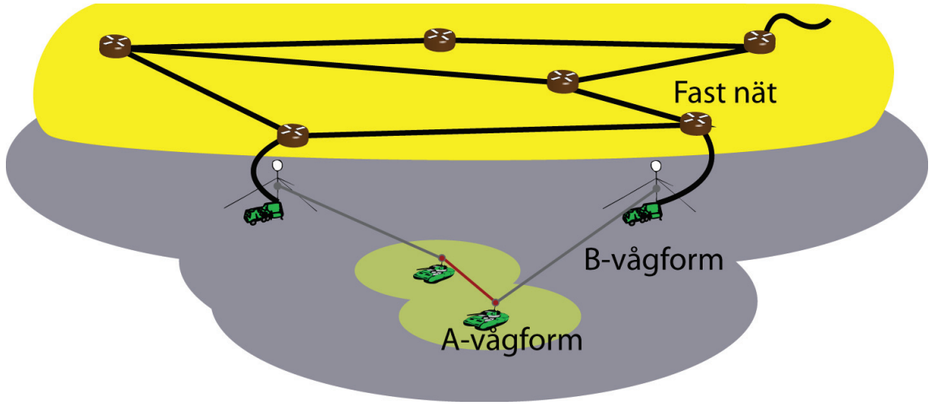
Heterogena taktiska kommunikationsnät

JIMMI GRÖNKVIST, JAN NILSSON,
ANDERS HANSSON, ERIKA JOHANSSON



FOI är en huvudsakligen uppdragsfinansierad myndighet under Försvarsdepartementet. Kärnverksamheten är forskning, metod- och teknikutveckling till nytta för försvar och säkerhet. Organisationen har cirka 1000 anställda varav ungefär 800 är forskare. Detta gör organisationen till Sveriges största forskningsinstitut. FOI ger kunderna tillgång till ledande expertis inom ett stort antal tillämpningsområden såsom säkerhetspolitiska studier och analyser inom försvar och säkerhet, bedömning av olika typer av hot, system för ledning och hantering av kriser, skydd mot och hantering av farliga ämnen, IT-säkerhet och nya sensorers möjligheter.

FOI
Totalförsvarets forskningsinstitut
Informationssystem
Box 1165
581 11 Linköping

Tel: 013-37 80 00
Fax: 013-37 81 00

www.foi.se

FOI-R--3033--SE
ISSN 1650-1942

Användarrapport
September 2010

Informationssystem

Jimmi Grönkvist, Jan Nilsson, Anders Hansson,
Erika Johansson

Heterogena taktiska kommunikationsnät

Titel	Heterogena taktiska kommunikationsnät
Title	Heterogeneous tactical networks

Rapportnr/Report no	FOI-R--3033--SE
Rapporttyp Report type	Användarrapport User Report
Månad/Month	September
Utgivningsår/Year	2010
Antal sidor/Pages	27 p
ISSN	ISSN 1650-1942
Kund/Customer	FM
Projektnr/Project no	E53057
Godkänd av/Approved by	Magnus Jändel

FOI, Totalförsvarets Forskningsinstitut
Avdelningen för Informationssystem
Box 1165
581 11 Linköping

FOI, Swedish Defence Research Agency
Information Systems
Box 1165
SE-581 11 Linköping

Sammanfattning

Olika typer av kommunikationssystem har sina karakteristiska styrkor och svagheter. Ett fast kommunikationsnät kan utformas för att ha en mycket hög kapacitet medan ett radiosystem kan utformas för att ha lång räckvidd, att klara hög mobilitet eller att vara robust. Alla dessa egenskaper är svåra att förena i ett och samma radiosystem.

Ett viktigt taktiskt krav på moderna mobila taktiska kommunikationsnät är att det ska vara möjligt att kommunicera även i områden utan täckning från radiomaster eller basstationer. Sådana helt mobila nät har av fysikaliska skäl ibland begränsad kapacitet. Genom att koppla samman olika typer av kommunikationsnät kan användarbehoven bättre tillgodoses, för att underlätta för mobila användare att kommunicera med det fasta nätet, uppnå högre kapacitet och få bättre förutsättningar för interoperabilitet.Vi kallar sådana sammansatta kommunikationsnät för *heterogena nät*.

Syftet med denna rapport är att kort beskriva möjligheter och utmaningar när olika radio- och kommunikationssystem kopplas samman, samt något om de tekniker som kan användas för att utnyttja den fulla potentialen i ett nätverksbaserat kommunikations- och ledningssystem.

Rapporten beskriver principer för att välja en bra väg genom näten från sändare till mottagare. Detta är viktigt, både för att kommunikationsnätet ska fungera effektivt och för att hantera tjänster som kräver höga datatakter. Dessutom behandlas olika tekniker för mobilitetshantering samt frågeställningar kring tjänstekvalitet i heterogena nät. Ett exempel är att behovet av att använda flera tjänster över heterogena nät medför att principer för tjänstekvalitet i de enskilda näten måste samordnas på en högre nivå. Rapporten innehåller även ett appendix som mer ingående beskriver relevanta tekniker och protokoll.

Nyckelord: Heterogena nät, mobilitetshantering, interoperabilitet, tjänstekvalitet.

Summary

Different types of communication systems have their characteristic strengths and weaknesses. A fixed network is often designed for a very high capacity, while a radio system can be designed to have long range, good support for mobility or robustness. All these qualities are difficult to reconcile in a single radio system.

An important tactical requirement for a modern mobile tactical communication network is that it should enable communication even in areas without coverage from radio masts or base stations. Such fully mobile networks have for physical reasons sometimes a limited capacity. By linking different types of communication systems together, user needs such as better opportunity for mobile users to communicate with the fixed network, higher capacity and better support for interoperability, can be better met. We term such complex networks *heterogeneous*.

This report aims to briefly describe the possibilities and challenges when different radio and communication systems are linked together, and some of the techniques that can be used to utilize the full potential of a network-based system for communication as well as command and control.

The report describes the principles for selecting a good path through the network from sender to receiver. This is important, both for the efficieny of the network and to handle services that require high data rates. In addition, we consider techniques for mobility management and quality of service in heterogeneous networks. An example is that individual network definitions and rules for QoS need to be coordinated at a high level. The report also contains an appendix with an in depth description of the relevant technologies and protocols.

Keywords: Heterogeneous networks, mobility management, interoperability, quality of service.

Innehållsförteckning

1 Inledning

Den här rapporten har tagits fram inom FOI-projektet "Kommunikationsnät för tal- och databaserad stridsledning" som undersöker hur olika typer av tjänster (såsom tal och lägesbild) samtidigt ska hanteras i taktiska mobila nät. Syftet med denna rapport är att kort beskriva möjligheter och utmaningar när olika radio- och kommunikationssystem kopplas samman, samt något om de tekniker som kan användas för att utnyttja den fulla potentialen i ett nätverksbaserat kommunikations- och ledningssystem.

Olika typer av kommunikationssystem har sina karakteristiska styrkor och svagheter. Ett fast kommunikationsnät kan utformas för att ha en mycket hög kapacitet och låga fördröjningar, medan ett radiosystem kan utformas för att ha lång räckvidd, att klara hög mobilitet eller att vara robust. Alla dessa egenskaper är svåra att förena i ett och samma radiosystem. Ett viktigt taktiskt krav på moderna mobila taktiska kommunikationsnät är till exempel att det ska vara möjligt att kommunicera även i områden utan täckning från radiomaster eller basstationer. Sådana helt mobila nät har av fundamentalt fysikaliska skäl ibland begränsad kapacitet. Genom att koppla samman olika typer av kommunikationsnät kan användarbehoven bättre tillgodoses:

- Bättre möjlighet att kommunicera med det fasta nätet
- Högre kapacitet och lägre fördröjningar
- Interoperabilitet

Vi kallar sådana sammansatta kommunikationsnät för heterogena nät.

Kapitel 2 beskriver principer för att välja en väg genom det heteorgena nätet från sändare till mottagare. I många fall kan flera olika vägar finnas samtidigt. Det är därför viktigt att välja en bra väg, både för att kommunikationsnätet ska fungera effektivt och för att hantera tjänster som kräver höga datatakter. Kapitel 3 beskriver olika tekniker för mobilitetshantering i heterogena nät. Kapitel 4 tar upp förplanering av kommunikationsnät. Vi ger även ett exempel på interaktion mellan nät i kapitel 5. Kapitel 6 tar upp frågeställningar kring tjänstekvalitet i heterogena nät. Behovet av att använda flera tjänster över heterogena nät kräver att QoS i de enskilda näten kan samordnas på en hög nivå. Slutligen ger vi i kapitel 7 några slutsatser av arbetet.

Rapporten innehåller även ett appendix som mer ingående beskriver relevanta tekniker och protokoll.

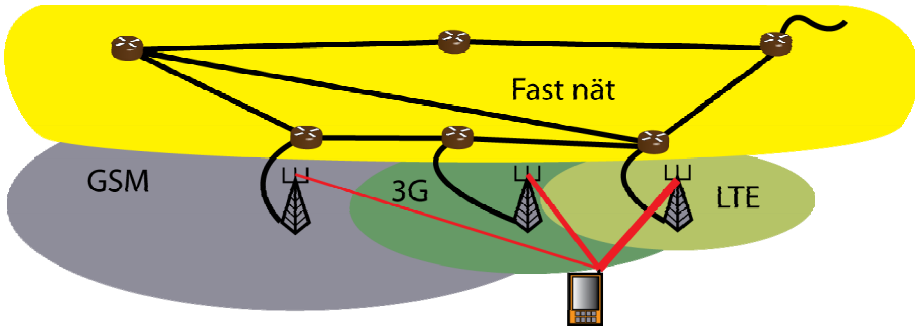
2 Hur hittar man bästa vägen till en nod?

Framtidens taktiska kommunikationsnät kan bestå av en kombination av flera olika radiokommunikationssystem: dels robusta mobila radiosystem såsom TDRS A, TDRS B, ESSOR, WOLF och COALWNW, dels system med högre kapacitet och lägre mobilitet såsom olika typer av radiolänkar, samt system med låg kapacitet, till exempel kortvågsradio. Utöver detta kan man även tänka sig att en rad andra system ibland kan vara tillgängliga, till exempel satellitkommunikationssystem och mobiltelefonisystem. Rörliga enheter kommer ofta att lokalt ha tillgång till flera kommunikationssystem. I dessa fall är det viktigt att kunna avgöra vilket av systemen som är lämpligast vid ett visst tillfälle, eller om trafik bör skickas över flera system samtidigt.

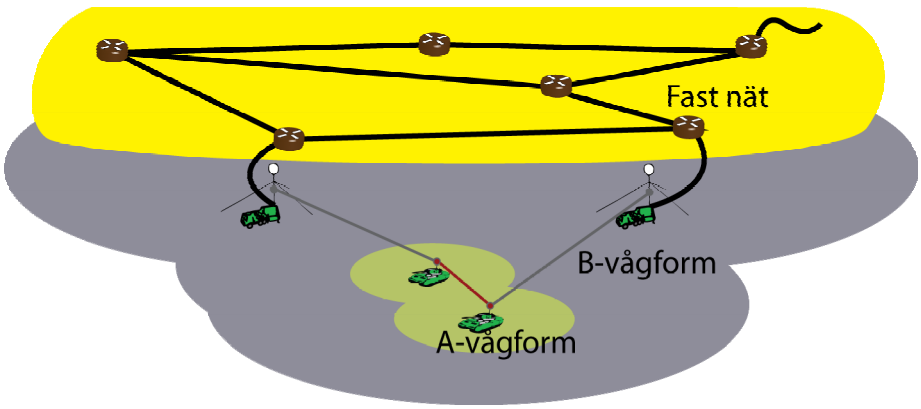
Vid en första anblick liknar detta de problem man kan ha i civila system, där man kan ha tillgång till flera radiotekniker i en enskild terminal (GSM, 3G etc.), men det finns dock väsentliga skillnader: I cellulära nät har man normalt sett ganska kort avstånd till det fasta nätet, i de flesta fall bara ett hopp. I denna situation kan man därför huvudsakligen inrikta sig på att välja den radioteknik i terminalen som ger bäst kapacitet eftersom det fasta nätet inte är begränsat på samma sätt, se figur 1 som exempel.

Detta gäller inte i samma grad för militära mobila nät. Första hoppet kan mycket väl vara en vågform med hög datatakt, men på grund av att vi ofta inte kan ansluta direkt till ett fast nät utan måste kommunicera via andra mobila radiosystem så varierar kapacitet och fördröjningar längs rutten. För att nå alla enheter, inklusive sådana som är anslutna via det fasta nätet, kommer även system med lång räckvidd och lägre datatakter att behöva användas. Detta innebär att en rutt som börjar med ett hopp med hög datatakt kan ha en länk med låg datatakt längre bort. Därför kan vi inte beräkna rutter enbart på lokal information utan behöver tillgång till ytterligare information på ett sätt som ofta inte är nödvändigt i civila nät.

Figur 2 visar ett enkelt exempel på hur militära nät kan kräva mer information än civila system. Vid ett val mellan TDRS A och TDRS B är förmodligen TDRS A att föredra, men det gäller då att veta att det inte finns några länkar över TDRS B längre bort i rutten. Detta är ett problem som sällan dyker upp i kommersiella lösningar, dessutom kommer det hela kompliceras ytterligare av att ad hoc-näten varierar i kapacitet över tiden, exempelvis genom att antalet hopp varierar.



Figur 1 Kommersiella heterogena nät



Figur 2 Taktiska heterogena nät

Routing-algoritmer (dvs. algoritmer för att hitta lämpliga vägar genom näten) hanterar detta genom att sätta olika kostnader (metriker) på att använda länkarna i näten baserade på länkarnas datatakter, där en länk med låg datatakt är dyrare än en länk med hög datatakt. För att lämpliga val ska kunna göras behövs dessa metriker då för hela vägen till destinationen, inte bara för första hoppet. Olika kommunikationssystem använder dock inte nödvändigtvis samma algoritm för att ta fram och förmedla sådana metriker. För att få ett system med flera vågformer att fungera väl behövs därmed väldefinierade gränssnitt och metoder för att informera om den tillgängliga kapaciteten över de olika vägarna. Att ta fram metoder för att åstadkomma detta är viktigt för att de olika vågformerna ska fungera bra tillsammans i ett heterogent nät.

En annan viktig skillnad mellan civila och militära system är att de civila systemen i stort sett alltid kan antas vara uppkopplade mot det fasta nätet, medan i militära system måste separerade nätdelar då kunna fungera autonomt.

3 Tekniker för mobilitetshantering i heterogena nät

I varje paket som skickas i ett IP-nät ingår en IP-adress för både sändare och mottagare. Dessa IP-adresser har traditionellt använts till att både markera identitet och för att beskriva var en enhet finns i nätet. Identiteten utnyttjas av applikationer för att identifiera rätt motpart vid en uppkoppling. Information om nodens plats i nätet används av routing-algoritmer för att välja en lämplig väg genom nätet. För att routingen ska kunna fungera i Internet och andra stora nät kan inte varje enhet hålla koll på var alla andra är om alla kopplas in på helt godtyckliga positioner. Den första delen av IP-adressen kallas nätdel och beskriver vilket nät en nod tillhör. Hur stor del av IP-adressen som utgör nätdelen avgörs av antalet noder i nätet. Genom att dela ut IP-adresser på ett smart sätt kan man lägga samman information om nät på sådant sätt att man istället för att skicka ut uppdateringar för varje litet nät när förändringar sker, kan summera dessa till en enskild uppdatering med kort längd på nätdelen. Så länge noderna är statiska kan de därför ges lämpliga IP-adresser för att minimera problemen med att hantera stora nät.

Om enheter däremot flyttas kan man få problem. Små lokala förändringar kan lösas lokalt men större förändringar (i nätstrukturen - geografiskt kan det fortfarande vara små förändringar) kan ställa till problem som måste hanteras. Behåller noden sin IP-adress kan det ställa till det för routingen, då noden har bytt vilket nät den tillhör men har fel nätdel på sin IP-adress. Om IP-adressen byts måste det finnas metoder för andra noder att avgöra vad den nya IP-adressen är annars kan man inte kommunicera med den.

Ovanstående är inga nya frågeställningar och det finns en rad tekniker som löser olika delproblem, baserat på vilka scenarier de utvecklats för. Beroende på hur en nod flyttas runt och var i nätet den kopplas in kan en fix IP-adress används om det finns mekanismer som kompenserar för detta. Alternativet är att låta applikationerna kompensera för problemet. Nedan är tre exempel på principer för hur detta kan gå till.

3.1 Mobilitet med fast IP-adress: basic routing

Även om IP-routing i Internet är hierarkiskt uppbyggd för att minimera overhead så kan man lokalt göra vissa uppdateringar av routing-informationen för att undvika byte av IP-adress varje gång noden byter anslutningspunkt till nätet. Många routing-algoritmer hanterar all information lokalt för att välja väg. De är dock normalt inte anpassade för att klara många mobila enheter utan snarare för att hantera att enstaka routrar till exempel slås av och på eller startas om.

Routing i ad hoc-nät inkluderar däremot full mobilitetshantering men för att detta ska fungera även vid övergångar från en vågform till en annan, passering av gateways, etc. behöver routing-information i dessa fall utvidgas för att ge information även in i de något mer ”fasta” delarna av nätet. Detta kan bli kapacitetskrävande om mobila enheter (och nät) har många (vitt skilda) anslutningspunkter till en mer fast infrastruktur. Fördelen är att metriker kan inkluderas och multipla sammankopplade ad hoc-nät kan fungera utan alltför mycket problem.

3.2 Mobilitetshantering med multipla IP-adresser

Den routing-lösning som beskrevs i förra stycket fungerar inte när många nät är sammankopplade. Istället kan man införa specifika tekniker för att hantera just de noder som förflyttas mellan nät. Detta görs genom att den mobila noden behåller sin IP-adress vid förflyttning men den tilldelas dessutom tillfälliga IP-addresser för att underlätta rutthanteringen. För interna förflyttningar, exempelvis inom ett ad hoc-nät, behöver de tillfälliga adresserna inte användas. En tillfällig IP-adress används när en nod behöver byta anslutningspunkt. Anslutningspunkternas routing-processer förhandlar då om vilken anslutningspunkt som ska användas. Trafik till noden kan sedan tunnlas till denna anslutningspunkt, vilket innebär att paket som var adresserade till den gamla adressen kapslas in i nya paket med den tillfälliga IP-adressen som destination.

Man kan dela upp tekniker i *host-based* eller *network-based* mobiltet. I det första fallet är den mobila enheten involverad i mobilitetshanteringen och i den andra hanterar nätet förändringar mer transparent för den mobila noden. Befintliga lösningar är ofta utformade för att de mobila näten är direkt sammanbundna med en fast infrastruktur, vilket gör att lösningarna ofta är beroende av funktionalitet i det fasta nätet. Det är därför osäkert om denna typ av mobilitetshantering kan fungera när alla delar av nätet är mobila.

3.3 Mobilitetshantering på applikationsnivå

Ett annat sätt att hantera mobilitet är att applikationen låter noden ta en ny IP-adress när det behövs. Detta flyttar en stor del av mobilitetshanteringen till applikationerna. Vissa befintliga applikationer har sådan funktionalitet men oftast är dessa lösningar avsedda för nät med en hierarkisk struktur, vilket kan försvåra hanteringen av distribuerade nät såsom ad hoc-nät. Ett annat problem är att en rad standardapplikationer helt saknar stöd för adressbyten. Vi kommer inte att studera lösningar med applikationsmobilitet närmare i denna rapport eftersom det är svårt att hitta gemensamma lösningar för alla tjänster och applikationer.

4 Förplanering

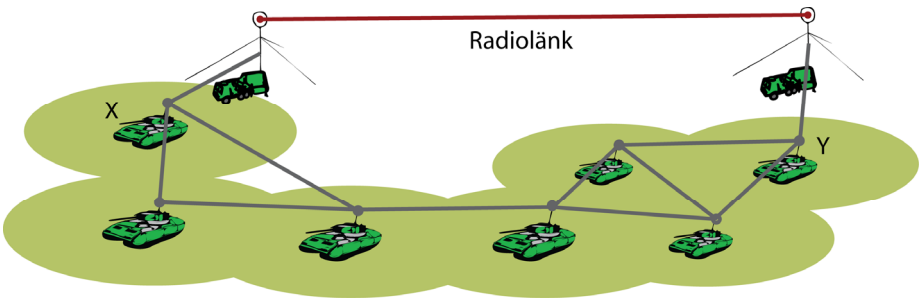
Till viss mån kan mobilitetshanteringen förenklas genom förplanering av näten och kunskap om hur man förväntar sig att förflyttning ska ske. Förplanering innebär här till exempel en lämplig konfigurering av noders IP-adresser eller statiska rutter över länkar med högre datatakt som man vet kommer att finnas. Förplanering kan också innebära val av vilka system som kan kopplas ihop och när man kan göra det (inkompatibla metriker är bara ett problem om det finns mer än en möjlig väg).

Förplanering är inte speciellt ovanligt i militära nät, framför allt när det gäller säkerhetsmekanismer, men vissa aspekter är svårare att förplanera. Det är exempelvis inte speciellt praktiskt att behöva konfigurera om näten för att man plötsligt behöver använda länkar med låg datatakt för att binda ihop näten på ett icke förutsett sätt. Om de mobila enheterna/näten är designade för att fungera ihop från början kommer de förmodligen inte ha några problem när de kopplas ihop. Det finns dock risk att system från olika tillverkare kommer att generera information på olika sätt och skapa interoperabilitetsproblem när de kopplas samman.

Interaktionen med det fasta nätet kan förenklas med hjälp av förplanering genom att man skapar ett virtuellt lokalt nät där alla anslutningspunkter till det fasta nätet är sammankopplade (via det fasta nätet). Detta nät visas upp för de mobila näten som att det är ett hopp mellan alla anslutningspunkter och den faktiska nätstrukturen behöver därmed inte importeras in i de mobila delarna. Detta virtuella nät ändras inte mycket om inte nya anslutningspunkter behövs som inte var förväntade från början. På detta sätt kan man kraftigt minska informationsspridingen mellan fasta och mobila delar. För att detta ska fungera effektivt krävs dock höga kapaciteter i den fasta delen av nätet eftersom kostnaden för att ta sig genom denna normalt inte kommer att synas när lämpliga vägar skall hittas.

5 Exempel på interaktion mellan nät

Ett exempel på interaktion mellan vågformer ges i figur 3. I detta exempel har vi ett mobilt ad hoc-nät (exempelvis GTRS) där man dessutom använder några radiolänkar för att öka kapaciteten mellan de yttre delarna av nätet. Nätet kommer att förflytta sig lite, så radiolänkstationerna kommer då och då att behöva förflytta sig för att inte bli frånåkta. Detta innebär att ständig uppkoppling mot det fasta nätet inte är möjligt och att det är viktigt att radiolänkstationerna kan göra snabba och automatiska uppkopplingar mot nätet för att maximera deras användbara tid.



Figur 3 Exempel på ett mobilt ad hoc-nät kompletterat med en radiolänk.

Antag nu att nod X i vänstra delen av nätet behöver kommunicera med nod Y i högra delen av nätet. Detta kan antingen ske genom många hopp genom ad hoc-nätet eller ett hopp till den närmsta radiolänkstationen, ett hopp över radiolänken, samt ett hopp till nod Y. Att utnyttja radiolänken kan alltså vara en klar fördel men vilken information behöver förmedlas mellan systemen för att routrarna ska kunna ta sådana beslut? I detta fall har vi två olika routing-algoritmer som måste interagera, dels den ad hoc-nätsinterna (med protokoll designade för effektivitet i just dessa vågformer), dels den som används av de externa routrarna (här förmodligen i första hand över radiolänkarna, men även som gränssnitt mot ad hoc-nätsnoderna). Exakt vad som händer i praktiken kommer att bero på vilka specifika komponenter som finns i systemet och detaljer i protokollen.

Nod X kommer här ha två huvudvägar till nod Y, en via ad hoc-nätet och en via radiolänken. För att ett lämpligt beslut ska tas måste nod X ha fått information från den vänstra radiolänkstationen om att den vägen finns och om den är bättre än den genom ad hoc-nätet. Den vänstra radiolänkstationen måste i sin tur ha fått denna information från den högra stationen som i sin tur fått den från sin ad hoc-nätssida. I detta fall måste alltså informationen från ad hoc-nätssidan inte bara ha varit ”väg finns” utan också kostnad för vägen som är jämförbar med den som skapats internt i ad hoc-nätet, annars kan inte nod X inse att det är så få hopp i

andra änden att genvägen är värd att ta. På samma sätt måste radiolänksidans information föras tillbaka till ad hoc-nätssidan som ett totalt mått.

Det kan vara värt att notera det inte är tillräckligt att enbart använda antal hopp som kostnadsmått eftersom vi kunde ha haft en kortvågslänk i stället för den antagna radiolänken. I detta fall hade man velat undvika att använda den kortare rutten så länge som alternativ inom ad hoc-nätet fanns.

En lösning som förenklar interaktionerna mellan olika nät är att använda samma routing-protokoll överallt. Detta är en typ av lösning vi studerar närmare i appendix. Problemen med att använda ett gemensamt protokoll är just att det behöver vara generellt och måste utformas för många olika accesstekniker. Interaktion med lägre lager och optimering för enskilda radiotekniker blir därmed svårare. I appendix tittar vi närmare på den standardiseringsprocess som pågår inom detta område och de begränsningar det medför för militära nät.

6 Tjänstekvalitet i heterogena nät

Antag nu att vägvalsproblemet är löst på ett lämpligt sätt. Även om vi i första hand väljer en väg med så höga datatakter som möjligt kommer vi ibland att behöva använda svagare länkar för att undvika överbelastning av de starka länkarna. Hur man hanterar tjänstekvalitet (vi använder även den engelska förkortningen QoS som står för Quality Of Service) är därmed en viktig fråga och genom att tjänsterna delas in i klasser så kan till exempel viktig data och tal prioriteras.

Antag att ett paket ska skickas genom flera olika nät för att nå destinationen. Om dessa nät har olika metoder för att dela in tjänster i QoS klasser, behöver den tjänsteklass paketet tilldelas i första nätet förstås och kunna stödjas i de andra näten. Detta innebär att det måste vara möjligt att översätta mellan tjänsteklasser i olika nät. Lämpligen görs den översättningen i en gateway mellan två olika nät.

Det finns ramverk för att hantera QoS över heterogena nät men dessa är främst användbara för statiska nät med hög kapacitet, till exempel TACOMS (TActical COMmunicationS in the land combat zone post 2000). På stridsteknisk nivå, främst för de mobila näten, finns idag egentligen inga tydliga lösningar för hur QoS ska samordnas mellan olika nät även om det finns förslag för olika specialfall.

Två olika grundprinciper används normalt för att klassificera trafik. Fördröjningskänslig eller speciellt viktig trafik brukar tilldelas en tjänsteklass som kräver att kapacitet reserveras för att garantera förbindelsen, så kallad ”förbindelseorienterad trafik”. Den andra principen, ”icke-förbindelseorienterad trafik” använder sig av en lokal prioritering av paket tillhörande olika tjänsteklasser i varje nod längs vägen från sändare till mottagare. I Internet motsvaras dessa grundprinciper av teknikerna ”Integrated Services” (IntServ) respektive ”Differented Services” (DiffServ). Även om många mekanismer och protokoll från dessa Internettekniker också kan användas i taktiska heterogena nät återstår flera problemställningar. Allmänt sett är det svårare och mer resurskrävande att stödja förbindelseorienterad trafik än icke förbindelseorienterad trafik. Att reservera resurser kan fungera bra inom ett mindre mobilt nät, eller inom delar av nät, där man har bra intern kontroll över resurserna och kännedom om topologin. För stora nät och framför allt för en förbindelse som går över flera mobila nät blir detta svårt eller i alla fall väldigt resurskrävande. En möjlighet skulle kunna vara att reservera mera kapacitet än som egentligen behövs genom att sätta upp inte bara en förbindelse utan också flera alternativa förbindelser så trafiken snabbt kan omdirigeras om den första bryts.

En annan frågeställning är hur översättningar mellan olika avancerade tjänsteklassindelningar ska göras. Ett första nät kanske har många klasser medan

ett andra nät bara har de två klasserna ”prioriterad” eller ”icke-prioriterad trafik”. Detta innebär att flera olika klasser från det ena nätet måste avbildas på samma klass i det andra nätet, vilket i sin tur innebär att det andra nätet kommer att ha svårt att skilja på dessa och erbjuda den QoS som efterfrågas. För många nät med olika QoS-klassindelningar blir det dessutom opraktiskt och svårt att bestämma hur alla översättningar ska se ut. En Princip som kan användas är att ta fram en standardiserad QoS-klassindelning. Varje nät får då definiera hur dess interna QoS-klasser ska översättas till och från de standardiserade QoS-klasserna. Det är denna princip som används inom TACOMs. I gateway-noden mellan två nät används den standardiserade QoS-klassindelningen som ett mellansteg. Eftersom man vill ha möjlighet att stödja kommunikation med många olika QoS klasser mellan näten behöver den standardiserade QoS-klassindelningen vara relativt avancerad med många klasser. Att bestämma hur man ska avbilda ett fåtal klasser på många, d v s översätta till de standardiserade klasserna, är ett relativt enkelt problem. Det omvända problemet, d v s hur man avbildar många klasser på ett fåtal, är däremot betydligt svårare.

Nät kan också ha väsentligt olika kapacitet, till exempel om man jämför ett bredbandigt UHF nät med ett smalbandigt kortvågsnät. Då kortvågsnätet bara kan hantera en bråkdel av trafiken i UHF nätet är det viktigt med inträdeskontroll för trafiken som släpps in i kortvågsnätet, där exempelvis endast särskilt viktig trafik där inga andra bra vägar till destinationen finns tillåts inträde. I andra fall kan man vilja tunnla trafik, till exempel över nät med dålig säkerhet. All QoS hantering måste då ske i ändpunkterna. Detta begränsar förstås möjligheterna att styra tjänstekvaliteten och tillhandahålla önskad prestanda. Om mycket kapacitet finns tillgänglig kan dock tunnling fungera bra.

QoS-hanteringen som beskrivs ovan avser en framtida dynamisk situation där flera mobila nät ska kunna interagera och stödja många olika trafiktyper. I dagsläget är situationen enklare, i regel används ett nät för tal, ett nät för data etc. men dessa nät behöver kunna kopplas samman med varandra och med det fasta nätet, till exempel via radiolänkar och satellitlänkar. I anslutningspunkten för sådana länkar kan det uppstå en flaskhals när trafik från flera olika taktiska nät behöver tas om hand. Eftersom även radiolänkar och satellitlänkar har begränsad kapacitet behöver någon form av prioritering av trafik göras. Prioriteringen kan dock göras i förväg och är ett betydligt enklare problem än vad som beskrivs ovan.

7 Slutsatser och diskussion

I denna rapport har vi diskuterat de potentiella problem som kan uppstå om olika nät och system kopplas ihop utan att från början vara anpassade för det. En sådan hopkoppling av system behöver inte nödvändigtvis leda till problem, men hela kommunikationssystemet riskerar att fungera sämre än förväntat.

Av de principer för mobilitetshantering som vi tittat på är Basic Routing intressantast, det är dock inte en fungerande lösning om näten blir alltför stora. En del frågeställningar kvarstår också innan man kan få en klar bild av nätens prestanda. Hur stora delnät klarar man av vid olika kapaciteter? Många lösningar är designade för system med betydligt högre datatakter än vad flertalet militära system kommer att ha. Hur påverkas lösningarna av militära säkerhetskrav? Kan vi anta att kostnadsmått kan överföras fritt mellan olika nät?

I appendix har vi också beskrivit och analyserat ytterligare några potentiella tekniker för att hantera mobilitet i heterogena nät. Det finns ett antal problem och frågeställningar som är av intresse för vidare studier. De följande problemställningarna är lämpliga att studera inom området heterogena nät:

Interaktion mellan vågformer:

Heterogena nät är mer komplexa att utvärdera än enskilda homogena nät, både ur analytisk- och ur simuleringssynpunkt. Men med undantag av speciella fall där enstaka routrar sätter begränsningar kommer flaskhalsarna vara de enskilda näten. Genom att modellera hur skilda nät genererar routing-information (inklusive metriker) för export till andra nät bör man kunna studera hur overheadinformationen växer med antalet nät, detta även utan att i detalj behöva implementera och simulera de enskilda näten. Sådana utvärderingar kan göras för nät av olika storlek och kapacitet och användas för att avgöra skalbarhet i systemet samt vilka typer av nät som är mest känsliga för denna typ av overhead. Mer detaljerade simuleringar kan sedan vara en naturlig fortsättning, men vilka detaljer som ska undersökas vidare är beroende av resultaten från den enklare utvärderingen.

Ett annat intressant problem är att utvärdera vinsten av att utnyttja heterogena nät även i fall när ett enskilt nät skulle kunna förmedla informationen. Ett sådant fall är det tidigare exemplet med en radiolänk med hög kapacitet som hjälp till ett ad hoc nät. Hur många sådana radiolänkar skulle behövas? Vilka räckvidder och kapaciteter behövs på radiolänkarna för att det ska vara till nytta för applikationerna/användarna? I detta fall är det inte interaktionen som sådan som skulle studeras utan snarare vilken nytta man skulle kunna ha av sådan interaktion.

QoS:

Kommunikation i heterogena nät kräver att QoS-hanteringen och tjänsteklass-indelningarna i de enskilda näten kan samordnas. En princip som kan användas är att använda en standardiserad QoS-klassindelning. Varje nät får då definiera hur dess interna QoS-klasser ska översättas till och från de standardiserade QoS-klasserna. Det är dels oklart hur en lämplig uppsättning av standardiserade QoS-klasser bör se ut och dels behövs metoder för att översätta QoS-klasser till och från dessa standardiserade klasser och frågan bör därmed undersökas vidare. Dessutom behöver man undersöka hur översättningar mellan QoS-klasser påverkar de olika tjänsternas prestanda.

Appendix: Analys av möjliga tekniker för att hantera mobilitet i heterogena nät

I denna del av rapporten diskuterar vi specifika tekniker som kan vara av intresse i mer detalj.

Basic routing: OSPF with MANET extension

Den för tillfället mest intressanta utvecklingen inom detta område är förmodligen utvidgningen av routing-protokollet OSPF (Open Shortest Path First) för mobila ad hoc-nät [RFC2328]. OSPF är ett av de mest välanvända protokollen på Internet och det finns mycket erfarenhet kring dess användande. Arbetsgruppen ”MANET working group” har utvecklat och standardiserat flera routing-protokoll for ad hoc-nät de senaste åren, men dessa har i första hand varit utvecklade för fristående ad hoc-nät utan kontakt med andra nät. Det är dock ur IP- och användarsynpunkt ingen principiell skillnad mellan mobila radionät och fasta nät, och specifik design av routing-protokoll för ad hoc-nät tvingar i många fall en radionod att hantera flera separata protokoll, både ad hoc-näts routing-protokoll och fastnätsprotokoll. Dessutom behöver rutter förmedlas mellan de olika protokollen vilket är ett potentiellt problem.

OSPFs arbetsgrupp inom IETF har därför börjat utveckla en utvidgning av den nuvarande OSPF specifikationen för att också kunna hantera ad hoc-nätsnoder. För tillfället finns tre konkurrerande standarder, beskrivna i [RFC5449, RFC5614, RFC5820]. Principiellt är alla dessa tämligen lika varandra, även om notationen skiljer sig något. Två av dessa är baserade på MPR (Multi Point Relaying), som också varit bas för OLSR [RFC3626] som sedan tidigare är ett standardiserat ad hoc-nätsrouting-protokoll. Den tredje baserar sig istället på en gemensam CDS (Connected Dominating Set) för att förmedla routing-information. I huvudsak fungerar alla tre varianterna ganska likt OSPF för fasta nät men en del tillägg görs bland annat för att reducera overhead och för att bättre hantera den snabbare uppdateringstakten utan att dränka nätet i signaleringsdata.

OSPF är ett så kallat länktillstånds-protokoll, vilket innebär att varje router genererar meddelanden om vilka nät och länkar till andra routrar den är ansluten till. Dessa meddelanden flödas sedan genom alla OSPF-nät i systemet och baserat på denna information kan varje enskild router beräkna den bästa vägen till alla andra routrar i området. För att göra det hela lite mer skalbart kan man dela in området som OSPF jobbar inom i olika areor, dessa är dock manuellt uppsatta vid start. För att minska på signaleringsdata finns mekanismer att

reducera meddelandeutsändningar om många routrar är kopplade till samma nät. Dessa fungerar dock inte bra i ad hoc-nät då de antar att alla routrar kan höra alla andra routrar i detta nät, något som oftast inte gäller i de ad hoc-nät vi studerar.

Det största nuvarande problemet alla de tre OSPF-varianterna är att de har utvecklats för länklagerprotokoll såsom IEEE802.11 (WLAN) med höga länkdatatakter [IEEE802.11]. Höga innebär datatakter på 1Mb/s och uppåt, ofta mycket mer, något som snarare kan ses som övre gräns i taktiska ad hoc-nät då krav på räckvidd och störtålighet är mycket högre. För att åstadkomma längre räckvidder kan man också vänta sig vågformer med betydligt lägre datatakter, ner mot tiotalet kb/s. Specifik hantering för att minska mängden overhead kommer att vara nödvändigt i dessa fall för att inte dränka näten i signaleringsdata. De metoder som idag är beskrivna är idag otillräckliga. Som ett exempel kan ges de simuleringsresultat som visas i OSPF-MDR [RFC5614] för mängden overhead vid olika nätstorlekar. Dessa mängder kommer att vara svåra eller omöjliga att hantera med de datatakter vi för tillfället ser som realistiska i militära ad hoc-nät.

Dessa protokoll har designats för att vara oberoende av vilken länkteknik som använts (lager 2), med så lite interaktion som möjligt enligt lagerprincipen. Det ska helst gå att byta ut ett lager utan att de övriga behöver ändras. Det finns då också bättre möjligheter att använda samma protokoll (och i vissa fall även samma implementation) i många system vilket gör det enklare med interaktion mellan olika system. Nackdelen med detta är ökade mängder overhead när samma data behöver genereras på flera lager. Speciellt blir detta märkbart allteftersom lägre lager blir mer avancerade och komplexa för att öka kapacitet och kunna ge QoS stöd.

Prestanda på ad hoc-nät är i mycket stor grad begränsat av hur väl Medium Access Control (MAC) lagret fungerar. Det vill säga den funktion som avgör när en nod får tillgång till radiomediet. Ett exempel på data som kan genereras på flera lager är HELLO-meddelanden, som används för att avgöra hur det lokala grannskapet till en nod ser ut. I vanlig OLSR är detta den största delen av overheadtrafiken [FOI2323]. Även om de nya protokollen har möjlighet att reducera detta genom en mer effektiv hantering av dessa meddelanden, är det troligt att de fortfarande utgör en stor del av overheadtrafiken och att de innehåller till största delen information som lägre lager redan kan ha genererat.

Ytterligare ett problem relaterat till HELLO-meddelanden är uppmätningen av vilka länkar som redan finns inte går lika bra på lager 3 som på lägre lager. På nätlagret finns i stort sett bara information om att meddelanden kom fram eller inte; lägre lager kan ha mycket mer information än så för att avgöra länkkvalitén. Utvidgningar av lägre lager för att hantera effektkontroll och variabel datatakt kan också vara knepigt. Dessa kan ha stor betydelse då de påverkar vilken metrik som bör användas över en länk. Detta skulle kunna hanteras genom standardiserade gränssnitt mellan länklagret och nätlagret som ger information

om länken, men sådana finns inte i de nuvarande RFC-dokumenten och det är osäkert om den typen av information kommer att bli tillgängligt.

OSPF med MANET-utvidgningar är en intressant utveckling för ad hoc-nät, men i sin nuvarande form kan den förmodligen inte användas i alla de militära ad hoc-nät vi i dag kan förvänta oss att använda/behöva.

Basic routing: Separata ad hoc-nätsprotokoll för routing

OSPF-lösningen som tidigare beskrevs är ett försök att använda ett gemensamt routing-protokoll över alla nät. Detta är en lösning som ger klara fördelar när det gäller att få interaktionen mellan nät att fungera. Men som tidigare nämnts finns också en del problem med protokollen som gör dem potentiellt svåranvända i vissa nät. Ett alternativ till att använda OSPF över alla länkar och nät är att använda det som gemensamt interface mellan olika system där varje respektive system kan använda egna lokala routing-protokoll internt om OSPF inte är lämpligt. Sådana protokoll kan därmed optimeras ihop med det lokala länklagret om behov av detta finns och kan själv anpassa uppdateringstakter och hur meddelanden skickas för att få signaleringsdata till rimliga nivåer.

Detta ställer dock en del krav för att allt ska fungera ihop, både på de interna protokollen och på hur rutter visas upp utåt. Alla nät som kan nås via ett interface måste uppdateras och kunna visas upp på samma sätt som OSPF skulle göra, dessutom är det också nödvändigt att detta görs med kompatibla metriker. För att en extern OSPF-baserad router ska kunna ta ett lämpligt beslut om vilket av sina interface som för tillfället är det bästa att sända ett paket via måste dessa interface inte bara förmedlat att de har en väg till slutdestinationen utan också ett kostnadsmått på rutten. Kostnadsmåttet behöver inte vara fullständigt korrekt, det är tillräckligt att ett bra val görs. Så länge det korrekta måttet skiljer sig lite spelar det inte så stor roll vilken väg som väljs, det är fallet att de skiljer sig mycket som är viktigast att detektera. Detta innebär exempelvis att det kanske inte är nödvändigt att uppdatera de yttre näten varje gång en rutt blir kortare eller längre i ett ad hoc-nät.

Detta leder inte bara till krav på de externa interfacen, utan också en del krav på den interna funktionalitetens egenskaper. Ett gemensamt standardiserat kostnadsmått på länkar behövs, detta behöver vara kompatibelt med hur OSPFs egna metriker fungerar (alternativt skulle något annat standardiserat protokoll än OSPF kunna användas, men det bör ha en metrik baserat på länkdatatakter då detta skiljer sig mycket mellan de olika radiosystemen).

Hur routingen sker internt är dock ett mindre problem i detta sammanhang. OSPF kan naturligtvis köras internt också om det passar ett nät, men om andra metoder är att föredra fungerar det lika bra. Detta innebär exempelvis att ett nät

kan välja att göra lokal routing baserat på lager 2 information istället för lager 3 information. Lager 3 information kommer naturligtvis också behövas i detta fall (för routing-informationen mellan nät) men den uppdateras förhoppningsvis inte lika ofta. Lager 2 routingen behöver dock generera metrik informationen till nätlagret annars kommer man inte kunna åstadkomma den funktionalitet vi diskuterat ovan.

Det gemensamma problemet med denna lösning och med att använda ett gemensamt protokoll är skalbarheten i systemet. Det är svårt att säga hur stora nät som rimligen kan hanteras, beroende på hur nättopologin ser ut kan man dessutom få väldigt olika resultat. Om ett ad hoc-nät fungerar som yttersta nät ut till en samling mobila trupper och är deras enda kommunikationssystem behöver ingen speciell information sändas ut i resten av nätet oavsett hur mycket de rör sig internt. De metriker vi har diskuterat här är egentligen bara viktiga om flera vägar existerar och snabb uppdatering av metrikerna är enbart nödvändig om vägarna (nätkopplingarna) förändras ofta. Detta är ett område som behöver undersökas mer.

Vid inköp av ett nytt kommunikationssystem skulle man helst vilja att man bara behövde ställa några enkla krav på hur det ska uppträda utåt för att det nya systemet ska fungera ihop med existerande system. Det är förmodligen en bit dit dock, troligen behöver vissa egenskaper vara konfigurerbara (eller ännu hellre vara självkonfigurerande), så att bara nödvändig information förmedlas ut från ett nät, men detta är idag ännu långt från någon form av standardisering.

Mobility management: Mobile IP

Mobile IP är IETFs standard i hur mobila enheter kan tillåtas att flytta sig från ett nätverk till ett annat och fortfarande ha samma permanenta IP-adress. Mobile IP för IPv4 är beskriven i [RFC3344] och för IPv6 i [RFC3775].

Mobile IP är en *host-baserad* teknik och grundprincipen är att en mobil nod har en fast IP-adress oberoende av var den för tillfället finns, en så kallad *home address*. När noden är iväg från sitt hemnät (dvs. det nät home address tillhör) skaffar den sig ytterligare en IP-adress, *care-of-adress*, som identifierar var den råkar vara just nu. I hemnätet finns en funktion, *home agent*, som fångar upp paket till noden och kapslar in dessa (tunnling) med care-of-adress som destination. Mobile IP specificerar hur en nod registrerar sig mot *home agent* samt hur paket tunnlas mot den mobila enheten. Noga räknat behöver inte *home adress* vara helt fast, om enbart sessionsmobilitet önskas, dvs sessioner ska inte brytas under mobilitet, räcker det med en dynamiskt tilldelad *home adress* som är konstant under sessionens gång.

Mobile IP har en rad begränsningar som gör den otillräcklig som teknik i heterogena militära nät. Man kan dock tänka sig att ha nytta av protokollen i kombination med andra lösningar.

Tillgång till hemnätet och *home agent* är nödvändigt för mobile IPs funktion. Även om det kan antas vara normalt att kunna nå alla punkter i ett nät så kommer det vara svårt att alltid garantera, till exempel kan två noder i närheten av varandra därmed få svårt att kommunicera på grund av att hemnäten inte kan nås. Partitioner måste kunna hanteras. Uppkoppling och registrering tar i allmänhet mycket tid. Mobile IP har hittills inte varit designad för snabba uppdateringar och sann mobilitet under gång. Behovet av tunnling är ytterligare ett problem, med hjälp av en agent i det besökta nätet (*foreign agent*) kan man undvika behovet att tunnla ända fram till den mobila noden genom att terminera tunneln i det fasta nätet. Detta fungerar dock inte så väl när man routar över flera mobila nät.

I grund och botten är Mobile IP utvecklat för att noder skulle kunna koppla in sig var som helst på Internet och fortfarande vara nåbara utifrån såsom om de fortfarande var inkopplade hemma. Mobilitet och föränderliga nät (enstaka noder är inte det enda som förändras) var inte huvudsyftet med protokollet.

Det finns förslagna utvidgningar till Mobile IP för att även kunna hantera mobila routrar. I [RFC3963] beskrivs Network Mobility (NEMO) som är ett Mobile IP kompatibelt protokoll för att kunna hantera att en router och därmed även alla noder bundna till denna byter anslutning till Internet. Detta fungerar även om de enskilda enheterna i det mobila nätet saknar funktioner för mobilitetshantering. I princip fungerar detta som vanlig mobile IP, en mobil router skaffar sig en temporär *care-of-address* som trafik tunnlas till, medan det lokala subnätet som följer med routern inte kommer att märka av mobiliteten. Även om detta protokoll är något mer generellt än vanlig Mobile IP så finns fortfarande de flesta begränsningar kvar.

Mobility management: NETLMM och Proxy Mobile IP

NETLMM står för network-based local mobility management [RFC4830] och är en av IETFs arbetsgrupper som tar fram ett protokoll som heter Proxy Mobile IP (PMIP) för att hantera lokal mobilitet utan att involvera den mobila noden [RFC5213]. Detta protokoll kan därmed ses som en nätverksbaserad variant av Mobile IP. Tanken är att noden kan växla mellan olika access routrar utan att behöva ändra sin IP-adress och därigenom göms all mobilitet för applikationerna. Detta protokoll kommer användas mycket i framtida mobiltelefoninät och utvecklingen har påverkats av mobiltelefonutvecklingen.

Proxy Mobile IP är baserat på Mobile IPv6, men fungerar på sådant sätt att den mobila enheten inte behöver ha någon funktionalitet för att hantera mobilitet. Sett ur den mobila nodens synpunkt lämnas aldrig hemnätet. Det kan påpekas att detta gäller IP-nivå och uppåt, nya accessnät kan ha varierande lager 2-tekniker som måste hanteras när noden byter nät.

PMIP använder två funktioner för att hantera mobilitet. Den första är *Mobile Access Gateways* (MAGs) som finns i de besökta näten och hanterar mobilitetssignalering för den mobila noden. Den andra är *Local Mobility Anchor* (LMA) vars roll liknar home agent i Mobile IPs fall. MAGs uppgift är att detektera mobilitet och initiera den signalering som behövs. Den kommer också att emulera den mobila enhetens hemnät i den mening att lager 3 inte märker någon skillnad efter förflyttning, IP-adresser och andra parametrar hålls konstanta. Utan att gå in på ytterligare detaljer rörande PMIP kan vi konstatera att det har liknande problem som Mobile IP för användning i militära nät.

Applikationslagermobilitet: SIP

Session Initiation Protocol (SIP) är ett exempel på protokoll som kan användas för att hantera mobilitet på applikationsnivå [RFC3261].

Referenser

[RFC2328] J. Moy, “OSPF Version 2”, RFC 2328, april 1998.

[RFC5449] E. Baccelli, P. Jacquet, D. Nguyen, T. Clausen, “OSPF Multipoint Relay (MPR) Extension for Ad Hoc Networks”, RFC 5449, februari 2009.

[RFC5614] R. Ogier, P. Spagnolo, “Mobile Ad Hoc Network (MANET) Extension of OSPF Using Connected Dominating Set (CDS) Flooding,” RFC 5614, augusti 2009.

[RFC5820] A. Roy, Ed., M. Chandra, Ed., Extensions to OSPF to Support Mobile Ad Hoc Networking, RFC 5820, mars 2010.

[RFC3626] T. Clausen, Ed., P. Jacquet, “Optimized Link State Routing Protocol (OLSR)”, RFC 3626, oktober 2003.

[IEEE802.11] “IEEE Std. 802.11-2007, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications,” IEEE Std. 802.11, 2007.

[FOI2323] Jimmi Grönkvist, Anders Hansson, Mattias Sköld, OLSR broadcast security in mobile ad hoc networks, FOI-R--2323--SE, 2007.

[RFC3344] C. Perkins, Ed., “IP Mobility Support for IPv4”, RFC 3344, augusti 2002.

[RFC3775] C. Perkins, Ed., “Mobility Support in IPv6”, RFC 3775, juni 2004.

[RFC3963] V. Devarapalli, R. Wakikawa, A. Petrescu, P. Thubert, “Network Mobility (NEMO) Basic Support Protocol”, RFC 3963, januari 2005.

[RFC4830] J. Kempf, Ed., “Problem Statement for Network-Based Localized Mobility Management (NETLMM)”, RFC 4830, april 2007.

[RFC5213] S. Gundavelli, Ed., K. Leung, V. Devarapalli, K. Chowdhury, B. Patil “Proxy Mobile IPv6”, RFC 5213, augusti 2008.

[RFC3261] J. Rosenberg et al., ”SIP: Session Initiation Protocol”, RFC 3261, juni 2002.