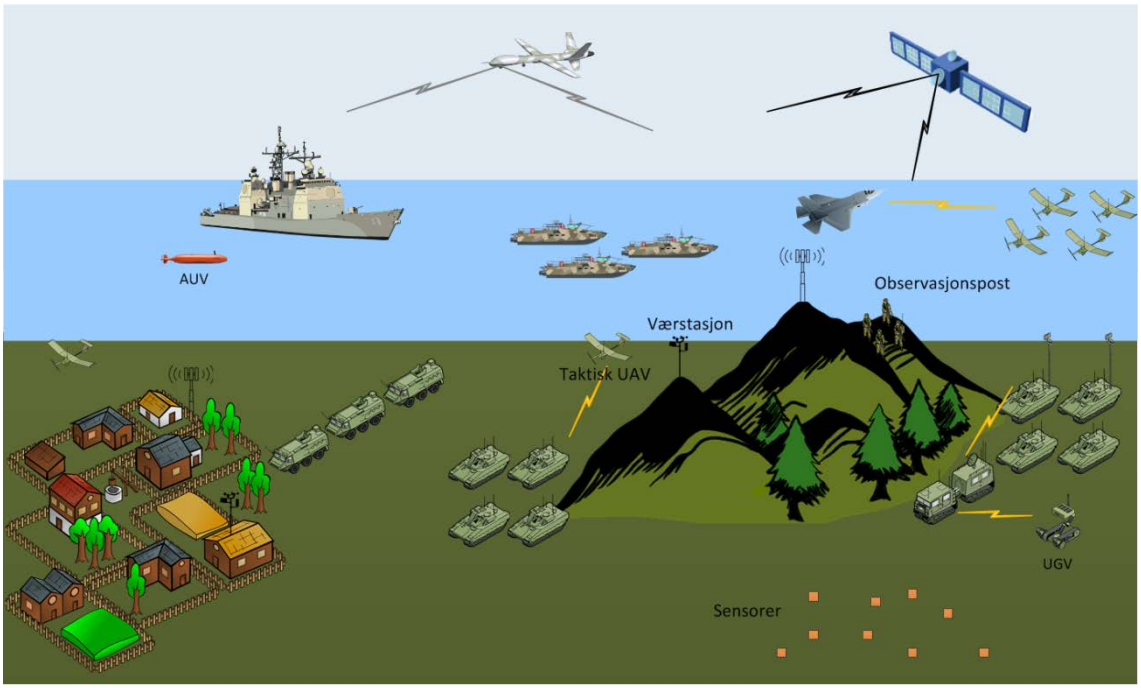
1.2 Fremtidens militære kommunikasjonsnettverk og dens evne til å levere tjenester ut til bruker

Fremtidens militære kommunikasjonsnettverk vil kunne bli mer ustabile enn dagens kommunikasjonsnettverk. Med ustabile nettverk mener vi her nettverk som, på grunn av omgivelser, vil variere i sin evne i å levere tjenester ut til brukerne. Det er spesielt noen faktorer vi forventer å se mer av i fremtiden som vil kunne føre til økt ustabilitet i trådløse nettverk. Dette er elektronisk krigføring (EK), mobilitet og spesielt bruk av flere ulike radiosystemer i samme nettverk.

Internett og kommunikasjonsarkitekturer har alltid og vil også i fremtiden være under kontinuerlig endring for å kunne besvare nye utfordringer. Kommunikasjonsutfordringer har i store trekk så langt blitt løst innenfor IP-teknologi. Derimot, det er ikke gitt at IP er den beste løsningen for dagens og fremtidens utfordringer. IP er designet rundt lokasjon, dvs. en IP-adresse og dens lokasjon i nettverket. I flerbruksnettverk med behov for økt fleksibilitet, og med ustabile nettverk vil tjenester kunne flytte mellom ulike IP-adresser, samtidig som IP-adressen bytter lokasjon i nettverket. Dagens systemer er utfordret med gode synkroniseringsrutiner for å kunne etablere stabile tjenester i et dynamisk miljø.

1.3 Information Centric Networking, en alternativ nettverksarkitektur

Information Centric Networking (ICN) er en nettverksarkitektur som potensielt kan imøtekomme flere av utfordringene vi har i dag med IP. Den er basert på en alternativ måte å drive informasjonsutveksling og har økende oppmerksomhet innenfor sivil og militær forskning, se spesielt kapittel 4, 5 og 7. ICN er en potensiell arkitektur for fremtidens Internett, men er trolig mer aktuell for spesialiserte kommunikasjonsnettverk, eksempelvis for militære anvendelser som illustrert i figur 1.1 på neste side.



Figur 1.1 Kommunikasjonsnettverk etablert ved hjelp av ulike radioteknologier med ulike egenskaper knyttet til datarate og transmisjonsrekkevidde.

Figur 1.1 illustrerer et nettverk hvor både bemannede og ubemannede enheter er koblet sammen ved hjelp av en felles trådløs kommunikasjonsinfrastruktur. Teknologiene som benyttes for sammenkobling vil naturligvis ha ulike egenskaper og derav også forskjellig evne til å håndtere ulike tjenester. Figuren viser et eksempel på et nettverk som i mange tilfeller vil være utfordret med hensyn på stabilitet med IP, ettersom IP-arkitekturen er orientert rundt stabile ende til ende forbindelser.

I dynamiske miljøer vil nettetverket endre seg på grunn av trafikk, mobilitet eller andre årsaker slik som f.eks feil. Som en konsekvens av endring, må nettetverket konvergere til ny tilstand lokalt eller globalt. Med ulike kommunikasjonsteknologier vil sannsynligheten for ulike syn på topologien øke, og med det øke faren for ustabilitet [15].

En egenskap ved ICN er at arkitekturen ikke er basert på endenodenes nettverksadresser som med IP. ICN navngir derimot selve informasjonen som skal utveksles. Informasjonen vil da selv være det sentrale, og ikke IP adressene til nettverksnodene. ICN skiller seg fra IP ved at det benyttes distribuert lagring, autentisering av informasjon og ved at informasjonen er integritetbeskyttet.

ICN bruk av mellomlagring er motivert med hensyn til blant annet utvikling og kostnad til data-lagring sett opp mot datarate. Over tid, så har data-lagring blitt billigere mens kostnad for datarate ikke har fulgt samme trend[33][34]. Midlertidig lagring av data og gjenbruk av data er derfor i mange tilfeller foretrukket fremfor det å sende samme informasjon flere ganger over samme nettverksressurs. ICN er orientert rundt små informasjonselementer og deling av disse

der hvor dette er mulig. Bruken av ICN kan derfor potensielt redusere kapasitetsbehovet på linklaget, og dermed potensielt redusere behovet for linker med høyere datarater. Dette gjøres med en mer effektiv bruk av minne, og ved å redusere transmisjon av samme data der hvor dette er mulig. Denne måten å kommunisere på muliggjør økt fleksibilitet, robusthet og ikke minst bedre støtte for gruppekommunikasjon. Med gruppe-kommunikasjon mener vi i denne rapporten teknologiske løsninger som muliggjør effektiv informasjons-utveksling mellom medlemmer av en gruppe der alle medlemmene er interesserte i samme informasjon. Et eksempel på dette er distribusjon av geografiske posisjoner mellom enheter i en militær avdeling, slik at alle enhetene kjenner hverandres posisjoner.

1.4 Fokus, metode og oppbygning av rapporten

På bakgrunn av forventede fremtidige utfordringer knyttet til mobile militære kommunikasjons-nettverk, diskuterer vi i denne rapporten hvordan ICN potensielt kan imøtekomme noen utvalgte utfordringer. Det presenteres også noen utfordringer ved ICN som bør adresseres videre. Fokuset i rapporten er hovedsakelig på anvendelser innenfor mobile militære nettverk.

Metoden for arbeidet med denne rapporten har vært litteraturstudier kombinert med FFIs kjennskap til mobile kommunikasjonsnettverk. Mye av bakgrunnsinformasjonen er hentet fra tidligere arbeid innen trådløse heterogene nettverk [14][15], og gruppekommunikasjon [16][17][18]. Vurderingene som er gjort med hensyn på ICN er også basert på utforsking av programvarekode og basert på resultater ved bygging av en ICN-demonstrator for trådløse nettverk [13].

Resten av rapporten er organisert som følger: I kapittel 2 peker vi på de store utviklingstrendene for IP-teknologi som en bakgrunn for å forstå utgangspunktet for ICN. I kapittel 3 ser vi på noen utfordringer vi forventer vil øke for Forsvarets fremtidige mobile kommunikasjonsnettverk og peker på konkrete problemer ved IP-arkitekturen. I kapittel 4 gir vi en overordnet introduksjon til ICN, eksemplifisert ved hjelp av Named Data Networking(NDN) som er et konkret implementert design av ICN. I kapittel 5 beskriver vi hvordan ICN-arkitekturen kan hjelpe på mange av de utfordringene beskrevet i kapittel 3. I kapittel 6 diskuterer vi utfordringer som bør adresseres videre innen ICN før kapittel 7 henviser til videre lesing. I kapittel 8 gir vi en kort oppsummering og anbefaling for veien videre.

2 Internetteknologien og de store utviklingstrender

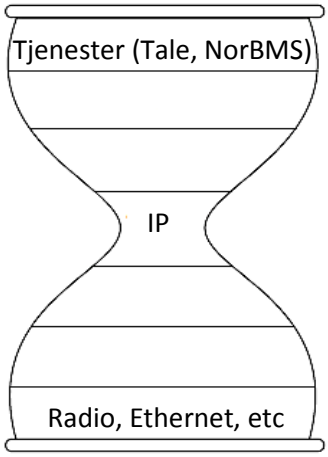
Tradisjonelle kommunikasjonsnettverk, slik vi kjenner og bruker dem i dag, har sin bakgrunn fra telefoninettet. Telefoninettet ble designet for å opprette forbindelser mellom stasjonære telefoner. Hovedoppgaven til telefoninettet var således å opprette forbindelser mellom vilkårlige telefoner ved hjelp av ett og samme nettverk. Siden telefonene var stasjonære, kunne de tilordnes en adresse (telefonnummer) som i stor grad var basert på telefonens geografiske lokasjon. Telefoninettverkene ble derfor bygget rundt linjesvistjet nettverk. Linje i forståelsen av å sette opp en linje mellom to telefoner.

Internetteknologien kom som en konsekvens av endring i bruk av nettverket. Endringen gikk fra å kunne støtte telefoni til å støtte overføring av generell digital informasjon. Med økt utveksling av digital informasjon kom også behovet for bedre utnyttelse av nettverksressursene[1]. I motsetning til telefoni, representerte nye digitale datatjenester ulike behov for informasjonsutveksling.

IP med pakkebasert kommunikasjon ble introdusert for å kunne utnytte nettverksressursene bedre enn linjesvitsjet nettverk. Overgangen fra linjesvitsjede til pakkebaserte nettverk gikk i store trekk ut på å dele opp datastrømmene i små informasjonselementer (pakker) som kan sendes uavhengig av hverandre i nettverket. Med pakkebasert nettverk fikk vi mulighet til å flette pakker fra forskjellige kilder og mottakere inn på delte kommunikasjonslinker. Med IP er hver enhet tildelt en IP-adresse. Denne globale adressen fører til at enheter kan knyttes sammen på tvers av nettverk uavhengig av underliggende link-teknologi og overliggende tjenester.

IP-arkitekturen blir ofte illustrert som et timeglass der IP står sentralt og binder sammen overliggende protokoller og tjenester med underliggende transmisjonsteknologier som vist i figur 2.1. Et IP-nettverk består av et nettverk av noder som alle støtter IP, men som kan bestå av ulike transmisjonsteknologier.

[1] Med nettverksressurser mener vi i denne sammenheng tilgjengelig datarate.



Figur 2.1 Internett-timeglasset. Tjenester kjøres over IP, og IP kjøres over forskjellige transmisjonsteknologier. Felles for alle Internettenheter er IP, mens det som er over og under IP vil kunne være forskjellig.

Med IP og pakkebaserte nettverk flyttet problemområdet seg fra å vite hvilken lokasjon en enhet befant seg på, til å vite hvilke tjenester som finnes på hvilken lokasjon. Bruken av Internett er derfor delt mellom tjenester, deres brukere og nettverket. Brukerne er opptatt av tjenester, mens nettverket som skal utveksle informasjon er fokusert på lokasjon i form av IP-adresse. For å få datatjenester til å benytte seg av Internetteknologi er vi i dag i mange tilfeller avhengig av katalogsystemer. Katalogsystemene knytter tjenester i form av navn til lokasjon gitt ved en IP-adresse. Et eksempel på en katalogtjeneste er Domain Name System (DNS). DNS er tjenesten som binder navn til IP-adresser. Et eksempel er når en bruker ønsker å bruke World Wide Web (WWW) og skriver inn en navn-adresse i en nettleser, f.eks (www.ffi.no). Navnet www.ffi.no blir da sendt til DNS-tjeneren som igjen returnerer IP-adressen (91.189.171.115). IP-adressen blir videre brukt av IP-nettverket for og nå frem til ønsket lokasjon.

I IP-arkitekturen utveksles informasjon mellom lokasjoner og er da avhengig av blant annet ruting, forwarding og nettverk management. Ruting er tjenesten i nettverket som sørger for at trafikk finner veien fra produsent til konsument. I et IP-nettverk vil alle enhetene ha en IP-adresse, og rutingen er derfor ansvarlig for å tegne et kart for hvordan IP-pakkene kan nå hver lokasjon adressert med en IP adresse. Videre, vil alle nettverksenheter som videresender IP-trafikk ha behov for funksjonalitet for å prosessere informasjonen fra inngående link/port til utgående link/port. Denne prosessen er ofte gitt ved navnet forwarding. Sammenhengen mellom ruting og forwarding er at rutingsprosessen skriver inn i en forwarding tabell for hvordan nå en destinasjon. Forwarding-prosessen slår opp i denne tabellen i prosessen med å flytte informasjon fra innkomne link/port til utgående link/port. Nettverk management er prosessen med å administrere datanettverk, hvor blant annet tjenester for feilsøking, ytelsesbehandling og vedlikehold av kvaliteten på tjenesten inngår.

Designet av Internett er, i likhet med telefoni, bygget rundt prinsippet om to kommuniserende enheter. Denne måten å kommunisere på er referert til som unicast. Med utvidet bruk av Internett ble det etterhvert behov for funksjonalitet som dekket flere kommuniserende enheter

innenfor én og samme tjeneste. Behovet var mulighet for informasjonsutveksling i en gruppe uten å sende samme informasjon flere ganger over én og samme nettverksforbindelse. Med andre ord: det ble et behov for å utveksle informasjon effektivt mellom flere. Behovet for gruppekommunikasjon ble da løst i form av teknologien multicast.

Multicast var ikke med i det opprinnelig IP-designet, men har kommet til i ettertid [20]. I ettertid er det også blitt behov for støtte for kommunikasjon i nettverk med stor forsinkelse og høy pakketapssannsynlighet. Slike nettverk blir ofte referert til som Delay Tolerant Networking (DTN) [23]. En annen viktig funksjonalitet som er lagt til i senere tid er mulighet for strukturert informasjonsdeling. I store trekk betyr det å skyve informasjon med forventet høy interesse ut til temporære lagringssteder i flere geografiske områder. En bruker vil da kunne etablere en forbindelse til nærmeste innholdsleverandør uten å måtte gå hele veien til innholdsprodusenten. Denne metoden for deling av informasjon er kjent som Content Delivery Networking (CDN) [24] og er mye brukt på Internett i dag. Oppsummert så var IP-arkitekturen designet for unicast-kommunikasjon, mens funksjonalitet slik som multicast, DTN og CDN ikke var en del av arkitekturen, men lagt til som tillegg.

Alle behov som ikke har hatt støtte i det opprinnelige IP-designet er blitt forsøkt dekket med spesialløsninger. Som et eksempel, har vi ingen gode løsninger for multicast mellom nettverk eid av forskjellige Internettleverandører. En foreslått løsning for multicast-støtte i større nettverk er ved bruk av Virtual Private Network (VPN) [25] for Cisco Systemer. Løsningen gir et godt bilde av kompleksiteten det innebærer å legge til tjenester som ikke har direkte støtte fra det opprinnelige IP-designet.

Bruken av IP har over tid utviklet seg på mange områder. Over samme tid har det vært mindre fokus på det å utnytte felles egenskaper eller informasjon på tvers av tjenester. Konsekvensen av utviklingen er at vi i dag har mange tjenestesiloer, og et stort utvalg av protokoller for å understøtte forskjellige tjenestetyper.

3 IP-arkitekturen og utfordringer med fremtidens mobile militære kommunikasjonsnettverk

> «Moderne krisehåndtering og krigføring kjennetegnes av korte tidslinjer, komplekse situasjonsbilder og stort informasjonsbehov. For å forbedre Forsvarets evne til å føre høyintensiv strid og håndtere kriser, må evnen til å fatte og iverksette rettidige beslutninger styrkes. Bedre situasjonsforståelse kan oppnås ved at data fra mange kilder sammenstilles i økende grad og gjøres tilgjengelig for brukere på ulike nivåer. Sensorer, våpen og plattformer knyttes sammen, uavhengig av forsvarsgren og våpenart, for å bidra til økt operativ evne.»
>
> Prop. 151 S (2015–2016)

Fremtidens mobile militære kommunikasjonsnettverk vil trolig måtte kunne tilby andre egenskaper enn hva dagens IP-nettverk er i stand til å tilby for å kunne understøtte fremtidens krisehåndtering og krigføring. Kommunikasjonsnettverkene må trolig støtte overføring av mer sensordata og økende informasjonsutveksling mellom mobile og stasjonære militære nettverk.

Informasjonstilgjengelighet er viktig i militære operasjoner. En metode for å øke informasjons-tilgjengelighet er å gjøre seg mindre avhengig av én nettverksteknologi. Flere ulike nettverks-teknologier vil kunne tilby ulike og redundante veier. Vi antar derfor at tjenester og/eller informasjonen i fremtiden ikke nødvendigvis er bundet til én teknologi, men kan hentes over flere tilgjengelige nettverksteknologier og da gjerne i parallell hvis mulig. Vi antar også at informasjon ikke bare blir produsert og konsumert i det mobile nettverk, men at informasjon vil kunne flyte mellom og over mobile nettverk. Denne forventningen kommer som en konsekvens av sammenknytting av ulike systemer som beskrevet i Prop. 151 S (2015–2016).

Det er spesielt noen faktorer vi forventer vil være motiverende for en endring: økt behov for effektiv støtte for gruppekommunikasjon, økt sannsynlighet for ustabile nettverk, økt behov for autentisering av data, økt behov for informasjonsoverføring og økt nettverkskompleksitet. Disse faktorene vil fremtvinges over flere områder i fremtiden, men kanskje spesielt i forbindelse med innføring av autonome systemer.

I dette kapittelet vil vi beskrive noen utfordringer med å imøtekomme endringene med IP.

3.1 Effektiv gruppekommunikasjon

Effektiv IP-basert gruppekommunikasjon kjennetegnes med liten bruk av nettverksressurser for informasjonsutveksling mellom kilde og mottakere. Informasjon som skal ut til flere

distribueres ved å sende informasjon kun én gang mellom to nettverksenheter uavhengig av antall mottakere. Det vil si, hvis én nettverksenhet har flere mottakere som er knyttet opp mot flere nabonettverksenheter, vil nettverksenheten duplisere informasjonen og sende den videre til nabonettverksenhetene som har mottakere. Duplisering kan enten gjøres ved kringkasting på lag 2 nivå (link), i selve nettverket på lag 3 (i kommunikasjonsinfrastrukturen) eller som et *overlay*-nettverk (i informasjonsinfrastrukturen). Hver metode har sine styrker og svakheter. IP-basert gruppekommunikasjon kan videre karakteriseres utfra hvordan informasjon deles, og over hvilken tidsperiode informasjonen deles, dvs. enten samtidig eller spredd over tid.

Med radiokringkasting løses gruppekommunikasjon kun lokalt, dvs. innenfor rekkevidden til radioen. Ved behov for gruppekommunikasjon utover rekkevidden til en radio må det brukes andre løsninger. For å oppnå effektivitet i form av lav ressursbruk, vil det være gunstig at gruppekommunikasjon blir utført direkte i nettverkslaget, lag 3. Alle noder må da støtte multicast, noe som krever spesialtilpasninger. Dette er i motsetning til en overlay-løsning hvor nettverkslaget kun trenger å støtte unicast, og dermed ingen spesialtilpasninger på nettverks-laget. Med et overlay-nettverk, som ved Publish/Subscribe [1], vil det være spesielle noder som dupliserer og fordeler informasjonen. Det kan bety at samme informasjon blir sendt flere ganger på samme link eller kanal og er således mindre ressursbesparende. Samtidig er styrken at bare spesielle noder, trenger å støtte gruppekommunikasjon.

I militære nettverk kan det være behov for to forskjellige typer gruppekommunikasjon. Den ene metoden er samtidig utveksling av informasjon. Det vil si at informasjon sendes ut til alle mottakere samtidig og kan da ikke hentes på et senere tidspunkt. Den andre typen er når informasjonen skal ut til flere, men hvor informasjonen blir hentet på forskjellige tider. I dag har vi ingen fullgode metoder som støtter begge disse typene samtidig, men vi har metoder som løser hvert enkelt problem. Gruppekommunikasjon som krever samtidighet (typisk distribusjon av sanntidsinformasjon) blir ofte løst i kommunikasjonsinfrastrukturen ved hjelp av multicast, mens informasjon som blir etterspurt over forskjellig tid blir ofte løst innenfor informasjons-infrastrukturen ved hjelp av CDN.

3.1.1 Effektiv gruppekommunikasjon, utfordringer innen kommunikasjons-infrastruktur

Tjenester som bygger situasjonsforståelse ved hjelp av utveksling av posisjoneringsdata og/eller video er avhengig av effektiv gruppekommunikasjon. Multicast på nettverksnivå (kommunikasjonsinfrastrukturen) er da den foretrukne metoden. I IP-arkitekturen er dette implementert med separate protokoller, både på forwarding, ruting og management. Ulempen med denne tilnærmingen er at det ofte må kjøres flere nettverksprotokoller parallelt med dertil økt protokolltrafikk og kompleks administrasjon og konfigurering.

Gruppekommunikasjon mellom forskjellige IP-nettverk har over lengre tid vært utfordrende. Det finnes metoder for utveksling av gruppeinformasjon internt i et trådbasert nettverk. I mobile militære nettverk er utfordringene større, og metoder som blir brukt på fast nettverk er ofte ikke tilstrekkelig. Det finnes noen metoder, deriblant [18], for innføring av gruppekommunikasjon

inn i et trådløst nettverk, men de foreslåtte løsningene så langt gir ingen fullgode løsninger. Som et resultat flyttes ofte funksjonalitet for gruppekommunikasjon over til informasjons-infrastrukturen på bekostning av god ressursutnyttelse.

3.1.2 Effektiv gruppekommunikasjon, utfordringer innen informasjonsinfrastruktur

Gruppekommunikasjon innen informasjonsinfrastruktur blir ofte løst ved å etablere et nettverk av møtepunkter (*broker*) og bruk av unicast. Møtepunktene kan enten selv være mottakere av gruppekommunikasjon, eller være et planlagt nettverk av møtepunkter som endemottakere kobler seg opp mot. Forskjellen ligger i dynamikken til møtepunktene. Hvis endemottakerne også er møtepunkter og på den måten med i distribusjonsnettverket, så vil distribusjons-nettverket endre seg med antall mottakere som melder seg på og av. Derimot, med et planlagt distribusjonsnettverk hvor endemottakerne ikke er med, vil distribusjonsnettverket være mer statisk og på den måten mer forutsigbart. Begge metodene har sine fordeler og ulemper.

Innenfor informasjonsinfrastrukturen blir møtepunktene i noen tilfeller også brukt til mellom-lagring av informasjon. Det vil si, produsenter skyver ut kopier av informasjonen til flere geografiske lokasjoner. Mellomlagringslokasjon og informasjonsoverføring kan da bestemmes utfra planlagt informasjonsutveksling. Gevinsten er redusert last på nettverket rundt informasjonsprodusent, og sluttbrukerne kan nå informasjonen raskere, gitt at mellomlagringslokasjon befinner seg nærmere enn dataprodusent. Denne måten å organisere informasjon blir ofte betegnet som strukturert informasjonsdeling. CDN er et eksempel på strukturert informasjonsdeling av informasjon på Internett. Typisk bruk av CDN er tv-programmer og nyheter. Katalogsystemene sørger for å koble bruker til den nærmeste mellomlagringsplassen.

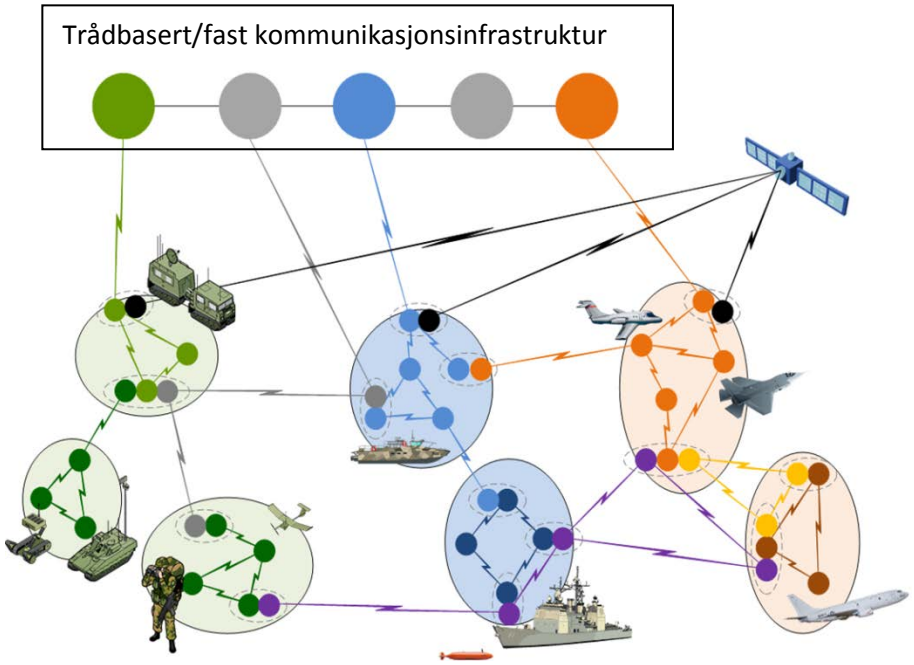
Ad hoc-informasjon, i motsetning til strukturert informasjon, er informasjon som en ikke vet at en vil trenge ved planlegging av kommunikasjonsinfrastruktur og informasjonsdeling. Ad hoc-informasjon er derfor informasjon som må distribueres uten en skreddersydd informasjons-distribusjonsmekanisme. Informasjonen kjennetegnes ved at den hentes ved kilden eller søkes opp.

Én av utfordringene med strukturert informasjonsdeling i mobile militære nettverk er planleggingen av lokasjon for mellomlagring. I motsetning til stasjonære nettverk, beveger enhetene seg i mobile nettverk og plassering av data vil variere med mobilitet og operative behov. I tillegg til plassering er utfordringen gitt ved hvilken informasjon som skal utplasseres, til hvilken tid og over hvilke informasjonsbærere.

Nytteverdien av strukturert informasjonsdeling vil bero på faktisk forespørsel av data. Strukturert deling av informasjon vil derfor kunne ses på som mer nyttig innenfor stasjonære og strategiske nettverk, som har høyere kapasitet, enn innen mobile militære nettverk. I et militært mo-bilt nettverk vil nytten ikke nødvendigvis stå i forhold til ressursbruken. Konsekvensen er at en større andel informasjon trolig vil bli kategorisert som ad hoc-informasjon og må søkes opp ved behov.

3.2 Økt sannsynlighet for ustabile nettverk

Fremtidens mobile militære nettverk er utfordret med behov for høyere datarate og samhandling over store avstander. For å kunne imøtekomme denne utfordringen, vil trolig nettverkene bli bygget ved bruk av ulike radioteknologier i et såkalt heterogent nettverk. Styrken med heterogene nettverk er robusthet, økt evnen til å kommunisere over avstand og utnytte høykapasitetslinker når disse er tilgjengelig slik som illustrert i figur 3.1. Ulempen er at sammenkobling av ulike radioteknologier medfører økt utfordring med stabilitet. Med IP er vi avhengig av en stabil rute mellom sender og mottaker innenfor tiden tjenesten skal utveksle informasjon. Med stabil rute mener vi en vei igjennom nettverket med få feil når det gjelder endring av topologi, tap av trafikk og endring av tilgjengelige overføringsressurser. Fremtidens mobile militære nettverk basert på heterogene nettverk vil trolig ha økte utforinger med stabilitet grunnet store forskjeller i kommunikasjonsteknologi og økt mobilitet. Med EK-trussel blir situasjonen trolig verre grunnet aktiv nettverksforstyrrelser. Vi vil i de neste to delkapitler gi et innblikk i hvordan elektronisk krigføring og heterogene nettverk gjør det utfordrende å bruke IP.



Figur 3.1 *Heterogent maskenettverk med flere alternative veier mellom hver bruker. Ulike radiokommunikasjonsteknologier er brukt for sammenknytning av ulike militære enheter. Fargene indikerer radioteknologi, dvs. ulike farger betyr ulike radioteknologier. Sirklene angir lokale nettverk. I figuren er ulike radioteknologier bundet sammen ved hjelp av ruting. Ulike teknologier gir ulike egenskaper i form av rekkevidde og datarate.*

3.2.1 Nettverksutfordringer relatert til økt EK-trussel

EK har alltid vært en utfordring for trådløse kommunikasjonssystemer. I de senere årene, har EK blitt kjent brukt i østre Ukrainia og Syria [26]. Virkningen av EK kan gi begrenset kommunikasjonsmulighet, enten over lengre tid eller sporadisk, eller i ytterste grad bortfall av evne til kommunikasjon. Fremtidens kommunikasjonsnettverk må derfor kunne tilpasse seg en forventet høy dynamikk. Når kommunikasjonsressurser blir redusert må nettverket og tjenestene kunne tilpasse seg.

En økende EK-trussel kan møtes med flere mottiltak. Ett mulig mottiltak er å benytte flere alternative transmisjonsteknologier for å redusere konsekvensen av utfall av én transmisjons-teknologi. Med dette mottiltaket, så vil noen av utfordringene med tilgjengelighet flyttes fra radio og over til nettverk og ruting. Nettverket vil bli mer dynamisk og må tilpasse seg endringene som måtte oppstå. Utfordringen ligger i dynamiske nettverk og andel feil. I dynamiske mobile nettverk er «feil» en normalsituasjon i motsetning til i stasjonære nettverk. Midlertidig brudd på tilgang til en tjeneste må derfor forventes.

3.2.2 Kommunikasjon over heterogene nettverk

I fremtiden forventer vi at Forsvaret vil ha behov for samband over både lang og kort avstand, høy datarate samt sømløs kommunikasjon mellom militære enheter uavhengig av forsvarsgren og våpenart som illustrert i figur 3.1.

Sammenkobling av flere ulike transmisjonssystemer til ett felles heterogent nettverk er et aktivt forskningsfelt i dag. Det er spesielt en utfordring å bygge slike nettverk med IP-arkitekturen [15]. Utfordringen ligger i det å få et heterogent nettverk til å vedlikeholde et tidsriktig bilde av topologien til enhver tid. Med ulike teknologier, signalfeil, mobilitet m.m, øker sannsynligheten for at forskjellige deler av nettverket besitter ulikt syn over topologien som igjen fører til økt sannsynlighet for inkonsistente rutebeslutninger. Inkonsistente rute-beslutninger kan føre til et ustabilt nettverk.

God utnyttelse av mobile heterogene nettverk vil kreve informasjonsinfrastruktur og kommunikasjonsinfrastruktur som i større grad enn i dag evner å kunne tilpasse seg hverandre. Tradisjonell fremgangsmåte, hvor informasjonsinfrastruktur og kommunikasjonsinfrastruktur i stor grad er individuelt rendyrket, vil trolig i mindre grad føre til god utnyttelse av et mobilt heterogent nettverk. Fremtidige tjenester og nettverk må derfor i større grad samarbeide om å søke etter informasjon og tjenester. Nettverk med støtte for søk etter informasjon vil derfor trolig øke i fremtiden som en konsekvens av det å kunne operere over heterogene nettverk og samtidig imøtekomme EK-trussel.

3.3 Behov for autentisering av data

I IP-nettverk i dag autentiseres i hovedsak endepunktene som utveksler informasjon, uavhengig av informasjonens faktiske opprinnelse. Dette gjøres ved å verifisere identiteten til

endepunktene gjennom sertifikater eller delte hemmeligheter, for deretter å etablere en sikker tunell som bare kan brukes av de autentiserte endepunktene. Informasjonen som benytter tunellen er derfor ikke direkte autentisert, men dens integritet og konfidensialitet beskyttes når den overføres mellom endepunktene. Det finnes flere måter å etablere slike tuneller hvor IPsec [21] og TLS [22] er kanskje de mest kjente metodene. Metodene virker for mer eller mindre statiske omgivelser hvor endepunktene ofte også er stedet hvor informasjonen var generert og infrastrukturen kan håndtere utstedelse, håndtering og distribusjon av de nødvendige sertifikatene eller hemmelighetene.

I omgivelser hvor enheter er mobile, hvor informasjonen kanskje må mellomlagres underveis på vei til konsumenter, eller hvor ukjente noder kan være involvert i transaksjoner vil denne type løsning ikke gi tilstrekkelig tillit. Et mulig alternativ, kan da være å autentisere selve informasjonen, uavhengig av endepunktene som utveksle den. En mulig tilnærming er allerede blitt foreslått, blant annet i NATO-sammenhenger der den refereres til som datasentrisk sikkerhet. Hovedidéen er å merke informasjon med metadata som sier noe om, for eksempel hvor informasjonen kommer fra, hvem som produserte dem, hvem som har lov til å bruke den og hvordan. Metadataene skal da bindes på en sikker måte til informasjonsobjektene de refererer til, slik at de kan brukes til å autentisere informasjonen uansett hvor den skulle ligge eller komme fra. Selv om konseptet i seg selv er ganske enkelt, ligger problemet i hvorvidt det er mulig å håndtere selve autentiseringsprosessen i den gitte infrastrukturen. Konseptet vil treffe lignende utfordringer som med sertifikathåndtering for autentisering av endepunktene.

3.4 Økt behov for informasjonsoverføringen

Det er vår oppfatning at informasjonsoverføringen i mobile militære nettverk vil øke blant annet som en følge av innføring av flere sensorer. Kapasitet i trådløse nettverk er, og vil fortsette å være begrenset sammenlignet med trådbaserte nettverk. En økning av kapasiteten kan løses på to forskjellige metoder: 1) økt radio datarate, det vil si anskaffelse av radioer med høyere datarate og/eller 2) bedre utnyttelse av eksisterende nettverksressurser. IP-arkitekturen har utfordringer med begge disse løsningsområdene i form av nettverksstabilitet og utnyttelse av nettverksressurser. Vi vil beskrive nærmere hvordan utfordringene gir seg til kjenne.

3.4.1 Økt radio datarate

Behov for økt nettverkskapasitet blir tradisjonelt besvart med å anskaffe transmisjons-teknologier som tilbyr høyere datarate. Utfordringen med en økning i datarate er sammenhengen mellom datarate og transmisjonsdistanse. Som en tommelfingerregel er datarate omvendt proporsjonalt med transmisjonsdistansen. En konsekvens av å øke dataraten er derfor et økende behov for reléfunksjonalitet. I trådløse dynamiske nettverk er økning av antall relé mellom produsent og konsument assosiert med økt sannsynlighet for ustabilitet og tap av overført informasjon. Det er derfor viktig å søke andre løsninger for økt datarate. Hvordan radio-ressursene utnyttes for utveksling av informasjon vil derfor være vel så viktig. Spesielt viktig vil det være for fremtidige militære mobile nettverk hvor informasjonen er ment for flere, men ikke nødvendigvis på samme tid.

3.4.2 Bedre utnyttelse av eksisterende nettverksressurser

I situasjoner hvor flere ulike brukere ønsker samme informasjon, vil hver bruker innhente sin egen kopi av informasjon. I et IP-nettverk vil IP-pakken gjenkjennes med IP-adresser, men det er ingen mulighet for å utrykke innholdet i datapakken. Løsningen på utveksling av innhold uten å sende selve informasjonselementet, er blant annet ved bruk av metadata i dagens systemer. Metadata hjelper til med å redusere datamengden, men har begrenset mulighet til å redusere deling av selve informasjonen mellom flere mottakere uten støtte funksjonalitet som igjen ligger utenfor IP.

I nettverk hvor majoriteten av trafikken skal ut til flere, eller er av interesse for flere, vil et godt nettverksdesign ivareta en fleksibel overgang mellom unicast og multicast og samtidig ivareta robusthet. IP-arkitekturen er utfordret med hensyn på denne fleksibiliteten. Vi har i dag ikke noen gode løsninger som kan bevege seg sømløst mellom unicast og multicast med innebygget robusthet basert på omgivelsene. Med omgivelser, menes for eksempel tjenester som benytter unicast ved få brukere og multicast ved mange brukere.

3.5 Økt nettverkskompleksitet

Problemet med IP er ikke at det ikke finnes funksjonalitet for et bestemt scenario. Problemet ligger i kompleksitet og konfigurering. Over tid er det foreslått en mengde nye protokoller som adresserer ulike behov for ulike scenario. Disse protokollene er imidlertid ikke godt samordnet og tilpasset hverandre.

Internet Engineering Task Force (IETF), som er de facto standardiseringsorgan for Internett, har utviklet en rekke standarder for å adressere nye nettscenarier og tilhørende funksjoner. Som et eksempel er det standardisert en separat protokollstakk for ustabile nett med høy forsinkelse med betegnelse Delay Tolerant Networking (DTN). Hvis vi i dag ønsker å utnytte mellomlagring av informasjon internt i et DTN nett, så er dette adressert gjennom DTN og funksjonalitet i HTTP[2] proxy[3].

Med IP-mellomlagring og DTN er det en forutsetning at HTTP brukes for informasjons-utveksling og at proxy-nodene alltid har en optimal plassering. Tjenester som skal kjøre over ustabile nettverk med høy forsinkelse må da utvikles med HTTP proxy-funksjonalitet. Samtidig må kunnskap om hvor en proxy skal plasseres være ivaretatt for en god utnyttelse. Denne kunnskapen vil ikke nødvendigvis være tilstede i dynamiske miljøer.

[2] Hypertext Transfer Protocol (HTTP) er metoden eller språket som blir brukt for distribuerte, samarbeidende, hypermedia-informasjonssystemer. HTTP er grunnlaget for datakommunikasjon for World Wide Web, hvor hypertekstdokumenter inneholder hyperkoblinger til andre ressurser som brukeren enkelt kan få tilgang til, for eksempel med et museklikk eller ved å trykke på skjermen. HTTP ble utviklet for å lette hypertekst og World Wide Web.

[3] En proxy-server er en server/tjener som er plassert mellom datamaskinen som etterspør data og serveren som besitter etterspurt data. Proxy-servere er brukt innen flere områder, men er ofte assosiert med funksjonalitet for økt ytelse ved å avlaste noden hvor tjenesten kjøres. Klienter vil da forespørre proxy i stedet for å gå hele veien inn til noden som kjører tjenesten.

Med IP-arkitekturen har vi i dag flere muligheter for å kommunisere under forskjellige omgivelser. Et utvalg av muligheter er mellom en enkelt sender og en enkelt mottaker (unicast), gruppekommunikasjon (multicast) og en tjeneste for nettverk med høy forsinkelse gitt ved DTN. Felles for alle disse metodene er egne tilpasninger eller knytninger mellom tjenesten og nettverk. Det vil si, tjenester utvikles i hovedsak for én av de tre kommunikasjonsmetodene og er ikke utviklet generisk. Hvilken metode som bør brukes kan noen ganger enkelt foreslås utfra generiske betraktninger, men er ofte mer utfordrende fra situasjon til situasjon uten kunnskap om forventet EK-trussel, kapasiteten til nettverket, trafikksituasjon og mobilitet. På grunn av den sterke knytningen mellom tjenesten, transport og nettverk tilbyr IP-arkitekturen mindre fleksibilitet i det å endre kommunikasjonsmetode mellom unicast, multicast og DTN eller å bruke dem i kombinasjon. Med IP-arkitektur er det også utfordrende å dele informasjon mellom informasjonstjenester.

4 Information Centric Networking

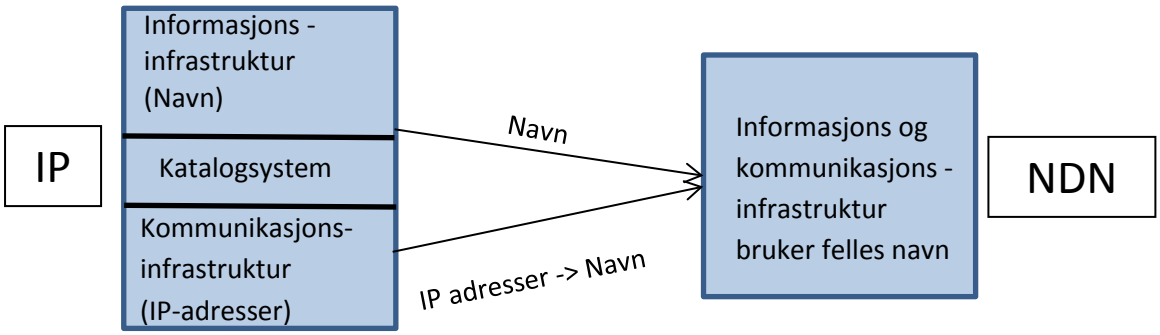
I dette kapittelet har vi valgt å forklare virkemåten til ICN på en overordnet måte. Det finnes et utvalg av designforslag under paraplyen ICN [3], hvorav Named Data Networking (NDN) er ett av disse. Når vi skal illustrere bestemte mekanismer bruker vi NDN-arkitekturen [2]. NDN har sitt utspring fra Van Jacobsen og Parc sin ICN-implementasjon, Content Centric Networking (CCN) [4]. Vi har valgt å fokusere på NDN, siden NDN har fått god støtte fra både industri og sivil forsking og har i tillegg et aktivt utviklingsmiljø.

NDN setter selve informasjonselementet i sentrum. Dette står i kontrast til IP, som adresserer endenodenes IP-adresser og ikke selve informasjonselementet. En IP-pakke er på mange måter en konteiner med adresseinformasjon for hvor den kommer fra og hvor den skal, men innholdet er ukjent. NDN er bygget rundt navngitte data hvor konteineren er gitt ved navn og ikke kilde eller mottakeradresse. Navnet på konteineren gir til kjenne innholdet av informasjon og informasjonen kan da enklere deles mellom flere som etterspør samme navngitte informasjon. Et informasjons element, eller en konteiner, må derfor i denne sammenheng være gitt med et unikt navn.

En annen fordel med navn gitt ved innhold istedenfor en IP-adresse gitt ved lokasjon er skalering av navnerommet som da ikke er endelig, i motsetning til IP-adresser i IP-arkitekturen. Når det gjelder navn, finnes det flere forslag for hvordan navn kan organiseres. Én tilnærming er hierarkisk navnestruktur som igjen deler mange likheter med hvordan navn brukes på Internett, for eksempel i DNS. Et eksempel på et navn kan være:

OperasjonXX/GeografiskOmrådeXX/StyrkeXX/effektorXX

Med NDN, så er vi mindre avhengig av katalogsystemer siden et felles navnesett er brukt innenfor informasjonsinfrastruktur og kommunikasjonsinfrastruktur som illustrert i figur 4.1. NDN sin bruk av navn vil ha en annen virkemåte for overføring av data enn ved IP. Overordnet, så er NDN orientert rundt søk etter informasjon.



Figur 4.1 Med IP, er informasjonsinfrastruktur og kommunikasjonsinfrastruktur fraskilt i to deler og bindeleddet er katalogsystemer. NDN har felles navn og har derfor mindre behov for katalogsystemer.

Med NDN, så vil ruting gi deg veien mot etterspurt navngitt informasjon. En annen egenskap ved NDN er mellomlagring av informasjon. Med NDN kan alle noder mellomlagre informasjon og derav videre besvare forespørsler. Hvem som opprinnelig produserte den etterspurte og levert informasjon verifiseres ved hjelp av signering. Det vil si, med NDN vil mottakeren av et informasjonselement kunne autentisere tjenesten som produserte informasjonen samtidig som informasjonselementets integritet sjekkes uavhengig av hvor informasjonen var hentet fra. Med denne egenskapen kan informasjon enklere deles, data kan lagres og hentes fra vilkårlige mellomlagringsplasser. Bruken av nettverksressursene blir derfor mer og mer optimalisert med økende informasjonspopularitet.

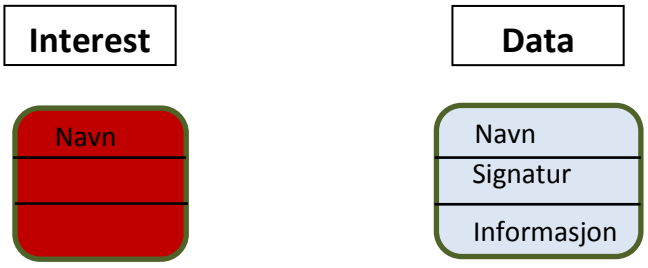
NDN sin bruk av mellomlagring og signering gjør at NDN ikke skiller mellom utveksling av unicast, multicast/CDN og har samtidig støtte for Delay Tolerant Networking. NDN har som mål å kunne tilby de samme funksjonene som tilbys med dagens IP-arkitektur like bra eller bedre, men med mindre kompleksitet.

4.1 ICN eksemplifisert ved Named Data Networking (NDN) – hvordan virker NDN på prinsipielt nivå?

Det er fire elementer ved NDN som skiller seg fra tradisjonell IP-arkitektur. I de følgende underkapitlene vil vi kort beskrive forskjellene.

4.1.1 To sentrale meldingstyper i NDN

NDN er basert på søk etter bestemt informasjon gitt ved navn. For utveksling av informasjon så er NDN orientert rundt to nettverkspakker som vist i figur 4.2 - én Interest-pakke og én Data-pakke. Interest brukes for å etterspørre ønsket informasjon gitt ved navn. Data er pakken som inneholder selve informasjonen, og som besvarer Interest-pakken.



Figur 4.2 Interest Name er navnet på data/informasjon som etterspørres. Name på Data-pakken er navnet på etterspurt informasjon og tilsvarer navnet som er brukt i Interest. Informasjon er selve dataen eller informasjonen som er etterspurt. Signatur er en signatur som knytter navn til data. En mottaker kan med signatur verifisere (data, datanavn) mot avsender.

Til forskjell fra IP-arkitekturen har ikke Interest en IP-adresse som angir lokasjonen hvor pakken skal, eller kilden hvor den kom fra. Derimot utrykker den interesse for ett spesifikk

informasjonselement. Som et resultat er etterspørselen etter informasjon ikke bundet til destinasjon gitt av lokasjon i nettverket, og en vilkårlig nettverksnode som besitter etterspurt informasjon kan svare.

Siden en vilkårlig node som besitter etterspurt informasjon kan svare, kan det komme flere svar på en Interest hvis man velger å sende Interest samtidig over flere veier. I NDN er styringen av Interest, og derav også hvem som kan svare på Interest bestemt av strategi. Strategi gir føring for hvordan Interest skal håndteres i nettet med hensyn på videresending. Ulike navn-områder kan ha ulike strategier. Med navn-område menes typisk ulike navn prefix slik som operasjonXX, eller operasjonXX/avdelingXX. Prefix i NDN deler mange fellestrekk med IP-maske i IP. Ulike navn områder kan ha ulike strategier og derav ulik oppførsel i nettverket. En Interest kan derfor videresendes på ett eller flere radiogrensesnitt eller kastes, basert på en strategi innenfor et navn område.

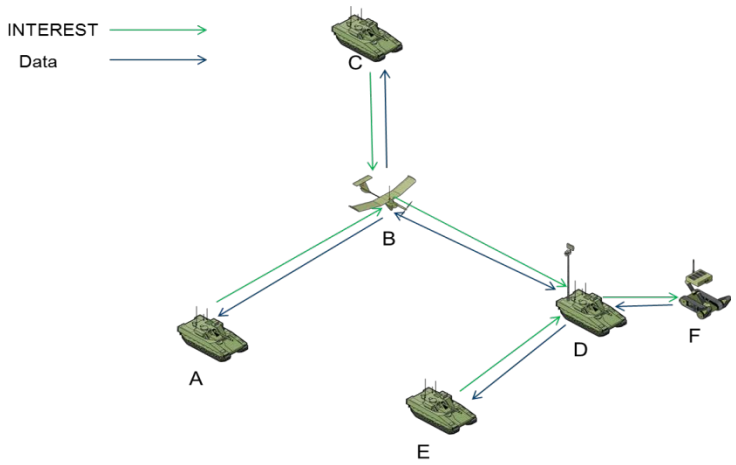
4.1.2 NDN er basert på tilstandsfull forwarding

NDN lagrer tilstand og er tilstandsfull, i motsetning til IP som er tilstandsløs. Med tilstandsfull menes her at hver ruter som mottar en Interest lagrer, blant annet, informasjon om hvilke kommunikasjonsmedium Interest ankom på. Hver NDN-node vil derfor ha en peker tilbake til forrige node etter hver mottatt Interest. Med andre ord, en Interest-melding vil legge igjen en rød tråd i nettverket tilbake til den som etterspurte informasjonen (konsument). Når en Interest ankommer en node som innehar etterspurt data, sendes informasjon tilbake langs den røde tråden. Den røde tråden slettes etter at datapakken har passert. Data i NDN vil således alltid følge samme vei som Interest bare i motsatt retning.

I NDN etableres den røde tråden per datapakke og slettes når datapakken er sendt videre. I NDN vil en Interest typisk aldri etterspørre et informasjonselement som er større enn hva som støttes av linkteknologi, typisk 1500 bytes. Fordelen med små dataelementer er flere. I ustabile nett-verk er fordelen at topologiendringer oppdages raskt. Med NDN oppdages topologiendringer per datapakke i motsetning til i IP som må vente på at ruting-funksjonaliteten oppdager endringen. En av utfordringene med IP i denne sammenhengen er at tiden for feildeteksjon kan være lang, og synkronisering av feildeteksjon vil i mange situasjoner være vanskelig, eller vil kreve lang tid som igjen medfører ustabilitet. IP er avhengig at alle nettverkselementene har et synkronisert syn på nettverket for å unngå rute loops. Med NDN, så kan en Interest oppleve en rute-loop, men denne vil bli detektert og stoppet. Data vil aldri inngå i en rute-loop. En annen fordel er gjenbruk av informasjon. Med små informasjonselementer er mulighetene for gjenbruk større, fordi små og kjente informasjonselementer kan kombineres på flere måter enn få store og mer skreddersydde informasjonselementer.

Figur 4.3 illustrerer mulig bruk av NDN i en militær sammenheng. Det er verdt å merke seg at radiobærerne som her er vist ikke er basert på et kringkastingsmiljø[4], men direkte radiolinker.

[4] Kringkastingsmiljø i denne sammenheng er hvor avsender sender en melding og hvor alle som er innenfor radio-rekkevidde av avsender mottar samme melding.



Figur 4.3 *Et mindre taktisk nettverk som belyser virkemåten til NDN. Node A etterspør informasjon fra autonom node F. En Interest blir sendt ut, og mot, node F basert på ruting. Interest når B (UAV) og blir videresendt til D før Interest når F. Både B og D lagrer over hvilke radiobærere Interest ankom og sendt. Interest fra A og på vei til F legger på denne måten igjen et spor hvor den har gått, eller med andre ord en «rød tråd». Etterspurt informasjon blir så sendt tilbake langs veien Interest etablerte på veien til F. Siden informasjon blir mellomlagret kan C på et senere tidspunkt hente mellomlagret informasjon hos B, og E kan hente informasjon hos D, uten å gå hele veien til F.*

4.1.3 NDN og distribuert mellomlagring

Mellomlagring (caching) er en innebygget funksjon i NDN i motsetning til i IP. I NDN vil alle noder som kjører NDN kunne mellomlagre informasjon. Størrelsen på mellomlageret på hver node er ikke bestemt eller anbefalt av NDN, men vil være avhengig av type trafikk og omgivelser. Konsekvens av små lagringsenheter er at informasjon med økt sannsynlighet må hentes nærmere data produsent.

Når det gjelder forskjell i caching mellom IP og NDN er det små forskjeller i selve lagringen av data. Forskjellen ligger på organiseringen av mellomlagringen. Den store forskjellen ligger i tilliten til enhetene som tilbyr mellomlagring. I et IP-nett er tilliten til informasjon knyttet implisitt til tilliten til noden i nettverket som mellomlagrer informasjonen. Det vil si, tilliten til et informasjonselement som er mellomlagret arver tilliten til noden som tilbyr mellomlagring. I et NDN-nettverk, derimot, er ikke informasjon knyttet til enheten som mellomlagrer, men tilliten til informasjon er en del av selve informasjonselementet. Hvert informasjonselement innehar tillit ved å være signert av den som opprinnelig produserte informasjonen. Signering av hvert informasjonselement gir mottaker mulighet til både å autentisere dataprodusenten, og å kontrollere at informasjonselementet ikke har blitt endret på veien fra produsent til konsumer.

Siden informasjon er navngitt og signert, kan lokalt mellomlagret data bli besvart med Interest fra andre konsumenter. Mellomlagring av informasjonselementer er derfor et viktig element i

arkitekturen. Samtidig er det ikke nødvendigvis begrensende, siden minne blir større og billigere, og strategier for utskifting av informasjon i mellomlagring er et veletablert felt.

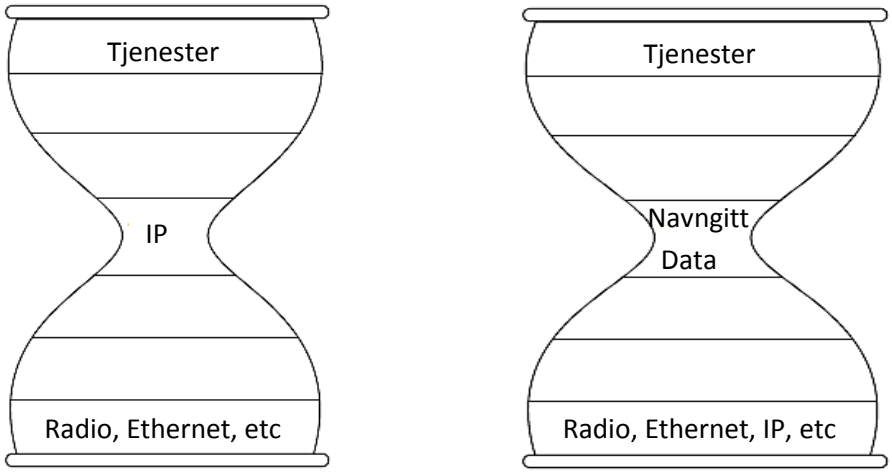
4.1.4 NDN-sikkerhet

NDN bruker signering på informasjonselement, dvs hver Data-pakke som vist i figur 4.2. I NDN er det påkrevd at hver Data-pakke kryptografisk signeres. Interest-pakken kan signeres, men det er ikke et krav. Som et resultat kan hver mottaker av signerte pakker verifisere integriteten til pakken og produsenten av informasjonen uavhengig av lokasjon til hvor dataen ble hentet fra.

Kryptering av informasjonsinnhold er ikke påkrevd i NDN, men bestemmes av hver tjeneste-utvikler. Hvorvidt selve informasjonen er beskyttet med kryptering eller ikke, begrenser ikke arkitekturen. Siden hvert informasjonselement har både autentisering og integritetsbeskyttelse, kan det hentes fra enhver nettverksnode. Annen sikkerhetsfunksjonalitet må implementeres utenfor ICN eller som tilleggsfunksjoner.

4.2 NDN og IP - Overordnet sammenligning

For å få et overordnet bilde av hvordan NDN virker sammenlignet med IP, sammenligner vi timeglass fremstillingen av IP med timeglass fremstillingen av NDN i figur 4.4.



Figur 4.4 Timeglasset hvor IP står som sentrum for IP-arkitekturen, sammenlignet med timeglasset for NDN hvor navngitt data står i sentrum.

Hovedforskjellen ligger i hvordan man adresserer data. Det er verdt å legge merke til hvor IP er plassert og brukt i timeglasset til NDN. IP er plassert på lik linje med Radio og Ethernet. Det betyr at NDN kan kjøre over alle bærere som kan flytte informasjon slik som med Bluetooth, Ethernet eller IP. NDN kan derfor kjøres over IP, og IP kan kjøres over NDN. Denne egenskapen var én av suksessfaktorene for overgangen fra telefoni og linjesvitsjing til IP. NDN

kan på denne måten gradvis utforskes og eventuelt gradvis introduseres i Forsvaret på eksisterende nettverksutstyr. Dette kan gjøres ved å kjøre NDN i områder hvor det er funnet hensiktsmessig.

5 Hvordan ICN/NDN imøtekommer identifiserte utfordringer i mobile militære kommunikasjonsnettverk

Utgangspunktet for dette kapittelet er utfordringene listet i kapittel 3 for fremtidige mobile militære nettverk. Vi vil her besvare på et overordnet nivå hvordan ICN/NDN kan imøtekomme disse utfordringene.

5.1 NDN-arkitekturen og effektiv gruppekommunikasjon

I NDN er informasjon gitt ved navn, og navn blir brukt både på tjeneste- og nettverksnivå. Skillet mellom kommunikasjons- og informasjonsinfrastruktur blir derfor mindre. Tjenester og nettverk får en felles del, her gitt ved navn, og behov for krysslagsteknologier mellom tjenester og nettverk vil bli mindre.

I NDN-arkitekturen skilles det ikke mellom multicast (gruppekommunikasjon) og én-til-én (unicast) kommunikasjon. Det er derfor ikke behov for egne metoder og protokoller for utveksling av multicast og unicast. Effektiviteten og utnyttelsen av nettverksressursene i NDN er derfor potensielt høyere enn i et IP-nett. Konfigurering vil også være enklere, siden det ikke er noe skille.

NDN-arkitekturen skiller ikke mellom ad-hoc informasjonsinnhenting og strukturert informasjonsinnhenting som var listet som en av utfordringene med IP arkitekturen i kapittel 3.1. Det vil derfor være mindre behov for å etablere et strukturert nettverk med mellomlagring, siden distribuert mellomlagring er en del av arkitekturen. Med NDN ligger ulikheten i tilgang på informasjon på sannsynligheten for at en nærliggende node har mellomlagret den etterspurte informasjonen.

5.2 NDN-arkitekturen og økt sannsynlighet for ustabile mobile militære nettverk

NDN-arkitekturen har noen egenskaper som gjør den potensielt bedre utrustet til å løse utfordringene ved ustabile nettverk enn IP-arkitekturen. Vi vil i dette delkapittelet se på hvordan NDN imøtekommer utfordringene.

5.2.1 ICN-arkitekturen og nettverksutfordringer relatert til økt EK-trussel

I mobile taktiske nettverk er ICN, i motsetning til IP, mindre avhengig av en sammenhengende og tilgjengelig rute mellom datakonsument og dataprodusent. ICN, vil derfor trolig være mer robust mot EK-trussel enn med IP. Årsaken til dette er NDN sin ustrakte bruk av mellomlagring, tilstandsfull *forwarding* og mulighet for søk etter data. Med et midlertidig linkbrudd nær en konsument i ICN, grunnet for eksempel EK-jamming, har dataen allerede blitt

flyttet nærmere konsumenten. Dataen kan derfor bli hentet fra den nærmeste enhet som da har mellomlagret dataen. Et eventuelt nytt linkbrudd mellom dataprodusent og noden som har mellomlagret informasjon har derfor ingen betydning. NDN er derfor mindre avhengig av tilgjengelig ende-til-ende forbindelse mellom datakonsument og dataprodusent for overføring av data, men trenger isteden kun forbindelse til nærmeste mellomlagringslokasjon. For populært innhold er det forventet at informasjonen raskt blir mellomlagret nær nye interessenter.

5.2.2 ICN-arkitekturen og kommunikasjon over heterogene nettverk

ICN er mindre avhengig av et nettverk med felles bilde av nettverkstopologien fordi selve data-forwardingen ikke er basert på topologiinformasjon, men kun følger veien som Interest brukte (tilstandsfull forwarding). For å håndtere at samme Interest kan ha brukt ulike veier, blir duplikater filtrert ut via bruk av Nonce[5]. En Interest som kommer til en node for andre gang vil bli gjenkjent og behandlet deretter.

ICN fokuserer på det å finne informasjon og ikke lokasjon. I et dynamisk nettverk vil nettverket endre seg over tid, og mulighet for å indentifisere når nettverket endrer seg er viktig. Med NDN sin bruk av tilstandsfull forwarding vil en endring i nettet bli oppdaget så snart det ikke kommer Data tilbake etter sendt Interest. IP, derimot, vil fortsette å sende trafikk basert på foreldet ruteinformasjon og må vente på at rutekontrolltrafikken oppdager endringen i nettet og oppdaterer ruteinformasjonen. NDN er derfor potensielt bedre egnet til å operere i ustabile heterogene nettverk.

Kommunikasjon over ustabile nettverk trenger økt robusthet slik som med mobile heterogene nettverk. Standard rutemetode i IP-nettverk er å begrense antall linker som kan brukes for å eliminere problemet med rute-loops. Som en konsekvens, etableres det kun én vei til hver destinasjon eller flere veier, men da med lik kost. Kost i denne sammenheng kan være antall hopp, båndbredde eller tilsvarende. Dersom dette ikke er tilstrekkelig på grunn av robusthet, må tjenesten eller mellombokser velge å utveksle kopier av pakker for å øke robustheten. For kommunikasjon over lengre avstand, dvs. over et heterogent nettverk, er dette ikke tilstrekkelig på grunn av ulike radioegenskaper i forskjellige deler av det heterogene nettverket.

Med ulike tjenester, så følger ulike behov. Det vil derfor være ønskelig å kunne søke etter informasjon via flere veier basert på ytelse eller behov for en spesifikk tjeneste/navn-segment basert på alle tilgjengelige linker. Denne typen dynamikk er mulig i et ICN-nettverk, men med en ekstra kostnad i form av økt Interest og Data trafikk. Med NDN kan avgjørelsen om bruk av én eller flere veier velges mer dynamisk og alle linker kan potensielt prøves ut.

5.3 ICN-arkitekturen og behov for autentisering av data

I større nettverk, særlig nettverk med ubemannede sensorer, vil autentisering av data være viktig. Som beskrevet i 4.1.4 er all data signert i ICN/NDN. Mottaker kan derfor verifisere

[5] Unikt nummer som kan brukes som identifikasjon av en pakke.

produsent av informasjon uten å være avhengig av å etablere tunneler. En av utfordringene for militære omgivelser i denne sammenheng er nøkkelhåndteringen. Dette problemet er ikke relatert til NDN alene, men gjelder også IP. En utfordring med NDN ligger også i gevinsten av å bruke NDN, dvs signering av informasjon på tjenestenivå. Utfordringen ligger i skalering av nøkkelhåndtering og ekstra generert trafikk som følge av at all pakkebasert Data er signert.

5.4 ICN-arkitekturen og økt behov for informasjonsoverføring

Tilgjengelig datarate i et nettverk beror på flere faktorer. I kapittel 3.4 ble utfordringen med økt datarate plassert innunder to delproblemer: link/radio-kapasitet og nettverkets evne til å utnytte nettverksressursene. I denne seksjonen ser vi på ICNs arkitektur og dens evne til å utnytte nettverksressurser.

Utfordringen med bruk av radioteknologier med økt datarate er ofte kortere radiorekkevidde med tilhørende utfordringer med nettverkstabilitet. For å få økt datarate så må det i mange tilfeller anskaffes flere radioer grunnet kortere radio rekkevidde. Innføring av flere radioer er forbundet med økte kostnader. Derimot er kostnaden for økt mellomlagringskapasitet til nettverksnodene langt lavere. NDN legger opp til bedre ressursutnyttelse i nettverket ved å utnytte mellomlagring i nettverket på en bedre måte enn hva IP gjør. Ved bruk av mellomlagring og utstrakt deling av informasjon, vil behovet for datarate reduseres med andel trafikk som kan deles. Behovet for anskaffelser av nye radioer som en konsekvens av økt datarate kan derfor i noen tilfeller reduseres.

Med NDN vil det være mindre behov for å skille mellom strukturert og ad-hoc deling av informasjon. Informasjon er ikke distribuert før noen etterspør, og distribueres kun i det tidsrommet informasjon er etterspurt. Det er således ingen skaleringsproblemer med antallet sensorer, men kun mot hva linkene/radioene setter av begrensing. Linkkapasitet er uavhengig av arkitektur.

5.5 ICN-arkitekturen og økt nettverkskompleksitet

En tjeneste i et militært nettverk under IP-arkitekturen må designes for å kunne forholde seg til ulike protokollstakker avhengig av operasjon og operasjonsomgivelser. Som et eksempel må en felles tjeneste skrives og utformes for bruk enten for DTN, stasjonære nettverk eller for mobile militære nettverk. Disse miljøene er forskjellige og trenger egne tilpasninger. NDN derimot er designet rundt søk etter informasjon, og alle tjenester vil ha støtte for DTN, unicast og multicast. Tjenestene som benytter nettverket vil ha et generisk grensesnitt ned mot nettverket og vil være mindre avhengig av spesialtilpasninger med hensyn på underliggende nettverksmetoder á la DTN. Tjenestene selv må håndtere om informasjonselementet ikke finnes, forsvant på veien eller kom til rett tid. Imidlertid er dette en funksjonalitet noen tjenester må eller bør ha, uavhengig av arkitektur og om det finnes en pålitelig transportmekanisme á la TCP eller ikke.

6 ICN og NDN i fremtidens mobile militære nettverk – hvilke utfordringer bør adresseres videre

ICN-arkitekturen har flere interessante egenskaper som potensielt kan løse noen av utfordringene med å etablere robuste mobile militære nettverk i fremtiden. I likhet med mange andre arkitekturer, har designvalgene til ICN og NDN noen utfordringer som bør utforskes videre før NDN kan sies å være moden nok til å kunne bli benyttet i en militær setting. Noen av disse har fått mye forskningsfokus som igjen har generert flere mulige løsninger, mens andre utfordringer ikke har blitt viet like mye oppmerksomhet.

En av de viktigste utfordringene er knyttet til design av navnestrukturen [27]. Det må på plass en navnesemantikk som gjør det mulig for både dataprodusenter og datakonsumenter å navngi informasjonen samstemt. Denne strukturen må kunne være skalèrbar. I militære nettverk tror vi dette kan løses lettere, siden både organisasjon og informasjon allerede, langt på vei, er godt strukturert med navn. I tillegg er mengden informasjonselementer som trenger unike navn trolig mindre enn i Internett. Sammenkobling av flere nettverk med ulike eiere vil kreve enighet om navnestruktur og ruting samtidig som nøkkelutveksling må på plass. Det er nødvendig med mer forskning for å få på plass en standardisert navnestruktur for bruk i militære nettverk.

Trådløse mobile kommunikasjonsnettverk vil kunne ha stor nytte av mulighet for mellomlagring og søk etter informasjon. Dette forutsetter imidlertid at utfordringer knyttet til navn, strategi, ruting og mellomlagring løses. Utfordringene kan deles inn i to delproblemer: 1) Søk etter informasjon og bruk av mellomlagring, og 2) Håndtering av navn, strategi og ruting. Delproblem 1) er relatert til kringkastingsmiljøer slik som radionettverk hvor flere mottakere innenfor radiorekkevidde mottar transmittert data. Gevinsten med flere redundante mellom-lagringsplasser vil, i militære mobile nettverk, trolig kunne komme på bekostning av økt trafikk i nettverket og mulighet for blokkering av brukere som er interessert i allerede etterspurt data. Utfordringen er å utnytte mellomlagring ved å bruke så lite ressurser som mulig. Denne utfordringen er ikke løst i skrivende stund. Delproblem 2) er mer rettet mot søk etter informasjon ved bruk av navn og ruting og mulighet for ulike strategier for søk. Navn, ruting og strategi er tett bundet i Named Data Networking (NDN). For å få god effekt av NDN i et militært nettverk, kreves studier av hvordan kombinere bruken av navn, ruting og strategi.

Quality of Service (QoS) er en utfordring med NDN. NDN gir mulighet for økt robusthet og fleksibilitet ved å kunne tilby søk etter informasjon over flere veier. Med NDN så kan nettverks-noder måle ytelse, ved hjelp av Interest og Data, på ulike veier mot etterspurt informasjon. Basert på ytelsen, så kan veier bli foretrukket. NDN vil derfor trolig egne seg godt til utforsking av nettverket for å imøtekomme QoS-krav[6]. Derimot, så vil NDN være mer utfordret i situasjoner hvor det er et krav om allokering av en ressurs gitt av et QoS-krav. Med IP finnes metoder for å allokere ressurser langs en vei mellom to kommuniserende enheter ved hjelp av for eksempel RSVP [31][7]. I NDN vil ikke kommunikasjonen nødvendigvis gå mellom to

[6] QoS-krav kan i denne sammenheng være gitt ved blant annet data-rate, jitter og dataforsinkelse.
[7] RSVP er en foreslått QoS metode, men har liten støtte i både applikasjoner og nettverk.

enheter. Derimot, så vil den gå mellom konsument og én eller flere mellomlagringssteder hvor produsent kan være én av dem.

En utfordring med NDN er nøkkeldistribusjon. Siden all informasjon er kryptografisk signert er det et behov for nøkkeldistribusjon. Å få til en god nøkkeldistribusjon er derfor av høy interesse og deler mange av utfordringene med nøkkeldistribusjon i IP. Se [5] for flere detaljer rundt ICN-sikkerhet i mobile militære nettverk.

Et annet problem med NDN er trafikkanalyse. En Interest-pakke vil bære med seg navn for hva den etterspør i form av datainnhold. Navnet kan være i klartekst, hvor utenforstående kan erverve seg kunnskap om hva som etterspørres. I tillegg så kan hvem som leverer data, og ev. også hvem som etterspør data hvis Interest er signert, verifiseres ved datasignatur. Det vil derfor være behov for metoder for å kunne motvirke trafikkanalyse.

NDN har til dels mekanismer som håndterer Denial of Service (DOS)-angrep. DOS-angrep mot et navn vil kunne bli begrenset ved bruk av aggregering av Interest siden Interest etterspør samme informasjon. Med aggregering mener vi at kun én Interest vil bli behandlet og sendt videre uavhengig av antallet mottatte Interest som etterspør samme informasjon. Som resultat vil en informasjonsprodusent aldri få mer enn én Interest, og derav i liten grad påvirkes av DOS-angrep. Derimot er ikke NDN i skrivende stund godt beskyttet mot et mangfold av forespørsler etter forskjellige navn. Et synkronisert angrep som etterspør data med gyldige navn vil kunne fylle minnet på nettverksenhetene og derav kunne blokkere ekte og gyldige søk.

Innføring av ny teknologi er alltid utfordrende, og spesielt utfordrende er overgang fra én arkitektur til én ny arkitektur slik som ved overgangen fra linjesvitsjet nett til IP. Historisk, har introduksjon av ny teknologi, som ikke allerede har støtte i eksisterende utstyr, gjerne vært gjennomført ved hjelp av såkalt overlay. Overlay innebærer at man bygger et nettverk basert på en (ny) teknologi som benytter seg av et nettverk basert på en annen (eksisterende) teknologi. Ny teknologi vil da kjøre som overlay over eksisterende teknologi. NDN har i dag støtte for kjøring over IP. Andre muligheter er å kjøre NDN og IP parallelt ved hjelp av en teknologi-gateway, det vil si en gateway som oversetter mellom NDN og IP. Med økt bruk av software-baserte nettverkssystemer vil behovet for eksisterende støtte i nettverksutstyret være mindre. Som et eksempel, vil en eventuell introdusering av P4: Programming Protocol-Independent Packet Processors [32] funksjonalitet gi netteier mulighet for å introdusere og støtte pakketyper utover de tradisjonelle. P4 vil i denne sammenheng gi mulighet for å støtte NDN uten innkjøp av ny nettverksplattform.

En aktuell problemstilling er å studere hvordan informasjonstjenestene til Forsvaret vil kunne passe inn i en NDN-arkitektur under forskjellige nettverksomgivelser. Siden NDN er bygget rundt navn vil det kreves mye av eksisterende tjenester og infrastruktur. Tjenester må utvikles med hensyn på navn og ikke TCP/IP eller UDP/IP, videre må kommunikasjons- infrastruktur støtte tjenester som bruker navn. Det er derfor hensiktsmessig å starte med noen utvalgte tjenester og nettverksomgivelser som vil kunne ha stor nytte av NDN. Samtidig vil det trolig være nyttig å kjøre disse tjenestene over IP i en utprøvingsfase/overgangsfase.

7 Videre lesning

Det finnes mye litteratur om ICN. Mye av litteraturen er fokusert rundt selve arkitekturen og dens egenskaper, men det finnes også litteratur som gir et mer kritisk bilde av ICN. For de som har lyst til å lære mer om arkitekturen er artikkelen «Networking named content» [4] en god start. En samling av artikler, rapporter og presentasjoner kan lastes ned å leses fra [28]

Det har vært flere store EU- og amerikanske forskningsprosjekt som har foreslått forskjellige ICN-arkitekturer. Det fins flere oversiktsartikler som sammenligner disse på forskjellig vis. [3] gir en god sammenligning og lister også de viktigste utfordringene med ICN. For en mer kritisk diskusjon, se «Information-centric networking: seeing the forest for the trees» [6]. De generelle oversiktsartiklene på ICN har stasjonært, høykapasitets Internett som fokus. Bruk i trådløse nettverk gir en del andre fordeler og utfordringer. [7] gir en bra oversikt over ICN for trådløse nettverk.

Det er også publisert noen få artikler som diskuterer ICN for militære mobile nettverk. Noen interessante artikler er vist i referansene [8-12].

Det er startet flere program i USA for å komme opp med ICN-løsninger som kan passe for militære nettverk, for eksempel Defense Advanced Research Projects Agency (DARPA) SHARE (Sharing Battlefield Information at Multiple Classification Levels [29]), og National Science Foundation (NSF)/Intel ICN-WEN (ICN at Wireless Edge Networks [30]). NATO Science and Technology Organization (STO) har også startet en forskingsgruppe, IST-161 «Efficient group and information centric communications in mobile military heterogeneous networks», som studerer ICN i mobile miltære nettverk.

Forfatterne kan også henvise til [13] som gir beskrivelse av NDN sin virkemåte og en oversikt over utfordringer med NDN i trådløse mobile militære nettverk.

8 Konklusjon

I dette arbeidet har vi studert noen av ICN sine egenskaper, eksemplifisert ved NDN, som potensielt kan imøtekomme mange av fremtidens utfordringer i mobile militære kommunikasjonsnettverk. NDN vil kunne gi økt gevinst utover IP i fremtidige mobile militære nettverk så lenge deling av informasjon innenfor én eller flere grupper av mottakere er en stor del av trafikkvolumet, og/eller endringsraten på nettverkstopologi medfører ustabilitet innenfor løsningsområdet for IP. Trender som peker i retning av økt deling av informasjon og ustabile nettverk er: forventet økt utbredelse av sensorer, økt behov for samhandling i grupper og økt bruk av taktiske heterogene radionettverk.

ICN sin bruk av mellomlagring og signering av data gjør at det ikke skilles mellom informasjonsutveksling én-til-én (unicast), én-til-mange (multicast eller Content Delivery Networking) og Delay Tolerant Networking.

NDN arkitekturen har som mål å kunne tilby de samme funksjonene som tilbys med dagens IP-arkitektur like bra eller bedre, men med mindre behov for konfigurering.

NDN er en ung arkitektur, og det er derfor behov for ytterligere analyse og utprøving i større skala. Utprøving innenfor trådløse mobile kommunikasjonsnettverk vil ha stor verdi for ytterligere å kunne belyse gevinster og begrensninger når det gjelder militær bruk. Spesielt viktig vil det være å få til en sømløs overgang og samhandling mellom IP og NDN, siden IP trolig vil være i bruk i lang tid fremover.

Referanser

[1] P. T. Eugster, P. A. Felber, R. Guerraoui, and A.-M. Kermarrec, "The many faces of publish/subscribe," ACM Comput. Surv., vol. 35, no. 2, pp. 114 - 131, 2003.

[2] Named Data Networking project (Tilgjengelig fra:) https://named-data.net/, (Hentet: Jan. 2019)

[3] G. Xylomenos, C. N. Ververidis, V. A. Siris, N. Fotiou, C. Tsilopoulos, X. Vasilakos, K. V. Katsaros, and G. C. Polyzos, "A Survey of Information-Centric Networking Research," IEEE Commun. Surveys Tuts., vol. 16, no. 2, pp. 1024 - 1049, 2014.

[4] V. Jacobson, D. K. Smetters, J. D. Thornton, M. F. Plass, N. H. Briggs, and R. L. Braynard, "Networking named content," in proceedings ACM CoNEXT, Rome, Italy, pp. 1 - 12, 2009.

[5] J. B. Evans, S. G. Pennington, and B. J. Ewy, "Named data networking protocols for tactical command and control," in proceedings SPIE Defense + Security, Orlando, FL, United States, p. 7, 2018.

[6] A. Ghodsi, S. Shenker, T. Koponen, A. Singla, B. Raghavan, and J. Wilcox, "Information-centric networking: seeing the forest for the trees," in proceedings ACM HotNets, Cambridge, Massachusetts, pp. 1 - 6, 2011.

[7] M. Amadeo, C. Campolo, A. Molinaro, and G. Ruggeri, "Content-centric wireless networking: A survey," Computer Networks, vol. 72, pp. 1 - 13, Elsevier, 2014.

[8] J. Burke, A. Afanasyev, T. Refaei, and L. Zhang, "NDN Impact on Tactical Application Development," in proceedings IEEE MILCOM, Los Angeles, CA, USA 2018.

[9] B. Etefia, M. Gerla, and L. Zhang, "Supporting military communications with Named Data Networking: An emulation analysis," in proceedings IEEE MILCOM, Orlando, FL, USA, pp. 1 - 6, 2012.

[10] J. B. Evans, S. G. Pennington, and B. J. Ewy, "Communication networks for the tactical edge," in proceedings SPIE Defense + Security, Anaheim, California, United States, 2017.

[11] C. Gibson, P. Bermell-Garcia, K. Chan, B. Ko, A. Afanasyev, and L. Zhang, "Opportunities and challenges for named data networking to increase the agility of military coalitions," in proceedings IEEE SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI, San Francisco, CA, USA, pp. 1 - 6, 2017.

[12] R. A. Rehman, J. Kim, and B.-S. Kim, "NDN-CRAHNs: Named Data Networking for Cognitive Radio Ad Hoc Networks," Mobile Information Systems, vol. 2015, p. 12, 2015.

[13] M. Hauge, L. Landmark, Ø. Kure and F.T. Johnsen, "Information-Centric Networking for Mobile Military Networks", FFI-rapport 19/00602, 2019, (Tilgjengelig fra:) www.ffi.no/publikasjoner.

[14] L. Landmark, E. Larsen, M.Hauge and Ø. Kure, "Nettverksarkitektur for heterogene mobile taktiske kommunikasjonsnettverk", FFI-rapport 16/01643, (Tilgjengelig fra:) www.ffi.no/publikasjoner.

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

[16] M. A. Brose and M. Hauge, " Group communication in mobile military networks", FFI-rapport 2012/00294 (Tilgjengelig fra:) www.ffi.no/publikasjoner.

[17] V. Thi Minh Do, L. Landmark and Ø. Kure, " A Survey of QoS Multicast in Ad Hoc Networks", Future Internet, vol. 2, no. 3, pp. 388 - 416, 2010

[18] L. Landmark, Y. Lacharite, and L. Lamont, "Multicast Forwarding Using Multiple Gateways and Hash for Duplicate Packet Detection in a Tactical MANET", in proceedings MILCOM. IEEE, pp. 1 - 7, Orlando, FL, USA, October 2007
[19] SJ Cyberforsvaret, "Plan for den videre utvikling av Fosrvarets Informasjonsinfrastruktur (INI) mot 2030", BEGRENSET
[20] S. E. Deering, "Multicast Routing in a Datagram Internetwork", Ph.D. thesis, Stanford University, Dec 1991.
[21] S. Frankel and S. Krishnan, " IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap", (Tilgjengelig fra:) https://tools.ietf.org/html/rfc6071 (Hentet: Jan. 2019)
[22] E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.3", (Tilgjengelig fra:) https://tools.ietf.org/html/rfc8446, (Hentet: Jan. 2019)
[23] V. Cerf et al, "Delay-Tolerant Networking Architecture", (Tilgjengelig fra:) https://tools.ietf.org/html/rfc4838, (Hentet: Jan. 2019)
[24] G. Pallis, A. Vakali, "Insight and perspectives for content delivery networks", Commun. ACM , Volume 49 Issue 1, January 2006, pp. 101 - 106
[25] E. C. Rosen, Y. Cai, " Multicast in MPLS/BGP IP VPNs", (Tilgjengelig fra:) https://tools.ietf.org/html/draft-rosen-vpn-mcast-11, (Hentet: Jan. 2019)
[26] J. Kjellèn, " Russian Electronic Warfare. The role of Electronic Warfare in the Russian Armed Forces.", FOI-R--4625--SE, (Tilgjengelig fra:) https://www.foi.se/rapportsammanfattning?reportNo=FOI-R--4625--SE
[27] Information-Centric Networking Research Group ICNRG, (Tilgjengelig fra:) https://irtf.org/icnrg, (Hentet: Jan. 2019)
[28] (Tilgjengelig fra:) https://named-data.net/publications/
[29] "Sharing Battlefield Information at Multiple Classification Levels via Mobile Handheld Devices", (Tilgjengelig fra:) https://www.darpa.mil/news-events/2017-01-10,(Hentet: Jan. 2019)
[30] "NSF/Intel Partnership on Information-Centric Networking in Wireless Edge Networks (ICN-WEN)", (Tilgjengelig fra:) https://www.nsf.gov/pubs/2016/nsf16586/nsf16586.htm, (Hentet: Jan. 2019)
[31] R. B, Ed, L. Zhang, S. Berson, S. Herzog, S. Jamin, " Resource ReSerVation Protocol (RSVP)", (Tilgjengelig fra:) https://tools.ietf.org/html/rfc2205 (Hentet: Jan. 2019)
[32] P. Bosshart, D. Daly, G. Gibb, M. Izzard, N. McKKeown, J. Rexford, C. Schlesinger, D. Talayco, A. Vahdat, G. Varghese, D. Walker, " P4: Programming Protocol-Independent Packet Processors", ACM SIGCOMM Comput. Commun. Rev., vol. 44, no. 3, pp. 87 - 95, 2014.
[33] J. Roberts, N. Sbihi, " Exploring the Memory-Bandwidth Tradeoff in an Information-Centric Network", Proceedings of ITC 25 (International Teletraffic Congress), Shanghai, September, 2013
[34] V. Jacobson, "A DESCRIPTION OF CONTENT-CENTRIC NETWORKING (CCN)", (Tilgjengelig fra:) https://named-data.net/wp-content/uploads/2014/04/van-ccn-bremen-description.pdf (Hentet: Jan. 2019)

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.

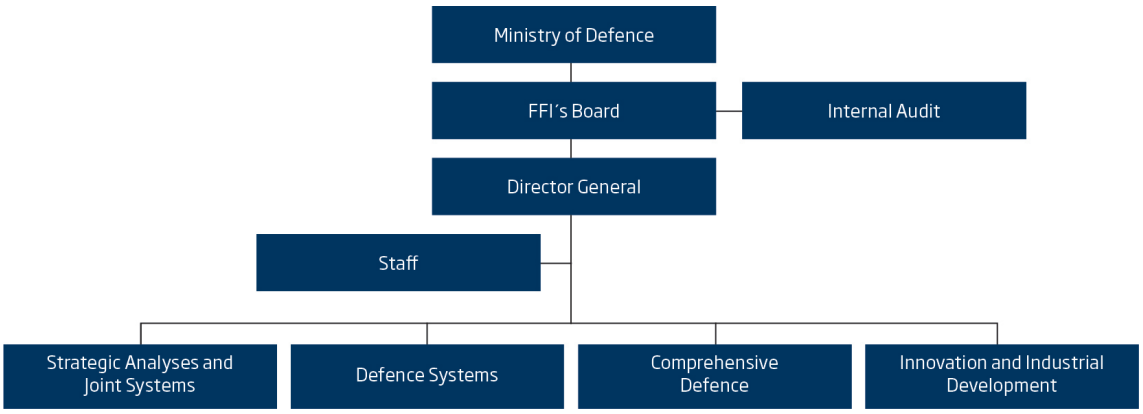
FFIs VISJON

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