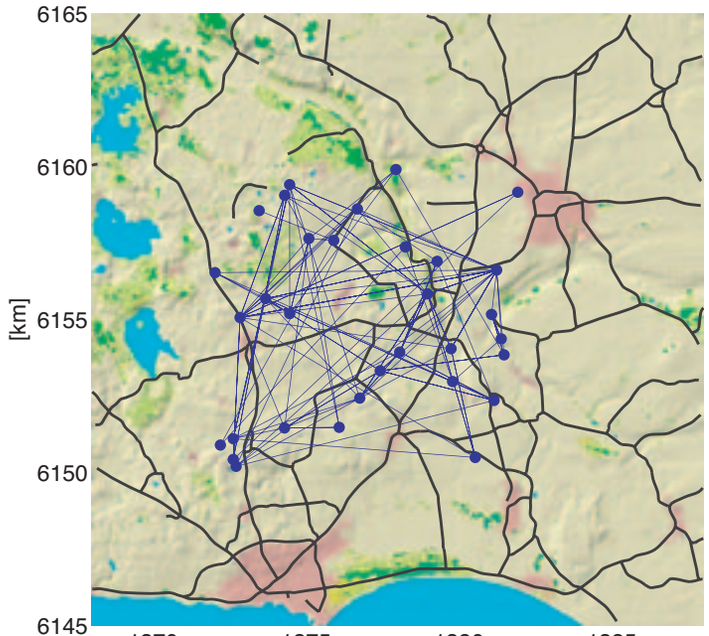
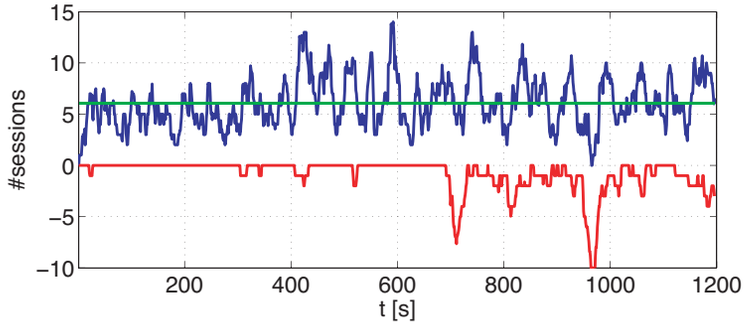
Mobila ad hoc-nät
- Utmaningar och möjligheter

REDAKTÖR: MATTIAS SKÖLD





FOI är en huvudsakligen uppdragsfinansierad myndighet under Försvarsdepartementet. Kärnverksamheten är forskning, metod- och teknikutveckling till nytta för försvar och säkerhet. Organisationen har cirka 1350 anställda varav ungefär 950 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
Ledningssystem
Box 1165
581 11 Linköping

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

www.foi.se

FOI-R--1799--SE Användarrapport
ISSN 1650-1942 December 2005

Ledningssystem

Mobila ad hoc-nät
- Utmaningar och möjligheter

FOI-R--1799--SE
ISSN 1650-1942

Ledningssystem
Användarrapport

December 2005

Utgivare Totalförsvarets Forskningsinstitut Ledningssystem Box 1165 SE-581 11 LINKÖPING	**Rapportnummer, ISRN** FOI-R--1799--SE	**Klassificering** Användarrapport
	Forskningsområde 4. Spaning och ledning	
	Månad, år December 2005	**Projektnummer** E7035
	Delområde 41. Ledning med samband och telekom och IT-system	
	Delområde 2	
Författare Linda Farman, Jimmi Grönkvist, Anders Hansson, Erika Johansson, Jan Nilsson, Katarina Persson, Mattias Sköld, Ulf Sterner, Otto Tronarp och Pelle Zeijlon	**Projektledare** Mattias Sköld	
	Godkänd av Sören Eriksson	
	Uppdragsgivare/kundbeteckning Försvarsmakten	
	Teknisk och/eller vetenskapligt ansvarig Jan Nilsson	
Rapportens titel Mobila ad hoc-nät - Utmaningar och möjligheter		
Nyckelord ad hoc-nät, access, MAC, routing, tjänstekvalitet, QoS		
Övriga bibliografiska uppgifter	**Språk** Svenska	
ISSN 1650-1942	**Antal sidor:** 56 s.	
Distribution enligt missiv	**Pris: Enligt prislista**	

Sammanfattning

Ett taktiskt ad hoc-nät är en viktig komponent i försvarets framtida kommunikationsarkitektur. Ett sådant nät måste vara robust, självkonfigurerande och självläkande och kunna tillhandahålla tillräcklig tjänstekvalitet för olika typer av tjänster också i ett scenario med hög mobilitet. För att uppnå tillräcklig tjänstekvalitet i ett scenario med hög mobilitet krävs en noggrann protokolldesign.

I rapporten ges en översikt över viktiga frågeställningar avseende styrning av ad hoc-nät. Dessutom presenteras den forskning som bedrivits inom projektet med avseende på design av MAC- och routingprotokoll samt inom områdena tjänstekvalitet och utnyttjande av adaptiva radio-noder.

Issuing organization Swedish Defence Research Agency Command and Control Systems P.O. Box 1165 SE-581 11 LINKÖPING SWEDEN	**Report number, ISRN** FOI-R--1799--SE	**Report type** User Report
	Programme areas 4. C^{4}ISR	
	Month year December 2005	**Project No.** E7035
	Subcategories 41. C^{4}I	
	Subcategories 2	
Author/s Linda Farman, Jimmi Grönkvist, Anders Hansson, Erika Johansson, Jan Nilsson, Katarina Persson, Mattias Sköld, Ulf Sterner, Otto Tronarp and Pelle Zeijlon	**Project manager** Mattias Sköld	
	Approved by Sören Eriksson	
	Sponsoring agency Swedish Armed Forces	
	Scientifically and technically responsible Jan Nilsson	
Report title Ad Hoc Networks - Challanges and Possibilities		

Abstract

A tactical ad hoc network is an important component in future military communications. Such a network must be robust, self-forming, self-healing and be able to support different types of service requirements even in a high mobility scenario. To support quality of Service (QoS) and high mobility careful design of the ad hoc network protocols is required.

This report gives an overview of important issues regarding ad hoc network control. Furthermore, our research in this area is presented here. The research have been focused both on the design of MAC and routing protocols, as well as on Quailty of Service (QoS) and the use of adaptive radio nodes.

Keywords ad hoc networks, MAC, routing, quality of service, QoS	
Further bibliographic information	**Language** Swedish
ISSN 1650-1942	**Pages** 56 p.
	Price acc. to pricelist

Förord

Den här användarrapporten syftar till att beskriva problemställningar för ad hoc-nät och kortfattat redovisa resultat och slutsatser från FoT-projektet Heterogena ad hoc-nät som bedrivits på FOI under åren 2003-2005. Vi har försökt att beskriva problemställningar och lösningar med ett inte alltför tekniskt språk. För den mer tekniskt intresserade läsaren rekommenderas vi den tekniska slutrapporten för projektet [1].

Innehåll

Kapitel 1

Inledning

1.1 Bakgrund

För att lösa försvarets uppgifter är förbanden beroende av robusta och effektiva kommunikationssystem. Det ska vara möjligt att utbyta information mellan olika enheter på ett stabilt och säkert sätt. Enheterna ska fungera tillsammans och behöver därmed vara sammankopplade i ett nät. Då många enheter är mobila krävs trådlös kommunikation och ett bra sätt är att använda radio. Information ska också kunna skicka till enheter som kan vara spridda över stora ytor och man ska kunna skapa en gemensam lägesbild. För att tillgodose bl a dessa behov krävs mycket dynamiska radionät, t ex ad hoc-nät

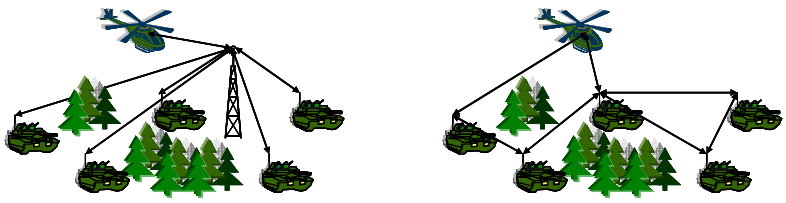
1.2 Vad är ett ad hoc nät?

För att undvika svaga punkter i radionätet bör nätet inte ha någon central styrning. Dagens mobiltelefonsystem är basstationsbaserade och kan lätt slås ut genom att basstationerna, de centrala enheterna, tas ur funktion antingen genom fysisk bekämpning alternativt att de störs ut med elektromagnetisk strålning. Denna typ av nät har fördelen att de mobila enheterna kan göras enkla och billiga men mobilerna är helt hjälplösa utan den centrala enheten. I basstationsbaserade nät kan långa kommunikationsavstånd krävas för de mobila enheterna ska nå in till basstationen, vilket i sin tur kräver antingen fri sikt, d v s upphöjda noder eller hög effekt och/eller bra antennförstärkning. Användandet av centra-

la enheter utgör onekligen en sårbar arkitektur, både med avseende på risk för upptäckt och när det gäller robusthet mot störning.

Genom att man istället för central styrning av nätet *distribuerar* nätstyrningen, d v s enheterna i nätet sköter själva styrningen av nätet, uppnås ett mer robust system. Varje enhet i nätet fungerar dela som sändare och mottagare men också som *router*, d v s de kan avgöra hur vidareförmedling av datapaket i nätet ska göras. Enheter i nätet som befinner sig utom räckhåll för varandra kan därmed kommunicera genom att mellanliggande enheter vidareförmedlar informationen. Detta innebär att nätet är ett s k *flerhoppsnät*. Denna typ av nät erbjuder en robust arkitektur där meddelanden snabbt kan hitta nya vägar vid t ex störinsatser. Förbindelseavståndet mellan två direktkommunicerande enheter kan dessutom hållas kort, vilket undviker minskar den utstrålade effekten per sändning och minskar risken för upptäckt från motståndaren. Priset som får betalas är att nätstyrningsfunktionen blir betydligt mera komplicerad.

Enheterna i ett nät kallas *noder*. Två noder som kan kommunicera direkt med varandra sägs ha en *länk* mellan sig. I figur 1.1 visas ett exempel på ett basstationsbaserat nät med en basstation och med länkar till de sex noderna i nätet och ett flerhoppsnät med sex noder och sju länkar.

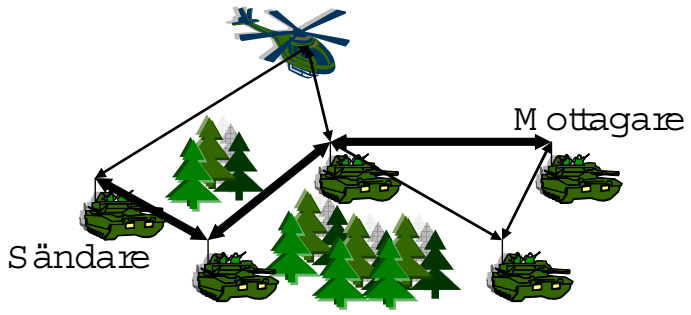


Figur 1.1: Jämförelse mellan ett basstationsbaserat nät och ett flerhoppsnät.

Ad hoc är latin och betyder för detta ändamål, med detta menas att nätet skapas vid behov och anpassar sig till förhållanden som råder för tillfället. Mobila ad hoc-nät är trådlösa flerhoppsnät med förmåga att dynamiskt anpassa sig efter varierande användarbehov, terräng, kommunikationsflöden och vågformer. Näten är självständiga, det vill säga oberoende av basstationer eller fast infrastruktur.

1.3 Grundläggande begrepp för nätstyrnigen

En viktig frågeställning i ett ad hoc-nät är hur *trafikstyrningen (routingen)* ska ske, d v s via vilka noder trafiken ska skickas genom nätet. Routingproblemet innebär att hitta bästa vägen, enligt något kostnadsmått, genom nätet från sändare till mottagare. I figur 1.2 illustreras vägen som meddelandet tar från sändaren till mottagaren.



Figur 1.2: Routingalgoritmen hittar en väg genom nätet från sändare till mottagare.

En annan viktig frågeställning är kanaltilldelningen, d v s hur användarna (noderna) i nätet ska dela på den gemensamma kanalresursen. För detta krävs någon slags regel för när och hur noderna kan sända och detta hanteras av en *kanaltilldelningsalgoritm (MAC - Medium Access Control)*.

1.4 Rapportens upplägg

I kapitel 2 beskrivs olika viktiga problemställningar som möter ett mobilt ad hoc-nät och tänkbara lösningar för dessa. Därefter, i kapitel 3, ger vi exempel på relevanta kommunikationstjänster för ett ad hoc-nät och vilka krav de ställer. I kapitel 4 presenterar vi kortfattat vår forskning inom mobila ad hoc-nät. Rapporten avslutas med en diskussion om några framtida viktiga forskningsområden för taktiska ad hoc-nät.

Kapitel 2

Viktiga frågor för nätstyrningen

2.1 Robusthet

Ett kommunikationsnät för bruk inom försvarsmakten eller totalförsvaret behöver vara robust. Detta eftersom det ska kunna operera i en godtycklig och eventuell fientlig miljö. Kommunikationen måste även fortsätta att fungera även om noder försvinner, till exempel genom att noden slås ut eller förflyttas till en position med otillräckligt kommunikationsförhållande. Noder måste även kunna tillkomma om de kommer inom kommunikationsräckvidd eller slås på efter radiotystnad.

2.1.1 Hur skapar vi robusthet i nätet?

För att tillgodose kraven på robusthet, till exempel med avseende på att noder kan slås ut, krävs *distribuerad nätstyrning*. Distribuerad nätstyrning innebär att det inte finns en/flera central noder som hanterar nätstyrningen såsom trafikstyrning och kanaltilldelning, utan detta sköts distribuerat genom samverkan mellan noderna. Ett exempel på detta är att noderna utbyter trafik sinsemellan för att avgöra vem som får sända när.

Fördelen med att ha distribuerad nätstyrning jämfört med centraliserad, är att det inte finns någon central nod som kan slås ut via fysisk bekämpning, störning eller dåligt kommunikationsförhållande. Noderna kan därmed fortsätta kommuniera även om en eller flera noder försvinner. I ett fall med ett centraliserat nät, t ex ett mobiltelefonnät, kommer däremot kommunikationen i hela det

område som den centraliserade noden (basstationen) betjänar att sluta fungera om denna nod slås ut.

Genom att använda *flerhopp*, d v s tillåta noder att reläa trafik till andra noder, ökar vi också robustheten. En nod behöver inte längre ha direktkommunikation med alla den önskar kommunicera med (i ett s k enhoppsnät) utan det räcker att man är med i samma nät. Dessutom kan lägre uteffekt användas (per sändning) i ett flerhoppsnät där närliggande noder kan reläa vidare meddelandet än om direktkommunikation används och detta minskar hotet från vissa typer av signalspaning.

2.2 Mobilitet

Eftersom bl a Försvarsmaktens kommunikation ska kunna fungera på godtycklig plats och under förflyttning måste nätet kunna hantera mobilitet. Mobiliteten påverkar indirekt vilka noder som kan ha direktkommunikation med varandra. Detta beror på ändrade positioner och terrängförhållanden påverkar länkarna mellan noderna och leder till att länkar blir bättre/sämre, tillkommer eller försvinner.

2.2.1 Hur påverkar mobilitet nätverket?

Eftersom mobiliteten påverkar vilka noder som kan kommunicera med varandra kommer också nätstyrningen att påverkas. Detta innebär att vid hög mobilitet måste trafikstyrningen och eventuellt också kanaltilldelningen uppdateras ofta medan det vid låg mobilitet inte behövs så många uppdateringar. Denna uppdateringstrafik brukar benämnas som *overhead-trafik* i nätet. Overhead-trafiken använder nätkapacitet som skulle ha kunnat användas för nyttotrafik. Det är därför önskvärt att hålla uppdateringstakten så låg som möjligt, samtidigt behöver nätstyrningen uppdateras tillräckligt ofta för att nätverket ska fungera och nyttotrafik ska kunna sändas i nätet. Detta innebär att en avvägning måste göras mellan hur bra kvalitet man vill ha i nätet, mätt i t ex sannolikheten att ett skickat meddelande når den avsedda mottagaren, och hur mycket av trafiken som får vara overhead-trafik.

När länkar tillkommer eller försvinner i nätet måste noderna hitta nya vägar för sin trafik i nätet. Detta kommer att ge upphov till fördröjningar av varierande storlek, beroende på hur lång tid det tar att finna en ny väg till den önskade

destinationen. Noden kommer därmed att få vänta olika länge innan den åter kan sända sin nyttotrafik.

2.2.2 Hur hanterar vi mobilitet i nätet?

För att hitta nya vägar genom nätet används routingprotokoll. Det finns två huvudtyper av routingprotokoll: *reaktiva* och *proaktiva* protokoll. Ett proaktivt protokoll innebär att routingprotokollet uppdaterar alla vägar i nätet med ett bestämt intervall. Ett reaktivt protokoll uppdaterar endast en väg när behovet finns, d v s när en nod har något att sända och saknar väg dit.

Om vi har hög mobilitet och använder ett proaktivt protokoll måste intervallen mellan uppdateringarna vara mycket korta. Detta innebär att det genereras och skickas mycket overhead-trafik. Fördelen med denna typ av protokoll är att det finns en väg direkt när noden vill sända, d v s fördröjningen blir låg. Om vi istället använder ett reaktivt protokoll kommer overhead-trafiken inte att bli lika stor eftersom vi endast uppdaterar en väg vid behov, men fördröjningen blir större än för ett proaktivt protokoll.

Om man för ett specifikt nätverk ska välja reaktiv eller proaktiv routing beror på vad nätverket ska användas till och vilka tjänster och applikationer som ska stödjas. Generellt gäller att reaktiva protokoll är bättre i nät där få förbindelser i taget är aktiva. I gengäld är proaktiva protokoll att föredra om man har kvalitetskrav, t ex maximal tillåten fördröjning, som måste uppfyllas.

Genom att kombinera ett proaktivt och ett reaktivt protokoll på ett lämpligt sätt kan man få både relativt låg fördröjning och relativt låg overhead-trafik. Ett exempel på hur ett sådant *hybridprotokoll* är uppbyggt är att använda ett proaktivt protokoll för noder i närområdet (lokalt) och ett reaktivt protokoll för kommunikation över längre sträckor (globalt).

Accessprotokkollet påverkas även den av mobiliteten. Detta beror på att när noder ändrar position förändras interferensförhållandena i nätet, t ex kan två noder som sänder samtidigt hamna intill varandra och därmed skapa interferenser och störa varandra. Det går att dela in accessprotokollen i två grupper: *konfliktfria* och *konfliktlösande* protokoll. Ett konfliktfritt protokoll innebär att noden får tilldelat sig en kanalresurs, t ex ett antal tidluckor att sända i eller en frekvens att sända på. Den konfliktlösande varianten tilldelar däremot inte noderna några kanalresurser utan noden får försöka ta resurser när den behöver dem. Ett konfliktfritt protokoll kommer vid hög mobilitet att behöva omförhand-

la resursfördelningen ofta och det resulterar i mycket overhead-trafik i nätet. Ett konfliktlösande protokoll påverkas däremot inte lika mycket av mobiliteten i nätet.

2.3 Heterogena noder

Noderna i nätet kan ha olika förutsättningar i form av olika antenner, batterier, processorkraft, uteffekt, plattform, frekvensomfång, tillgängliga datatakter etc. Att noder med olika förutsättningar ingår i samma nät ger ett *heterogent* nät.

Ett heterogent nät innebär både för- och nackdelar. En fördel är att noder med låg mobilitet kan utnyttjas för att reläa trafik. En annan fördel är att noder, mellan vilka högkapacitiva länkar finns, kan utnyttjas till fullo och mer trafik kan därmed överföras. En nackdel är att noder med mycket hög mobilitet, t ex en helikopter, försvårar nätstyrningen eftersom vägar och resurstilldelning till dessa noder måste uppdateras mycket ofta. Ytterligare nackdelar är att användningen av riktantenner försvåras då positionerna ändras ofta och att vissa antenner, t ex större gruppantenner och högantenner, kan vara svåra att använda under förflyttning.

Ett heterogent nät innebär en ökad kompexitet hos nätstyrningen för att kunna hantera och utnyttja nodernas olika förutsättningar på bästa sätt. I gengäld ger heterogeniteten också möjligheter till bl a ökad kapacitet och bättre sambandskvalitet.

2.4 Kapacitet

Kapacitet är ett svårtolkat begrepp eftersom det är starkt kopplat till en mängd olika faktorer, t ex vilken modell som används för att beskriva användarnas generering av trafik och vilka tjänster som nätet ska stödja. Det finns därmed ett flertal olika sätt att mäta ett näts kapacitet. Vi har här valt att använda ett av de vanligare sätten - nämligen att nätets *kapacitet* mäts som den mängd trafik som samtidigt kan överföras i nätet.

När man valt kapacitetsdefinition finns det ett antal olika faktorer som påverkar hur stor kapaciteten i nätet blir. En viktig faktor är den *bandbredd* som finns tillgänglig för varje länk. Ju större bandbredd en länk har, desto mer information kan föras över på en gång vilken minskar fördröjningarna över länken i

fråga. Tilldelningen av bandbredd är dock oftast utanför nätets kontroll, den kan t ex avgöras av Post- och Telestyrelsens restriktioner för aktuellt frekvensband eller av den utrusning noden har till sitt förfogande.

En annan viktig faktor, som också den är svår att styra, är *nättopologin*. Enkelt uttryckt är nättopologin en beskrivning av vilka noder som var och en av noderna kan ha direktkommunikation med i ett givet ögonblick. Om en länk kan bildas eller inte beror på inbördes positioner, terrängen mellan noderna och dessutom på hurdan utrustning noderna har iform av antenn, uteffekt, bandbredd o s v.

Vissa typer av nättopologier är mycket svårare än andra att hantera och få hög kapacitet i. En sådan situation är när topologin råkar bli sådan att mycket trafik måste överföras via ett fåtal noder. Detta kan ske t ex om några få noder utgör förbindelsen mellan två delnät eller om nätet blir "långt och smalt". I det första fallet, få förbindelser mellan två delnät, bildas en flaskhals som trafiken måste passera. Detta kan lätt resultera i kapacitetsförluster då alternativa vägar saknas och köer bildas och nätets övriga kapacitet inte kan uttnyttjas fullt ut. Ett liknande fenomen fås även i det andra fallet då vi har ett "långt och smalt" nät. Eftersom (om man antar att alla noder genererar lika mycket trafik) en mycket stor del av trafiken då måste passera mitten av nätet för att nå sin destination och det inte finns särskilt många alternativa vägar. Detta innebär att kapaciteten som finns tillgänglig för var och en av noderna sjunker. Generellt gäller detta alltid i flerhoppsnät, när antalet gånger ett meddelande reläas ökar, sjunker kapaciteten/användare. Om ett *trafikadaptivt* accessprotokoll används, kan noder som utgör en flaskhals tilldelas mer kanalresurser jämfört med övriga noder i nätet och situationen kan på så sätt förbättras.

Beroende på nodernas inbördes positioner, d v s på nätets topologi, kan kanalresurser användas samtidigt av flera noder om dessa befinner sig tillräckligt långt ifrån varandra. Detta kallas *spatiell återvinning*, se avsnitt 4.1. Att ha ett accessprotokoll som klarar att hantera denna fråga är en stor fördel och kan ge stora kapacitetsvinster. Samtidigt måste protokollet ha tillgång till mer data om noderna för att kunna göra en bra resursfördelning och detta ger upphov till att mer overhead-trafik måste sändas för att upprätthålla en bra resursfördelning.

Inom en begränsad bandbredd är *datatakten*, det vill säga överföringshastigheten, avgörande för länkens kapacitet då man har digitala sändningar i form av t ex filöverföring. Datatakt mäts ofta i bitar/s, ibland i tecken/s. En högre datatakt innebär att mer data kan överföras per sekund, t ex innebär en fördubbling

av datatakten på alla länkar en fördubbling av nätets kapacitet. Det finns dock ett antal begränsningar som avgör vilken datatakt som kan användas.

Till att börja med finns gränser för vilka datatakter nodernas utrustning klarar, ibland saknas helt möjlighet att välja datatakt. Sedan sätter nätstyrningsprotokollen ofta ytterligare gränser, t ex klarar IEEE802.11b datatakterna 1, 2, 5.5 och 11 Mbit/s. Dessutom så gäller att ju högre datatakten är, desto bättre kommunikationsförhållanden krävs för att inte få försämrad överföringskvalitet.

För att höja datatakten krävs i praktiken en starkare nyttosignal (jämfört med brus och interferenser). En starkare signal kan uppnås t ex genom att sända med högre uteffekt, använda en högre antenn, omgruppera till ett fördelaktigare terrängavsnitt eller genom att flytta sig närmare mottagare. Vilka (om någon) av dessa åtgärder som är möjlig beror på situationen och den tillgängliga utrustningen. Om/när sambandsförhållandena försämras p g a förändringar i nättopologin, terrängen eller signalmiljön, innebär detta ofta att en sänkning av datatakten blir nödvändig för att upprätthålla förbindelsen.

2.4.1 Nyttotrafik

För användaren är det egentligen inte nätets totala kapacitet som är intressant utan den andel av kapaciteten som kan användas för att skicka *nyttotrafik*. Ett mål för nätstyrningen är därmed att maximera andelen nyttotrafik. Hur väl nätstyrningen kan uppfylla detta mål beror på många olika faktorer, vi kommer här att lista några av de viktigaste:

Overhead-trafik Mängden overhead-trafik beror bl a på valda routing- och accessprotokoll, mängden trafik i nätet och nätets mobilitet.

Trafikadaptivitet Hur bra fördelar nätstyrningsprotokollen trafiken i nätet? Finns det långa köer av trafik i vissa noder medan andra noder inte använder all sin kapacitet? Om det finns flera möjliga vägar genom nätet, kan trafiken spridas prallellt på dessa. Total trafikutjämning är dock i princip omöjlig att uppnå då nätet oftast har flaskhalsar som man inte kan göra något åt, t ex kan vissa noder bli tvugna att hantera mer trafik beroende på sina fysiska positioner eller p g a att de själva genererar mycket trafik (stab etc.).

Kostnadsmått Vilka *kostnadsmått* klarar nätstyrnigen av att hantera? Ett kostnadsmått mäter, baserat på något kriterie, hur bra en väg genom nätet är.

Det vanligaste kostnadsmåttet är *min-hopp*, detta innebär att man i ett flerhopps nät försöker minimera antalet noder man passerar mellan sändaren och destinationen (sändning över en länk = ett hopp). Man kan med detta kriterie inte väga in andra vikiga aspekter så som att få hopp ofta innebär långa länkar vilket i sin tur ofta innebär lägre datatakt/sämre kommunikationsförhållande än för kortare länkar. Det är dessutom mer sannolikt att en lång länk kommer att brytas p g a att någon av de inblandade enheterna flyttar sig eller att en (mindre) interferens/störning/brushöjning uppstår. Det är därför mycket intressant att använda sig av mer komplexa kostnadsmått än min-hopp.

Paketstorlek Hur bra hanterar nätstyrningsprotokollen olika paketstorlekar? Vissa kommunikationstjänster kan t ex generera många små paket medans vissa genererar stora paket. Om accessprotokollet inte är bra på att hantera varierande paketstorlekar, kommer i detta fall endera de stora paketen att delas upp eller de små paketen att få sig tilldelade för stora kanalresurser (t ex en tidlucka/paket). I det första fallet genereras mycket overhead-trafik, i det andra kommer stora delar av kanalresurserna att låsas upp och inte utnyttjas (det lilla paketet fyller bara en bråkdel av tidluckan).

Heterogenitet Kan nätstyrningen utnyttja eventuell heterogenitet i nätverket och hur bra? Det är en stor fördel om nätstyrningen kan ta tillvara alla noders fulla potential. Ett exempel på detta är att utnyttja en UAV (Unmanned Airial Vehicle) som relänod då den har fri sikt (d v s bra kommunikationsförhållanden) till många av noderna i nätet. Ett annat exempel är att styra mer trafik över noder som har länkar med hög kapacitet/datatakt. Om nätstyrningen inte kan utnyttja denna typ av möjligheter utan t ex istället sänder all trafik på den datatakt som den sämsta noden klarar, kommer nätets maximala kapacitet aldrig att kunna utnyttjas.

Spatiell återvinning kan öka nätets kapacitet betydligt. Samtidigt innebär det komplexare nätstyrning och mer overhead-trafik. Frågan blir då - för ett givet nät och de tjänster nätet är avsett för - kommer ökningen av kapaciteten att vara tillräckligt stor för att ökningen i nyttotrafik uppväger komplexitetsökningen?

Reläande (flerhopp) Kapaciteten i nätet påverkas också av hur många gånger paketen reläas innan de når sina respektive mottagare. Om mängden re-

läad trafik är stor kommer nätets nyttokapacitet att minska eftersom varje nyttopaket sänds många gånger innan det når mottagaren och därmed använder mer kapacitet än vad som hade behövts för en direkt överföring. Flerhoppsnät, med sin reläfunktionallitet, har dock många andra fördelar t ex att möjliggöra kommunikation i situationer där direktkommunikation är omöjlig och kapaciteten annars hade varit noll.

2.5 Tjänstekvalitet

En utmaning i ett ad hoc-nät är att tillhandahålla någon typ av tjänstekvalitet, mer känt som Quality of Service, QoS. Nätet måste kunna hantera en rad olika tjänster så som taltjänst, SA-tjänst och filöverföring. Dessa tjänster ställer alla olika krav på tjänstekvalitetn så som krav på fördröjning, genomströmning, paketförlust etc.

Trådlös kommunikation innebär i sig svårigheter att garantera tjänstekvalitet eftersom ett system med trådlös kommunikation utsätts för flervägsutbredning, försvagning av signalen på vägen och interferenser. Detta kan skapa snabba förändringar och förutsättningar som kan vara svåra att prediktera, vilket i sin tur gör det svårare att skapa ett system med en viss garanterad fördröjning, genomströmning etc. En annan aspekt som påverkar tjänstekvalitetn är att noderna i ett ad hoc-nätet har begränsade resurser. Två kritiska parametrar som i stor grad påverkar förmågan att tillhandahålla tjänstekvalitet är bandbredd och energi.

Nätets utseende ändrar sig även över tiden med avseende på position och existerande länkar, d v s nätet har en dynamisk nättopologi, vilket bl a beror på mobilitet hos noderna. Detta försvårar förmågan att garantera tjänstekvalitet i nätet. Ett exempel på detta är att om en taltjänst, som kräver en låg fördöjning, skickas över en lämplig väg i nätet och denna väg får ett länkavbrott någonstans så måste en ny väg hittas i nätet och tjänsten omdirigeras den vägen. Denna återupprättelse av en ny väg och omdirigering leder till fördröjningar som i sin tur kan leda till att paket är för gamla när de väl kommer fram till destinationen. Nättopologin påverkar även kapaciteten i nätet som i sin tur påverkar förmågan att tillhandahålla tjänstekvalitet. Om t ex nätet är näst intill delat i två subnät som dock hålls samman till ett nät via ett fåtal noder i form av en hästsko kan interferenen mellan subnäten vara så hög (tillräcklig för) att den spatiella återanvändningen försämras. En försämrad spatiell återanvändning ger en försämrad

kapacitet i nätet vilket i sin tur kan innebära t ex en sämre förmåga att garantera en viss fördröjning i nätet.

Ytterligare en aspekt som försvårar förmågan att tillhandahålla tjänstekvalitet är att respektive nod (troligen) saknar precis information om tillståndet i nätet. Det är önskvärt att noden har information om tillstånd på länkarna så som fördröjning, paketförlust, bitfel, avstånd etc. samt information om vad tjänsterna ställer för krav på tjänstekvalitetn. Dessa tillstånd är dock naturligt onoggranna p g a den dynamiska nättopologin och radiokanalens egenskaper. T ex kan ett beslut som tas för trafikstyrningen vara felaktiga eftersom noderna saknar precis information om tillståndet i nätet, vilket kan resultera i att paket inte hinner fram i tid.

Om ett konfliktfritt accessprotokoll av t ex TDMA-typ (Time Division Multiple Access) används i nätet är det lättare att garantera någon form av tjänstekvalitet eftersom noderna har tilldelats en fix resurs. Detta innebär att noden endast behöver vänta en bestämd tid på att få sina tidluckor, vilket ger en garanterad fördröjning. Ett konfliktlösande protokoll, t ex CSMA (Carrier Sense Multiple Access), har inte denna fixa kanaltilldelning och det blir därmed svårare att garantera fördröjningen. Denna typ av protokoll är också mer lämplig för låga trafiklaster eftersom det blir mycket kollisioner vid höga belastningar. Ett konfliktfritt protokoll däremot fungerar inte bra vid skuraktig trafikbelastning och har ett bättre resursutnyttjande vid en hög trafikbelastning i nätet, relativt ett konfliktlösande protokoll. Detta beror på att tilldelade resurser inte används, t ex tidluckor går tomma, vid låg trafikbelastning och vid skuraktig trafikbelastning kommer en del noder ha för lite resurser medan andra noder har alldeles för mycket resurser.

Att alltid uppfylla alla de krav som tjänsterna ställer på nätet är inte möjligt, utan det handlar istället om att utnyttja och göra det bästa av de tillgängliga resurserna som finns.

2.5.1 Prioritet

En metod för att försöka tillhandahålla tjänstekvalitet vad gäller fördröjning är att använda sig av en prioritetskö på länklagret. När informationen inkommer till noden i form av paket köas dessa i noden innan de skickas ut på kanalen. Genom att sätta en prioritet på paketen beroende på vad de har för krav på fördröjningen kan ett paket med krav på låg fördröjning gå före i kön medan ett

paket med lägre krav på fördröjning får lämna plats till detta paket med högre prioritet. Paketet med lägre prioritet sänds först då när kön är tom på paket med högre prioriet. Exempel på paket med högre prioritet skulle kunna vara paket som genereras av en taltjänst. Problem med denna form av prioritetskö är att om det blir mycket paket med högre prioritet komer aldrig paket med lägre prioritet att skickas, d v s denna trafik kommer då att tryckas undan, samt att om trafikbelastningen blir tillräckligt hög kommer inte paketen fram i tid trots att endast paket med högre prioriet skickas. Detta beror på att paketen får vänta så länge i kön.

Paket i en kö kan, som nämnts tidigare, prioriteras utifrån det tekniska kravet, d v s prioritering bygger på att tjänsten ställer ett visst krav på fördröjningen för att tjänsten ska fungera. Det finns även en annan aspekt på hur paket kan prioriteras i nätet. Beroende på hur viktigt en användare anser att information är, t ex om det är ett opilmeddelande eller ett alarmmeddelande, så bör paketen ha olika prioritet. I detta fall tas ingen hänsyn till vad tjänsten har för tekniska krav utan endast vad användarer anser att informationen har för prioritet. Om t ex paket genererade av en filöverföring får en högre klassning än paket genererade av en taltjänst kan detta leda till att taltjänsten inte fungerar. Om istället prioriteten hade gjorts utifrån en rent teknisk aspekt hade kanske taltjänsten fungerat och filöverföringen ändå hunnit fram inom rimlig tid. Det är alltså möjligt att prioritera på olika sätt i nätet och det ger i sin tur olika konsekvenser.

2.6 Säkerhet

En grundläggande del i ett ad hoc-nät är fungerande, tillförlitlig och säker kommunikation. Ad hoc-nät kan i militära sammanhang verka i en fientlig miljö, vilket ökar risken för olika attacker på kommunikationen. Data som skickas i nätet måste skyddas så att den inte förvrängs, förstörs, förfalskas, avlyssnas, försvinner etc. Dessa krav innebär att IT-säkerhet måste integreras i nätet på olika nivåer. Det kan även vara viktigt att säkerheten byggs in redan från början eftersom det kan kosta mycket mer att lägga till det efterhand.

Eftersom kommunikationen i ett ad hoc-nät är trådlös, vilket är ett broadcast medium, är det svårare att skydda jämfört mot trådbunden kommunikation. Den viktigaste aspekten är dock att ad hoc-nät har en distibuerad nätstyrning. Det innebär att nätet saknar centraliserade enheter som annars med fördel kunde

hanterat säkerhetsmekanismer så som autentisering av noder, d v s verifiera en nods identitet. Den distribuerade nätstyrningen öppnar även upp för eventuella säkerhetsattacker genom att den bygger på att noderna i nätet samarbetar, t ex vid routingen. Nätets begränsade resurser, som t ex bandbredd, påverkar även förmågan att tillhandahålla säkerhet i nätet. Autentisering av noder kräver t ex mer skickande av data samt extra beräkning i noderna.

Kapitel 3

Tjänster

Det finns en mängd olika tjänster som måste stödjas av nätverket. Vilka dessa tjänster är varierar från nätverk till nätverk beroende på vad nätverket är till för. Vi kommer här att presentera ett antal olika tjänster som är intressanta då de dels visar spännvidden av tjänsterna och dels då de ställer olika krav på nätverket. Nätstyrningen måste vara anpassad för de grundläggande tjänster som ska kunna köras i nätverket, om inte så är fallet kan vissa tjänster fungera dåligt eller inte alls. Ett exempel på detta är att om prioritetshantering saknas kommer inga garantier kunna ges på fördröjning i ett nät med mycket trafik och QoS kommer alltså bara att kunnas få för tjänster som "saknar" fördröjningskrav.

3.1 Olika typer av informationsöverföring

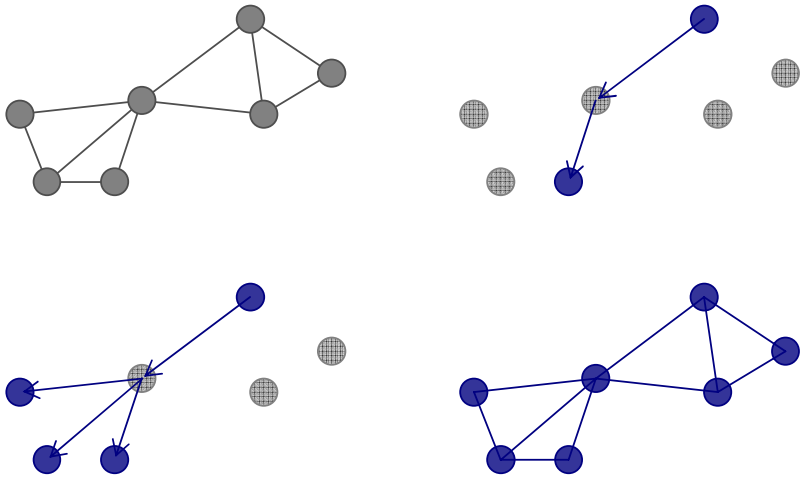
En möjlig indelning av tjänsterna kan göras baserat på vilken typ/vilka typer av informationsöverföring som är aktuell. Överföring kan ske med unicast, multicast, broadcast eller en kombination av dessa. Skillnaden mellan dessa överföringstyper kommer att förklaras nedan:

Unicast är kommunikation mellan två specifika noder, trafiken kan dock reläas av andra noder. Ett klassiskt exempel på en unicast sändning är ett vanligt telefonsamtal.

Multicast är kommunikation från en nod till en specifik grupp av noder. Ett exempel på multicast är att skicka e-post till en grupp av kollegor.

Broadcast är ett specialfall av multicast. Det finns två olika betydelser av broadcast:

- En nod sänder ett meddelande till alla andra noder som kan uppfatta den. Ett exempel på här är amatörradiosändningar på fria frekvensband där alla som hör får lyssna/svara.
- En nod sänder ett meddelande som reläas vidare till alla noder som ingår i nätet. Detta är den betydelse vi använder i denna rapport.



Figur 3.1: Ett exempel på ett helt förbundet nätverk finns överst till vänster. Överst till höger visas unicastöverföring. Multicast- respektive broadcastöverföring visas nere till vänster respektive nere till höger.

Multicast är mer komplext än broadcast. För att kunna använda multicast måste man dela in nätet i ett antal grupper. Att upprätthålla vägar till alla enheter som ingår i någon av de grupper man själv ingår i kräver extra overhead-trafik. Att vägarna från en nod till de andra i gruppen är uppdaterade betyder dessutom inte nödvändigtvis att mottagarna av meddelandet också har uppdaterade vägar till sändaren. Om nätet är mobilt kan en stor mängd uppdateringar av vägar vara nödvändiga och därmed genereras mycket overhead-trafik. Om en grupp

innehåller en stor andel av enheterna i nätet kan det till och med vara effektivare att sända meddelandena via broadcast än att försöka hålla vägarna inom gruppen uppdaterade. Huruvida multicast eller broadcast är den tekniska lösning som används märker användaren inte något av men det påverkar nätstyrningen och nätverkets design.

3.2 Tal

Taltjänsten är en grundläggande tjänst i många militära nätverk. En taltjänst kan vara både unicast (ett telefonsamtal mellan två personer) och multicast (ordergivning över radio till underlydande enheter). Taltjänsten kan också vara via broadcast, ett exempel här är radiosändning av alarmmeddelande om B- eller C-stridsmedel.

En taltjänst ställer inte så höga krav på nätets kapacitet som fil- eller videoöverföringar. Däremot kan det finnas krav på att nätverket ska kunna hantera prioritet, vissa samtal (t ex alarm- och blixtmeddelanden) måste kunna få "stjäla" nätkapacitet från andra samtal eller tjänster då de innehåller mycket viktig information. En taltjänst ställer också krav på fördröjningen. Fördröjningen ska vara relativt låg, vid samtal via satellit kan man dock vara tvungen att acceptera fördröjningar i storleksordningen flera sekunder men detta minskar den upplevda sambandskvaliteten åtskilligt. Fördröjningen bör vara relativt konstant under hela samtalet.

Problem kan också orsakas av till exempel störninger, interferenser eller dåliga kommunikationsförhållanden. Detta kan i fallet med digital radio leda till paketförluster, paket som kommer i fel ordning för att de tagit olika vägar genom nätet eller fått vänta olika länge på att få tillgång till kanalresurserna eller korrupta paket vars innehåll inte går att tyda (rätt). En del av detta kan korrigeras via nätstyrningen; paket kan (inom rimliga gränser) läggas i rätt ordning, felrättande koder kan utnyttjas och så vidare. Alla korrigeringar leder dock till ytterligare fördröjningar varför man i praktiken måste acceptera vissa förluster och hoppas att operatören kan uppfatta meddelandet trots kvalitetsförsämringen. Om sändningen är analog, är det helt upp till operatören om han/hon kan förstå vad som sägs trots distorsionen.

3.3 Filöverföring

Filöverföring kan till exempel innebära utväxlande av e-post eller överföring av ett dokument. Här är kraven på överföringshastighet och fördröjningar lägre. Kraven på överföringskvalitet är dock högre, filen ska nästan alltid öppnas eller köras av någon applikation hos användaren och det räcker ofta med att några enstaka tecken blir fel i filen för att den inte ska gå att läsa eller använda.

Ett sätt att öka kvaliteten är att använda så kallad *felrättande kodning*. Genom att använda en kodningsalgoritm på filen lägger man till extra bitar/tecken i varje paket. Detta gör att man kan upptäcka respektive rätta ett antal överföringsfel. Generellt sätt kan man upptäcka fler fel än man kan rätta men det går i ett sådant läge att begära omsändning av (en del av) filen och felen kan då korrigeras på detta sätt istället. Eftersom en del av varje paket måste avsättas till kodningens extra tecken så minskar mängden informationsbitar i varje paket. Detta behöver inte medföra att mängden överförd infromation minskar eftersom de extra kodningsbitarba gör att fler paket tas emot korrekt (då uppkommna fel kan rättas) och därmed kan ökad kapacitet i nätet erhållas.

Filöverföring kan, beroende på situationen, vara av uni-, multi- eller broadcasttyp. Även här kan hantering av prioritet vara en viktig fråga. Om till exempel en fil kommer att ta 30 minuter att överföra kanske nätstyrningen måste kunna pausa överföringen en liten stund för att skicka annan, högre prioriterad, trafik som behöver uttnyttja de kanalresurser som filöverföringen lagt beslag på.

3.4 Realtids-video

Överföring av realtids-video kan ses som ett specialfall av tal. På liknande sätt som i en taltjänst finns ett krav på låg fördröjning för att upprätthålla realtidskraven. Dessutom är realtids-video avsedd att tittas på direkt av användaren och detta gör att kvalitetskraven kan sänkas - lite brus eller enstaka pixelbortfall i bilden får oftast inga allvarligare följder. Exempel på detta är kommersiella tjänster som NetMeeting eller videokonferens.

Att överföra bild och ljud kräver mer kapacitet än att bara överföra tal eller data/text. Detta innebär att de enheter som vill kunna kommunicera via realtidsvideo måste vara förbundna med länkar med hög kapacitet. Detta kan till exempel åstadskommas genom att dessa länkar har stor tillgänglig bandbredd och/eller kan använda en hög överföringshastighet. Hög överföringshastighet

är bara möjlig om sambandskvaliteten är god. Om någon av de inblandade enheterna befinner sig på en postion med dåliga kommunikationsförhållande kan därmed en höjning av överföringshastigheten vara omöjlig att genomföra utan att kvaliteten sjunker oacceptabelt mycket.

3.5 Eldledning

Överföring av eldledningsdata kan ses som ytterligare ett specialfall av filöverföring. Eldledningsdata är oftast mycket små paket (till exempel en positionsangivelse) men denna typ av data har mycket hög prioritet och ställer också krav på låg fördröjning och överföringskvalitet. Dessutom är någon form av garanti för att informationen faktiskt nådde mottagaren önskvärd.

3.6 Situation Awareness

En tjänst som diskuterats mycket de senaste åren är *Situation Awareness (SA)*. Detta innebär att man har en tjänst som tillhandahåller information om de olika enheterna i nätverket. Exempel på sådan information är position, kurs, fart, tillgång till drivmedel och hur mycket ammunition som finns kvar. I de flesta utföranden innebär denna tjänst att en enhet dels sänder SA-meddelanden med bestämda mellanrum och dels prenumererar på information från de andra noderna i nätet. Oftast vill man ha frekventare uppdatering av information som berör noder nära ens egen enhet än av information om noder långt borta. Tjänsten är av sin natur nästan alltid en multicast tjänst.

Om SA-information används för t ex eldgivning i närheten av egen trupp så är det ytterst viktigt att ha färsk positionsinformation för att undvika vådabeskjutning. Nätverket måste då uppfylla höga krav. Både hög uppdateringstakt och låga fördröjninger behövs, speciellt för att hantera mobila enheter. Samtidigt måste informationskvaliteten vara god för att undvika bl a fel i positionsangivelserna.

En SA-tjänst skickar vanligtvis många små paket innehållande information om en enhet i nätet. Tjänsten kan ta upp en stor del av nätverkets kapacitet. Andelen ökar då kraven på uppdateringstakt och maximal tillåten fördröjning skärps. Kapacitetsåtgången för tjänsten påverkas också av de valda nätstyrningsprotokollen. Om accessprotokollet t ex inte kan hantera varierande paketstorle-

kar utan använder principen en kanalresurs (t ex en tidlucka) per paket så innebär många små paket att kanelen "går tom" en stor del av tiden och inte kan användas för annan trafik. Om protokollet istället kan samla ihop flera små paket och skicka dem gemensamt (t ex i samma tidlucka) utnyttjas kanalresurserna effektivare och kapacitetsåtgången sjunker. Ett sätt att komma ifrån problemet med att delar av tidsluckan "går tom" är att istället för att skicka många små paket skicka större tabeller som innehåller information om flertal enheter. Fördröjningen kan då öka eftersom

Valet av routingprotokoll kan också påverkas om man vill ha en SA-tjänst. Det är extra svårt att ge garantier på fördröjningar och uppdateringstakt om man använder ett reaktivt protokoll där en ny väg genom nätet måste skapas varje gång ett SA-paket ska skickas. Ett proaktivt routingprotokoll ger betydligt bättre kvalitetskontroll eftersom protokolluppdateringar skickas med jämna mellanrum. I vissa (proaktiva) protokoll är det också möjlighet att kombinera sändningen av SA-paket med den kontrolltrafik som trafikstyrningsprotokollet ändå sänder, fördröjningarna hos SA-paketen blir då direkt beroende av hur ofta protokollet uppdaterar vägarna i nätet [2].

3.7 Best-effort

Vissa tjänster är av så kallad *best-effort*-typ. Detta är tjänster som "saknar" tidskrav, d v s det ställs väldigt låga krav på fördröjningen. Ett exempel på en sådan tjänst är vissa typer av filöverföringar, ett annat exempel är surfande på internet - det gör oftast inte så mycket om det tar en stund innan sidan laddats hem.

Eldledning är ett exempel på en tjänst som inte får vara best-effort. Realtidsvideo bör inte heller vara best-effort om kvalitetskrav finns.

Kapitel 4

Forskningsområden

Detta kapitel beskriver och presenterar några resultat från vår forskning inom tre olika områden som är viktiga för ad hoc-nät; *access*, *routing* och *tjänstekvalitet*. En mer detaljerad och teknisk beskrivning av vad vi har gjort finns i [1].

4.1 Access

Noderna i ett ad hoc-nät måste dela på den gemensamma kanalresursen. Vi har fokuserat våran forskning på STDMA (*spatial reuse TDMA*) som är ett konfliktfritt protokoll som kan ge höga kapaciteter och har bra egenskaper för att kunna erbjuda hög tjänstekvalitet. Vi ger här en översiktlig beskrivning av STDMA, för en mer utförlig teknisk beskrivning se [3].

4.1.1 STDMA

STDMA är ett konfliktfritt acessprotokoll utvecklat för ad hoc-nät. STDMA står för *spatial reuse TDMA* och innebär såsom TDMA att kanalresursen delas upp i tidluckor för att lösa kanaltilldelningsproblemet, men om noderna är tillräckligt långt ifrån varandra så kan de få använda samma tidlucka. Eftersom varje nod har bestämda konfliktfria tidluckor har protokollet naturliga fördelar för att ge fördröjningsgarantier. Det är också möjligt att uppnå höga kapaciteter genom att låta så många som möjligt återanvända tidluckorna.

Problemet är dock att ta fram sändningsscheman som säger när varje nod får sända, speciellt för att inte bara låta varje nod få en tidlucka utan också kunna ta

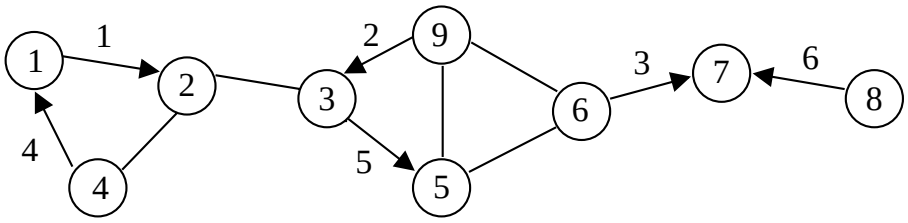
fram algoritmer ger scheman med önskvärda egenskaper. Exempelvis kan man vilja ta fram schemana distribuerat och/eller skapa scheman som uppfyller de fördröjningskrav som vissa tjänster kräver.

Innan vi diskuterar STDMA mera visar vi ett litet exempel på ett radionät. I figur 4.1 visar vi en grafrepresentation av ett 9 nods nät. Vi kan här se att länk 1,2, och 3 kan dela en tidlucka då de är tillräckligt långt från varandra. En annan uppsättning är 4, 5 och 6, men inte 1, 5, och 6 eftersom vi här antar rundstrålande antenner och när nod 3 sänder kommer den att störa mottagningen i nod 2.

Från en sådan graf kan man avgöra vilka noder eller länkar som kan sända samtidigt och detta används för att skapa ett helt schema. Tyvärr kommer det inte fungera så länge då noderna flyttar sig och noder som tidigare kunnat sända samtidigt nu inte längre kan det.

Man kan lösa detta på olika sätt. Ett sätt är att samla in allting till en central punkt när något händer, sedan skapa ett nytt schema som sänds ut till hela nätet. Fördelarna med detta är att den centrala punkten kan skapa ett mycket effektivt schema som utnyttjar kanalresursen effektivt, nackdelen är att om nätet är stort eller rör sig snabbt riskerar schemat vara dåligt redan då det når noderna. Dessutom blir det inte en robust lösning eftersom en utslagning av den centrala noden får så stora konsekvenser.

En alternativ lösning är att uppdatera schemat distribuerat, d v s bara låta den lokala omgivningen till en förändring reagera på en förändring. Detta kräver dock en algoritm som kan hantera lokal information på ett effektivt sätt.



Figur 4.1: Ett 9-nods nät exempel.

Nätmodeller

För att kunna avgöra vilka noder som kan sända samtidigt behöver en model av radionätet. De mest använda modellen för ad hoc-nät är den grafbaserade som vi använde i vårt exempel ovan. I denna antar man att radioräckvidden är begränsad (vanligtvis cirkulärt) och bortom denna räckvidd skapas inte ens interfenser hos andra noder. Använder man denna model kan enkelt ta fram algoritmer för att ta fram scheman med hjälp av grafteori. Nackdelen med den är att den inte beskriver radiomediet speciellt väl då den inte tar hänsyn till den sammanlagda interferensen från flera störande noder. Dessutom kan den inte hantera fall där en mottagen signal är tillräckligt stark för att klara av existerande interferenser.

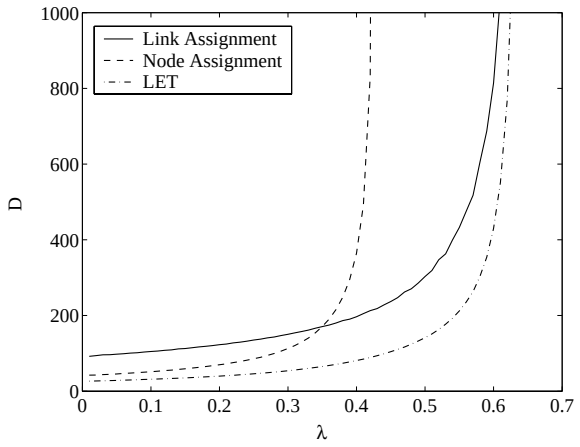
En mer realistisk modell är en den interferensbaserade modellen, där ett paket antas kunna tas emot om den mottagna signalen är tillräckligt stark i förhållande till bruset och summan av alla interfererande signaler. Användningen av interfernsbaserade modellen har varait focus för mycket av STDMA foskningen och mycket av de följande påståendena baseras på denna modell.

Tilldelningsstrategier

I exemplet ovan ges sändingsrättigheterna till länkarna, d v s både sändare och mottagare är bestämda i förväg. Detta kallas *länktilldelning*, en annan tilldelningsstrategi är *nodtilldelning*, i detta fall bestäms bara vilken nod som ska sända i en tidlucka, mottagare kan vara vilken som helst av dess grannar (eller alla).

Länktilldelning har fördelen att bara kräva konfliktfrihet i den mottagare som verkligen tar emot ett sänt paket. I nodtilldelning måste alla grannar kunna ta emot ett meddelande konfliktfritt då man i förväg inte kan veta vem sändaren skickar till. Det här leder till högre *spatiell återanvändning* för länktilldelning, d v s tidluckan kan återanvändas för fler sändare. Å andra sidan kan nodtilldelning användas för multicast och eftersom det finns färre noder än länkar krävs kortare protokoll vilket för lägre trafiklaster ger kortare fördröjning.

Det går dock utvidga länktilldelning till *LET (Link assignment with Extended Transmission rights)*, som utvidgar ett länkschema och låter noder sända även till andra än de förutbestämda mottagarna. I medel ger denna tilldelningsstrategi lägst fördröjning men kan inte garantera en bättre fördröjning än länktilldelning och inte hantera multicasttrafik lika bra som nodtilldelning. I figur 4.2 visas fördröjningen som funktion av trafiklasten för *länktilldelning*, *nodtilldelning* och *LET*.



Figur 4.2: Medelfördrjning för ett 30-nodersnät för olika tilldelningsstrategier.

Schemalängd

Eftersom noderna även reläar andra noders trafik kommer trafiklasten på de olika länkarna nätet vara mycket olika. Länkar som kopplar ihop två delar av nätet behöver hantera mycket mer trafik än en länk i utkanten av nätet. För att hantera detta använder man trafikadaptiva scheman, d v s en vissa länkar eller noder får multipla tidluckor i relation till deras trafiklast.

Att ge flera tidluckor till vissa noder eller länkar påverkar också schemalängden. Helst vill man ge varje länk tidluckor i proportion till trafiklasten på den men för att göra detta kräbvs en lång schemalängd, vilket är olämpligt för exempelvis distribuerade algoritmer som behöver förhandla om rättigheterna att sända i varje tidlucka.

Viken schemalängd som är bäst blir en avvägning mellan mobilitet och kapacitet på länkarna. För låg mobilitet och hög datatakt blir overhead-trafiken låg och en lång schemalängd med hög kapacitet kan bibehållas. Om mobiliteten blir hög i förhållande till datatakten kommer overhead-trafiken äta upp en stor del av den kapaciteten vid långa schemalängder.

Viktigt att ta hänsyn till är också att nodtilldelning kräver färre tidluckor för utjämning eftersom det finns färre noder och mindre variation i trafiklast än över länkarna. Detta innebär att för hög mobilitet kan nodtilldelning vara att föredra

även om den under ideala förhållanden kan uppnå högre kapacitet. En bättre lösning är dock att använda en kombination av tilldelningsmetoderna. Varje nod tilldelas en tidlucka, men resten av schemat tilldelas länkar. Denna metod ger höga kapaciteter även för låga schemalängder då den nodens tilldelade tidlucka hjälper till att jämna ut trafiken i en nod.

Distribuerad Schemaläggning

Att ta fram distribuerade algoritmer är en viktig del av STDMA-forskning som har utförts. De flesta algoritmer är dock framtagna för att bara fungera än för att vara effektiva i olika situationer. Ett antal egenskaper är önskvärda i en distribuerad STDMA-algoritm förutom att den ska hantera de egenskaper vi redan nämnt ovan. Exempelvis behöver schemalängden kunna varieras beroende på förbundenheten i nätet. Detta ska helst kunna ändras under gång och ska leda till så få globala (hela nätet) effekter som möjligt. En möjlighet att låta schemalängden ändras med en faktor två hela tiden då det möjliggör olika schemalängd i olika delar av nätet.

Det är också önskvärt att en distribuerad algoritm ger så effektiva scheman att de blir jämförbara med vad en centraliserad algoritm kan ge (i alla fall om overhead-trafik ignoreras). Dessutom bör den vara adaptiv så detta gäller vid förändringar utan behov av manuell omkonfiguration. Exempelvis från mobilt utspritt nät till statiskt nät där alla har samgrupperat.

Vi har utvecklat en distribuerad interfernsbaserad algoritm i ett första steg i att ta fram en STDMA algoritm med lämliga egenskaper. Alla tidigare existerande algoritmer har i en eller annan form utnyttjat den graphbaserade modellen för att ta fram scheman distribuerat. Overhead-trafiken för vår algoritm är fortfarande tämligen hög, speciellt för hög mobilitet, men de genererade schemana fungerar bra vilket kan ses vid en jämförelse med CSMA.

Jämförelse med CSMA/CA

CSMA står för *Carrier Sense Multiple Access* och fungerar i princip såsom att när en nod har ett paket lyssnar den på kanalen för att se om någon använder den. Om så inte är fallet kan noden sända. CA står för *Collision Avoidence* och är ett tillägg för att hantera det så kallade *Hidden terminal*-problemet, d v s man lyssnar för att se om kanalen är använd i sändaren, men kollisioner sker i mottagaren och störande signaler i mottagaren kan vara utom räckvidd för sändaren. I detta fall sänds en kort begäran om att sända (RTS) och mottagaren

svarar om det går (CTS). Om mottagaren är störd förloras bara det korta RTS-paketet.

IEEE 802.11 är baserad på CSMA/CA är det klart mest använda accessprotokollet för ad hoc-nät idag. Anledningen är att det är en existerande standard och WLAN komponenter kan köpas billigt idag. Det är också ett enkelt protokoll att implementera och göra tester på och det kan hantera hög mobilitet. CSMA har dock några egenskaper som gör det mindre lämligt i ad hoc-nät än vad man kan tro från antalet som använder det:

- Paketstorlek: CSMA/CA är effektivast på långa paket så att RTS och CTS-paketen tar kort tid att sända i jämförelse med det riktiga palketet. Vändtiden från att lysnna till att sända på kanalen leder till samma konsekvens. STDMA har inte detta problem utan ger minst fördröjning för små paket. Stora paket kan delas upp i mindre av applikationerna (eller TCP). Att sätta ihop små paket till stora leder till fördröjningar, något som är oacceptabelt i t ex en taltjänst. CSMA tappar en mycket stor del av sin kapacitet just för taltrafik.

- Multicasttrafik: För låga trafiklaster fungerar CSMA normalt sett bra då få noder samtidigt försöker få tillgång till kanalen. Ett problem är dock när man vill nå många noder i nätet med ett paket. Ett paket kan nå flera noder på en gång och behöva återsända paketet samtidigt. Detta kan leda till att ett paket kolliderar med sig självt fast utsänt från andra noder. I STDMA med nodtilldelning tillåts endast fler sändningar samtidigt om de inte leder till konflikter.

- Fördröjningsgarantier: Vid låga trafiklaster ger CSMA normalt sett låga fördröjningar, men vid högre laster har protokollet en tendens låta vissa sessioner slumpmässigt “fånga” kanalen medan andra inte får någon kapacitet. Detta leder till stora varianser i fördröjning vilket inte är bra för fördröjningskänsliga applikationer.

CSMA har dock fördelen av att inte påverkas speciellt mycket av ökad mobilitet vilket har en klar fördel i mobila nät men mindre effektiva sättet att utnyttja kanalen ger att denna fördel mot STDMA först blir relevant för mycket höga mobiliteter. I [1] ges en mer utförlig jämförelse mellan de båda protokollen som visar att STDMA klarar av att hantera betydligt fler samtidiga användare än CSMA för låg mobilitet (speciellt för taltrafik där STDMA kan hantera tre gånger

så mycket trafik). Skillnaden är mindre för filtrafik då CSMA kan använda stora paket. För hög mobilitet är skillnaden mindre mellan protokollen. En annan skillnad är att i CSMA har man mindre kontroll på vilka kommunikationspar som tappar sin session, i STDMA kan detta styras bättre.

4.2 Routing

Vi kommer här att ge en översiktsbild över den forskning på routingprotokoll som vi har bedrivit. Genom att studera ett proaktivt respektive ett reaktivt trafikstyrningsprotokoll, båda avsedda för ad hoc-nät, har vi haft möjlighet att utforska skillnaderna mellan dessa typer av protokoll. Protokollen vi har valt att titta på är *Fisheye State Routing (FSR)* och *Ad Hoc On-Demand Distance Vector (AODV)*. Hur dessa fungerar och våra resultat rörande respektive protokoll förklaras i korthet nedan. Se [4], [5] och [6] för mer detaljerad information.

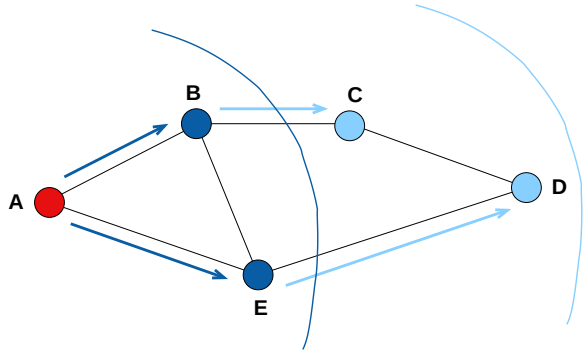
4.2.1 FSR

FSR är ett distribuerat, proaktivt trafikstyrningsprotokoll. “Fisheye” i protokollets namn syftar på att en fisk bara ser skarpt i mitten av sitt synfält och sedan allt suddigare ut mot kanterna. Protokollet är uppbyggt på samma sätt, noden har bäst information om noder i sitt närområde och sedan gradvis sämre information om noder ju längre bort de befinner sig.

Hur fungerar FSR?

Eftersom FSR är ett proaktivt protokoll skickar varje nod ut informtion om sig själv med en viss periodicitet. Dessa uppdateringar utgör overhead-trafik och det är önskvärt att hålla denna så liten som möjligt. För att hantera detta delar varje nod in resten av nätet i zoner och hur ofta den skickar information om sig själv till en viss nod beror på vilken zon noden tillhör, se figur 4.3.

När en nod (källa) i FSR ska sända nyttotrafik har den i princip alltid en väg färdig till destinationen eftersom protokollet hela tiden håller alla möjliga vägar i nätet uppdaterade. Det är dock inte säkert att källan har fått de senaste uppdateringarna. Källan skickar meddelandet, på den senaste väg den vet om, till destinationen och mellanliggande noder som känner till en bättre/nyare väg styr in meddelandet på denna väg istället. Detta innebär att vägen förbättras under



Figur 4.3: Ett exempel på zonindelning i FSR. Information om nod A skickas oftare till nod B än till nod C eftersom B ligger i en zon närmare A. Zonindelningen är här baserad på hur många hopp från A noden ligger.

hela meddelandets färd till destinationen.

Vad har vi försökt uppnå och varför?

FSR är ett intressant exempel på ett proaktivt protokoll. Att vi valde just detta protokoll berodde på att dess indelning av nätet i zoner har en motsvarighet i kraven på uppdatering hos en SA-tjänst. Vi såg i detta en möjlighet att prova att kombinera spridningen av trafikstyrningsmeddelanden med spridningen av SA-information. Detta innebär en möjlighet att merutnyttja overhead-trafik, som ändå måste sändas i nätet, till att överföra nyttotrafik för en relativt kapacitetskrävande tjänst.

Det ingår en mängd parametrar i FSR, hur dessa skall sättas för att maximera den kapacitet som är tillgänglig för nyttotrafik är en viktig fråga. Det är önskvärt att hålla overhead-trafiken så låg som möjligt men samtidigt vill vi ha så bra vägar som möjligt. Samtidigt vill vi ha så bra vägar som möjligt. Dessa två krav står i konflikt med varandra. Vi har därför tittat på och tagit fram olika mått för väga samman dessa faktorer och mäta/beräkna hur stor andel nyttotrafik vi kan skicka.

Några resultat och slutsatser

Vi har för ett antal olika nätverk jämfört hur tillgänglighet och andel nyttotrafik i näten påverkas av vilka värden som satts på parametrarna i FSR. Tillgänligheten

är här definierad som den andel vägar som FSR hittar, jämfört med de vägar som skulle hittas av ett optimalt routingprotokoll.

Tillgängligheten minskar när näten är mindre sammanbundna, vilket troligen beror på att det är svårare att finna vägar i dessa nät. Om tiden mellan uppdateringarna ökar, sjunker också tillgängligheten eftersom vägarna då skapas baserat på gammal information. Hur stor andel av nätets kapacitet som är tillgänglig för nyttotrafik är kraftigt beroende av valda parametervärden.Värdena måste väljas anpassat för den kapacitet nätet i fråga har, annars kan prestandan sjunka kraftigt

Det är fullt möjligt att kombinera overhead-trafiken i FSR med distribution av SA-information [2]. För att kunna uppfylla krav på tjänstekvalitet bör SA-informationen spridas med de overhead-paket en nod skickar om sig själv. Kraven på SA-tjänsten, t ex maximalt positionsfel för enheter inom ett visst avstånd, kommer dock att översättas till krav på uppdateringstakten i FSR. Detta innebär en inskränkning av vilka värden som kan väljas för de olika parametrarna i FSR.

4.2.2 AODV

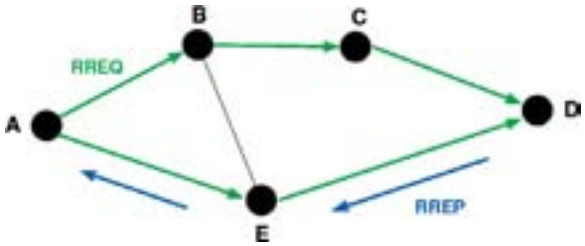
Eftersom AODV är ett reaktivt protokoll skapas en väg mellan två noder först då den ena (källan) vill skicka nyttotrafik till den andra (destinationen).

Hur fungerar AODV?

När en nod behöver en ny väg skickar den via broadcast ut ett trafikstyrningspaket, Route Request (RREQ), som frågar efter en väg till destinationen. När destinationen, eller en mellanliggande nod som känner till en väg till destination, tar emot RREQ-paketet svarar den med ett RREP-paket (Route Reply). När källan nås av RREP-paketet är vägen klar att använda för nyttotrafik. I figur 4.4 ges ett exempel på hur RREQ och RREP skickas i nätet. För mer detaljerad information, se [6].

Egna modifieringar och motiv till dessa

Det kostnadsmått som används i AODV är min-hopp, d v s protokollet försöker minimera antalet hopp som ingår i en väg. Som nämnts i kapitel 2.4.1 är detta inte alltid det bästa sättet att maximera överföringskapaciteten vare sig på vägen eller i nätet som helhet. Det är dessutom mer troligt att en väg med få (men långa) länkar drabbas av avbrott än att en väg med fler (men kortare)



Figur 4.4: Ett exempel på hur RREQ och RREP för AODV sprids i nätet då nod A behöver en väg till nod D.

länkar gör det, d v s maximal robusthet i nätverket är svår att uppnå med detta kostnadsmått.

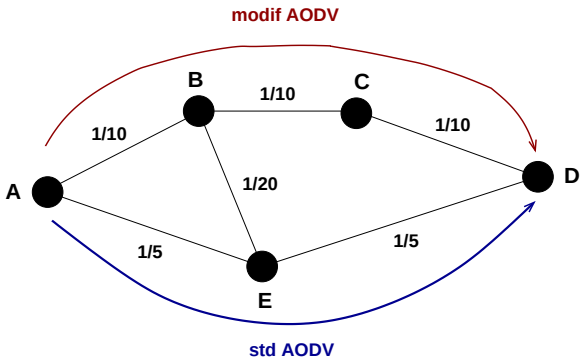
Vi ville därför undersöka om det var möjligt att modifiera ett reaktivt routingprotokoll, på vilket AODV är ett bra exempel, så att ett kostnadsmått baserat på andra faktorer kan användas. Hur svårt är det att göra detta? Hur mycket förbättring ger modifikationen?

Vi valde ett enkelt alternativt kostnadsmått som dock ändå kan ta hänsyn till nodernas (eller länkarnas) hetrogenitet. Genom att för varje väg summera $1/datatakten$ för de ingående länkarna kan vi hitta den väg som har högst kapacitet.

Ett exempel på hur resultatet skiljer sig mellan detta mått och min-hopp visas i figur 4.5. Om nod A ska skicka trafik till nod D och min-hopp används kommer en väg $A- > E- > D$ att väljas (2 hopp). Om istället vägens kapacitet maximeras kommer vägen $A- > B- > C- > D$ att väljas (3 hopp). Kostnaderna för respektive väg enligt måttet ovan är 0.4 respektive 0.3.

Med det nya kostnadsmåttet är det inte längre säkert att det till en nod först anlända RREQ-paketet eller RREP-paketet är det som innehåller den bästa vägen fram till noden. Detta innebär att vi förutom att byta själva kostnadsmåttet i AODV behövde göra ett par andra modifieringar av protokollet:

- Mellanliggande noder kan behöva skicka vidare fler än ett RREQ-paket, om det nya paketet innehåller en bättre väg (enligt valt kostnadsmått).
- Noder måste också kunna skicka flera RREP-paket om ett nyinkommet RREQ-paket innehåller en bättre väg än den/de man redan skickat RREP-paket för.



Figur 4.5: Exempel på nätverk vars länkar har olika datatakt. Vald väg med vanliga AODV respektive med vår modifierade version.

Några resultat och slutsatser

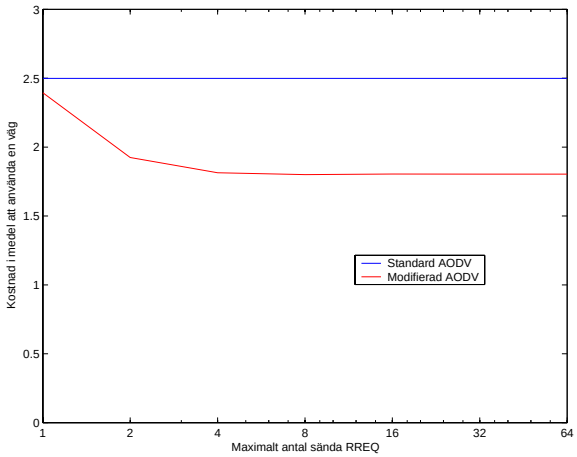
Vi har, för ett antal olika nätverk, dels jämfört kostnaden för att använda vägar genererade med olika versioner av AODV och dels jämfört den mängd overhead-trafik som behövdes för att ta fram dessa vägar. Kostnaden är här beräknad med vårt nya mått och inte min-hopp. I figur 4.6 och 4.7 visas exempel på resultat. De blå linjerna visar resultat för vanliga AODV och de röda för vår modifierade version. Resultaten visas som funktion av hur många RREQ/RREP som får skickas vidare/skickas om de innehåller bättre vägar.

Som synes i figur 4.6 resulterar våra modifikationer i att vägar med högre datatakt oftare väljs och därmed ökas kapaciteten i nätverken. Vi kan å andra sidan se i figur 4.7 att den modifierade versionen av AODV, genererar mer overhead-trafik än orginal versionen. En avvägning måste därför göras mellan kapacitetsförbättring och ökning av overhead-trafik för varje nätverk. Är vinsten med att använda ett annat, mer komplext, mått än min-hopp värt priset?

4.2.3 Slutsatser

Baserat på vår analys av AODV och FSR kan vi dra vissa generella slutsatser:

- Reaktiva och proaktiva protokoll är bra i olika situationer. Vad som ska väljas beror på en mängd faktorer och är beroenre bl a av vilka tjänster



Figur 4.6: Medelkostnad enligt vårt mått för vägar i ett 32 noders nät. Resultatet är normerat med medelkostnaden för de optimala vägarna. Detta innebär att ju närmare 1 resultaten är ju bättre är de.

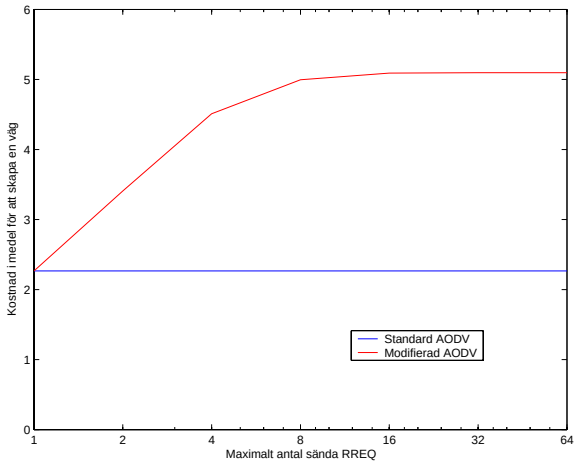
som ska användas i nätverket och vilka krav dessa ställer för att fungera.

- I de flesta protokoll måste värden på ett större eller mindre antal parametrar väljas. Dessa värden måste väljas så att de passar för nätverket ifråga och de krav på tjänstekvalitet som finns. Om dåliga val görs, kommer protokollet att fungera dåligt.

- Adaptiva trafikstyrningsprotokoll som “under gång” automatiskt ställer in bra parametervärden skulle innebära förbättrad prestanda.

- Det är ganska svårt att byta från min-hopp till ett mer avancerat kostnadsmått för reaktiva routingprotokoll. Om sådan modifiering av ett reaktivt protokoll görs, ökar protokollets komplexitet. Ökningen av overheadtrafik när ett mer komplext mått införs är dessutom större för reaktiva protokoll.

- Att använda andra kostnadsmått än min-hopp är ofta nödvändigt för att kunna maximera kapaciteten i, framför allt hetrogena, nätverk.



Figur 4.7: Overhead-trafik i medel som behövs för att skapa en väg i ett 32 noders nät.

- Det är svårare att utnyttja eventuell hetrogenitet i nätverket då reaktiva protokoll används.
- Det är enklare att uppfylla krav på tjänstekvalitet när proaktiva trafikstyrningsprotokoll används.
- Eftersom ett proaktivt protokoll alltid har vägar färdiga till alla destinationer blir fördröjningen när användaren vill skicka nyttotrafik lägre än om ett reaktivt protokoll används.
- Ett proaktivt protokoll genererar hela tiden overhead-trafik, denna kan ta en stor del av nätets kapacitet. Reaktiva routingprotokoll genererar bara trafik då en ny väg behövs och resulterar i de allra flesta fall i betydligt mindre overhead-trafik.
- En avvägning mellan krav på tjänstekvalitet och mängden overhead-trafik måste göras för varje nätverk.
- Hänsyn måste också tas till eventuellt hot från kommunikationssignalspaning (KOS) när man väljer protokoll. I en del protokoll måste nämligen noderna göra periodiska sändningar för att trafikstyrningen ska fungera

och detta innebär en ökad risk för upptäckt (och därmed också för pejlning och bekämpning).

4.3 Tjänstekvalitet

Det finns olika metoder för att försöka tillhandahålla tjänstekvalitet i nätet. Vi har i våran forskning huvudsakligen undersökt de två metoderna variabel datatakt och prioritetsköer. I detta avsnitt beskrivs dessa metoder översiktligt, för mer information och fler resultat se [7], [8], [9] och [10]

4.3.1 Ökad genomströmning med variabel datatakt

Olika datatakt på länkarna innebär att lika mycket information tar olika lång tid att sända. Beroende på vilka datatakter som används kan en nod få över olika mycket information under en tidlucka. Det bästa är att försöka utnyttja tidluckan fullt ut, d v s sända under hela tidluckan om det finns något att sända.

Vad har möjligheten att kunna utnyttja olika datatakter för inverkan på genomströmningen i nätet? Vi har försökt svara på detta genom att ge respektive nod möjligheten att kunna anpassa med vilken datatakt den sänder i diskreta steg. Om noderna ges möjlighet att kunna sänka sin datatakt kommer nättopologin förändras genom att fler länkar dyker upp i nätet och nätet blir mer sammanbundet. Den största vinsten med att kunna sänka datatakten är att ett nät kan gå från ej sammanbundet till sammanbundet.

Om noderna istället ges möjligheten att kunna höja sin datatakt, i de fall kanalförhållandena tillåter, kommmer nättopologin förbli oförändrad. De noder som inte har möjlighet att höja sin datatakt kommer att fortsätta att sända på en lägre datatakt. Genom att höja datatakten i en del noder kommer genomströmningen i nätet att öka, men de noder som fortsätter att sända med lägre datatakt kommer hålla nere genomströmningen i nätet. För att minska denna effekt är det nödvändigt att använda ett trafikadaptivt access-protokoll som ger de noder som sänder med lägre datatakt mer kanalresurser. Att noderna kan anpassa sin datatakt, både genom att sänka eller höja den, och använda ett trafikadaptivt access-protokoll ger en ökad genomströming i nätet och i vissa fall även en ökad förbundenhet i nätet.

En routingmetrik som ofta nämns är att minimera antal hopp. Att använda en sådan routingmetrik fungerar dock inte speciellt bra om variabel datatakt

används i nätet. Detta beror på att metriken inte tar någon hänsyn till vilka datatakter som noderna kan sända med vid valet av väg. Det blir till och med så att denna metrik oftast väljer att gå via de noder som sänder med lägst datatakt eftersom dessa länkar oftast är längre och antal hopp blir färre. För att kunna dra nytta av variabel datatakt och de högre datatakterna krävs det därmed att routingmetriken tar hänsyn till vilken datatakt en nod kan sända med. Istället för att kostnaden räknas i antal hopp räknas den istället som summan av ett genom datatakterna på respektive länk. Denna metrik maximerar därmed utnyttjandet av länkar med högre datatakt, d v s paketen routas över de noder som kan sända med hög datatakt. Att på detta vis basera routingmetriken på datatakten istället för hopp när variabel datatakt används i noderna ger på ett enkelt vis en avsvärd högre genomströmning i nätet.

Att hantera en fördröjningskänslig tjänst i ett mobilt nät

I ett ad hoc-nät där noderna ständigt rör sig är det en utmaning att tillhandhålla en tillräcklig tjänstekvalitet. Vad krävs t ex för att hålla nere födröjningen på paketen, så att en taltjänst fungerar tillfredsställande?

Om variabel datatakt används är det ur genomströmningssynpunkt bäst att utnyttja de vägar som använder den högsta datatakten, d v s beräkna kostnaden för vägen baserat på datatakten och inte baserat på minst antal hopp. Hög genomströmning förbättrar förutsättningarna för att kunna stödja fördröjningskänslig trafik. I ett fall där nätet är väldigt mobilt är det dock risk att det är de länkar med hög datakt som går ner först eftersom de är mer känsliga för förändringar. Detta innebär att nya vägar måste hittas i nätet. Det i sin tur skapar oönskade fördröjningar i nätet och kan leda till att en fördröjningskänslig tjänst misslyckas. Om noden istället kan anpassa sin datatakt genom variabel datatakt kan den istället för att leta reda på en ny väg sänka datatakten den sänder med och därmed bibehålla länken och vägen i nätet. På så vis kan noden fortsätta att skicka paketen samma väg, dock med en lite högre fördröjning. Om omroutingen tar lång tid kan det alltså vara bättre att för en fördröjningskänslig tjänst att noden sänker datatakten för att bibehålla vägen.

4.3.2 Tjänstekvalitet i ett nät med olika tjänster?

I ett ad hoc-nät kommer det finnas olika tjänster. Dessa tjänster har olika krav på tjänstekvalitet. Det kan t ex finnas två typer av tjänster igång, en som har ett lågt krav på tjänstekvalitet i form av fördröjning, t ex överföring av en fil, och en tjänst som har ett högt krav på fördröjning, t ex en taltjänst. Hur ska nätet kunna hantera denna kombination av olika tjänster på ett tillfredsställande sätt?

Genomströmningen för en tjänst som saknar krav på fördröjning är betydligt större än för en tjänst med krav på fördröjning. Detta beror på att vissa paket är för gamla då de kommer fram till slutdestinationen. I ett nät som är glest förbundet blir genomströmningen ännu sämre för en fördröjningskänslig tjänst eftersom antalet hopp ökar i nätet och därmed fördröjningen. När tjänster med olika fördröjningskrav finns tillgänliga i nätet samtidigt och noderna inte har någon teknik för att hantera detta fungerar en tjänst med ett högt krav fördröjning dåligt. Detta beror på att paket inte hinner fram till slutdestinationen i tid innan de är för gamla eftersom de måste dela de tillgänliga resurserna på lika villkor med paket från andra trafiktyper. För att minska effekten av detta kan prioritesköer användas eller att gamla paket slängs. Att slänga gamla paket innebär att paket i kön som är äldre än den tillåtna fördröjningen hos tjänsten kastas. Därmed tar inte dessa paket upp onödiga resurser. Att endast slänga gamla paket ger dock endast en viss förbättring för en fördröjningskänslig tjänst. Att använda prioritetsköer, d v s att låta paket med krav på låg fördröjning få gå före paket som saknar direkta krav på fördröjning, ger en klar förbättring för en fördröjningskänslig tjänst. Detta beror på att tjänsten inte påverkas i någon större utsträckning av andra trafiktyper.

Att använda prioritesköer kan dock innebära att trafik med fördröjningskrav kommer trycka undan den andra trafiken och till slut kan det bli så att det endast går trafik av denna typ och den andra trafiken utan krav på fördröjning blir helt undantryckt.

Bästa resultat ges om prioritetsköer kombineras med att slänga gamla paket. Detta ger även den högsta genomströmningen jämfört mot att endast använda prioritesköer eller slänga gamla paket eller i värsta fall att inte göra något alls.

4.3.3 Slutsatser

Att kunna anpassa datakten i noden till rådande situation kan innebära fördelar så som att genomströmningen ökar, fördröjningen minskar, att nätet blir mer förbundet eller att länkar kan upprätthållas. För att kunna utnyttja variabel datatakt krävs det att routingen beaktar datatakten vid val av väg så att utnyttjandet av högre datatakter maximeras. Det finns troligen ytterligare vinster att göra genom att väga in andra apseketer i denna routingmetrik, t ex att fler hopp kan leda till en ökad kostnad genom att det totalt blir mer beräkningar i respektive nod.

Det är även nödvändigt att de noder som av olika skäl inte kan använda högre datatakter tilldelas mer kanalresurser genom att använda ett trafikadaptivt access-protokoll. Detta innebär även en mer rättvis fördelning av resurserna i nätet.

Genom att använda prioritetsköer och slänga gamla paket förbättras förmågan att hantera en mix av tjänster med olika krav på tjänstekvalitet i ett ad hoc-nät och genomströmningen ökar.

Kapitel 5

Viktiga framtida forskningsfrågor

Som avslutning på denna rapport vill vi nämna några forskningsområden som vi anser viktiga för att skapa effektivare nätlösningar för framtida ad hoc-nät. Forskningsområderna är inte angivna i någon prioriteringsordning och vi hoppas att i framtida forskningsprojekt kunna ta oss an några av dessa.

5.1 Förbättrad tjänstekvalitet genom cross-layer design

Hur påverkas tjänstekvaliteten av den mer övergripande nätstyrningen i ett ad hoc-nät? För att kunna hantera flera olika typer av tjänster krävs någon typ av prioritering av trafiken. Tilldelningen av tillgängliga nätresurser måste vägas mot tjänstens prioritet. I ett nästa steg används routingprotokollet då en väg för trafiken ska tas fram. Detta måste matcha kanaltilldelningen, som hanteras av accessprotokollet. Att ha en bra protokollinteraktion mellan routing- och accessprotokoll är viktigt för att kunna erbjuda tjänstekvalitet.

En viktig frågeställning för ett ad hoc-nät är hur *adaptiviteten* hos noderna ska kunna utnyttjas effektivt. Adaptiva noder har flera egenskaper som är viktiga för kanaltilldelningen. Exempel på sådana egenskaper kan vara adaptiv datatakt, smarta antenner, effektkontroll och interferenshantering. Hur ska interaktionen mellan accessprotokollet och nodens adaptionsegenskaper designas på ett effektivt sätt? Denna typ av protokollinteraktion kallas *cross-layer design*.

5.2 Fördröjningstoleranta nät

De flesta som forskar inom ad hoc-nät studerar nät där det ofta finns en förbindelse, eventuellt via flerhopp, mellan källan och destinationen. Detta är dock inte möjligt i alla nät, utan man måste ibland ta hjälp av nodernas mobilitet för att kunna förmedla informatinen. Fördröjningarna kan i dessa fall bli stora. Många av dagens protokoll fungerar inte i denna typ av nät och nya protokoll behöver därför tas fram.

5.3 Interaktion av mobila ad hoc-nät med andra nät

Ad hoc-nät ska kunna fungera autonomt utan kontakt med någon fast infrastruktur. I många fall är dock noder i ad hoc-nätet i behov av att kunna kommunicera med noder i andra nät. För att detta ska fungera på ett smidigt sätt för användaren måste gränserna mellan näten hanteras på ett bra sätt. Detta blir speciellt svårt då näten är mobila och gränsen mellan näten ändras hela tiden. Det vi vill uppnå är s.k. *sömlöshet* d v s att användaren inte märker vilket fysiskt nät andra noder tillhör utan trafiken kan flyta sömlöst mellan näten.

5.4 Störtålighet i ad hoc-nät

Generellt kan man säga att ad hoc-nät är störtåliga eftersom trafik kan dirigeras om till andra vägar om någon av vägens noder är utsatta för störning. Det kan dock finnas smarta sätt att störa ett ad hoc-nät, t ex genom att störa viss kontrolltrafik. Hur ska vi designa protokollen så att de blir störtåliga även mot mer intelligenta störare? Man kan även tänka sig att störaren inte består av en enskild enhet utan bestå av ett nät av störare. Hur ska nätet ha ett störskydd mot ett nät av störare. Det traditionella sättet är att ansätta ett visst störskydd på varje länk men detta är ineffektivt då störskyddet stjäl möjlig nyttokapacitet i nätet.

5.5 Multicast

Mycket av trafiken som skickas i taktiska nät är av typen multicast (d v s en enhet sänder samma information till ett flertal enheter). För att detta ska kunna göras på ett bandbreddseffektivt sätt krävs bl a ett bra multicastroutingprotokoll.

Detta är komplicerat i ett mobilt ad hoc-nät. För att upprätthålla bra vägar till ett flertal enheter i nätet kan det behöva skickas mycket overhead-trafik vilket minskar kapaciteten för nyttotrafik. I vissa fall, beroende på t ex mobilitet, mängd av trafik och antal mottagare, kan det vara effektivare att använda ett enklare protokoll med mindre bra vägar men som inte skickar så mycket overhead-trafik. Hur ska denna avvägning göras och kan den göras adaptiv?

5.6 Skalbara ad hoc-nät

För att kunna hantera nätstyrningen i ad hoc-nät med många noder krävs ofta att man inför någon typ av hierarki för att begränsa overhead-trafiken. Exempelvis kan nätet delas in i *kluster/domäner* där man begränsar viss kontrollinformation inom klustret/domänen. Hur ska dessa kluster/domäner ska se ut och vilken information som ska skickas mellan dem. Ett annat alternativ att införa hierarkisker är att skapa ett virtuellt backbone-nät. Med detta menas att vissa noder utses ingå i ett backbone-nät. Alla noder kan ingå i backbone-nätet och de utses dynamiskt beroende på nätets utseende. Noderna i det dynamiskt tilldelade backbone-nätet hanterar större delen av nätstyrningen och därmed kan mängden overhead-trafik som skickas i nätet minskas.

5.7 Styrbara antenner i ad hoc-nät

Med hjälp av adaptiva antenner finns möjlighet att öka kapaciteten i ad hoc-nät avsevärt. Även störtålighet och smygegenskaper kan förbättras. Detta innebär t ex att accessprotokollet kan styra antennerna så att mycket energi strålar i riktningen mot mottagaren och därigenom t ex kunna sända med högre datatakt. Denna teknik kräver dock att man har flera antennelement på kommunikationsplattformarna vilket inte alltid är möjligt.

5.8 Säkerhet i ad hoc-nät

Säkerhet i ad hoc-nät är ett forskningsområde som kommer att växa i takt med att dessa nät används allt mera. Ännu finns inga färdiga lösningar eller produkter. Dagens förslag på säkerhetslösningar är framförallt baserade på olika skydd mot intrång såsom autenticering, accesskontroll och kryptering. Detta är inte

tillräckligt för att bemöta attacker från kompetenta motståndare mot militära system. En viktig framgångsfaktor är att kunna detektera intrångsförsök och agera mot dessa.

Litteraturförteckning

[1] J. Nilsson *et al.*, “Ad hoc networks - routing and mac design,” Swedish Defence Research Agency., Div. of Command and Control. Linköping, Sweden, Technical Report FOI-R--1801--SE, December 2005.

[2] K. Persson, U. Sterner, M. Sköld, and E. Johansson, “Distribution of situation awareness data in mobile tactical ad hoc networks using the fisheye routing algorithm,” in *Proc. of NATO-RTO-MP-IST-054*, Rome, Italy, April 2005.

[3] J. Grönkvist, “Interference-based scheduling in spatial reuse TDMA,” KTH, Stockholm, Sweden, Doctoral Thesis TRITA-S3-RST-0515, September 2005.

[4] E. Johansson, K. Persson, M. Sköld, and U. Sterner, “An analysis of the fisheye routing technique in highly mobile ad hoc networks,” in *IEEE VTC2004-Spring*, 2004, reg: FOI-S--1468--SE.

[5] K. Persson, E. Johansson, U. Sterner, and M. Sköld, “The fisheye routing technique in higly mobile ad hoc networks,” Swedish Defence Research Agency., Div. of Command and Control. Linköping, Sweden, Methodology Report FOI-R--1058--SE, December 2003.

[6] E. Johansson, K. Persson, M. Sköld, and U. Sterner, “AODV Routing in Ad Hoc Networks with Variable Data Rates,” Div. of Command and Control Systems, FOI, Swedish Defence Research Agency, Technical Report FOI-R--1430--SE, December 2004.

[7] L. Farman, U. Sterner, and O. Tronarp, “Analysis of Capacity in Ad Hoc Networks with Variable Data Rates,” Div. of Command and Control

Systems, FOI, Swedish Defence Research Agency, Technical Report FOI-R--0928--SE, June 2003.

[8] L. Farman, J. Nilsson, and O. Tronarp, “On QoS and Throughput Tradeoffs for Tactical Ad Hoc Networks,” Div. of Command and Control Systems, FOI, Swedish Defence Research Agency, Technical Report FOI-R--1425--SE, December 2004.

[9] O. Tronarp, “Quality of Service in Ad Hoc Networks by Priority Queuing,” Div. of Command and Control Systems, FOI, Swedish Defence Research Agency, Scientific Report FOI-R--1156--SE, January 2004.

[10] L. Farman, J. Nilsson, and O. Tronarp, “Using Variable Data Rate in Mobile Ad Hoc Networks Supporting Delay Sensitive Traffic,” Div. of Command and Control Systems, FOI, Swedish Defence Research Agency, Technical Report FOI-R--1725--SE, October 2005.