Tjänstekvalitet i ad hoc-nät

Slutrapport

ANDERS HANSSON, JAN NILSSON, JIMMI GRÖNKVIST, ULF STERNER, 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 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--2644--SE
ISSN 1650-1942

Användarrapport
December 2008

Informationssystem

Anders Hansson, Jan Nilsson, Jimmi Grönkvist,
Ulf Sterner, Mattias Sköld

Tjänstekvalitet i ad hoc-nät

Slutrapport

Titel	Tjänstekvalitet i ad hoc-nät Slutrapport
Title	Quality of Service in Ad Hoc Networks Final report
Rapportnr / Report No.	FOI-R--2644--SE
Rapporttyp	Användarrapport
Report Type	User Report
Månad / Month	December / December
Utgivningsår / Year	2008
Antal sidor / Pages	39
ISSN	1650-1942
Kund / Customer	Försvarsmakten
Forskningsområde	7. Ledning med MSI
Programme area	7. C^4I
Delområde	71. Ledning
Subcategory	71. Command, Control, Communications, Computers, Intelligence
Projektnr / Project No.	E7108
Godkänd av / Approved by	Martin Rantzer

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

FOI, Swedish Defence Research Agency
Information Systems
P.O. Box 1165
SE-581 11 LINKÖPING

Sammanfattning

Mobila ad hoc-nät ger en möjlighet att upprätthålla kommunikation under olika typer av taktiska förhållanden, med hög mobilitet, i olika typer av terräng och med varierande tillgång till fast infrastruktur. För att på ett effektivt sätt kunna hantera tjänstekvalitet i ad hoc-nät behövs designkriterier för protokollen och för hur kommunikationslagren ska interagera. I rapporten ges en sammanfattning av de problemområden som har studerats inom projektet ”Tjänstekvalitet i ad hoc-nät”: routing, konfliktfri access, tillträdeshantering, MIMO och säkerhet i ad hoc-nät.

Nyckelord: ad hoc-nät, tjänstekvalitet, tillträdeshantering, broadcast, accessprotokoll, MIMO, säkerhet

Abstract

Mobile ad hoc networks is a technique for maintaining communication in different types of tactical situations, with high mobility, in different types of terrain, and with sparse availability of communication infrastructure. In order to efficiently manage quality of service in ad hoc networks we need design criterias for the protocols and the interaction between communication layers. In the report we conclude the problem areas that have been covered within the project “Quality of Service in ad hoc networks”: routing, conflict free multiple access, admission control, MIMO and security in ad hoc networks.

Keywords: Ad hoc networks, QoS, admission control, broadcast, multiple access, MIMO, security

Innehållsförteckning

1 Inledning

Rapporten sammanfattar resultaten av de forskningsproblem som har undersökts inom FoT-projektet ”Tjänstekvalitet i ad hoc-nät” under åren 2006–2008. *Mobila ad hoc-nät* är trådlösa flerhoppsnät som fungerar oberoende av basstationer. Trafiken i kommunikationsnätet förmedlas istället av kommunikationsnoderna själva. På så vis kan noder som befinner sig utom räckhåll för varandra kommunicera genom att mellanliggande noder vidareförmedlar informationen (s.k. *flerhoppsteknik*). Genom att distribuera kommunikationsnätets funktioner och därmed undvika en central styrning blir nätet robust i den meningen att nätet klarar att godtyckliga kommunikationsnoder försvinner eller tillkommer. Uttrycket *ad hoc* är latin och betyder ”för detta ändamål”, vilket i det här sammanhanget betyder att nätet anpassar sig till nodernas aktuella geografiska placering och till de förhållanden som råder för tillfället. En mer utförlig översiktlig beskrivning av ad hoc-nät finns i [1]. Se även [2] för en sammanställning av tidigare ad hoc-nätsforskning inom FOI.

Med begreppet *tjänstekvalitet* avser vi i vilken utsträckning kommunikationsnätet kan tillgodose användarnas krav på de kommunikationstjänster som hanteras i nätet. Forskningen inom projektet fokuserar på scenarion där hela ad hoc-nätet är mobilt. Detta innebär att antennhöjderna är låga, vilket resulterar i en förhållandevis låg tillgänglig datatakt på kommunikationsnätets länkar. Detta innebär att alla protokoll som används måste fungera effektivt trots nodernas mobilitet och kommunikationsnätets begränsade resurser.

1.1 Ad hoc-nät: forskning och utveckling

Det finns idag protokoll framtagna som fungerar och möjliggör att mobila taktiska ad hoc-nät kan realiseras. Detta märks i och med att radiosystem med ad hoc-nätsfunktionalitet börjar komma ut på marknaden och användas i allt större utsträckning.

Även om det inte finns några militärspecificerade produkter som används operativt så finns det system för försök och demonstration, t ex fordonsmonterad GTRS-nod med vågformsapplikationen TDRS A som demonstrerades i oktober 2008 [3].

Forskningen inom ad hoc-nät har de senaste åren varit fokuserad på att göra algoritmer och protokoll smartare för att de ska kunna anpassa sig till rådande situation, till exempel anpassa sig till terräng, trafik och mobilitet. Detta är ett måste om många av de applikationer som man vill använda ska fungera i ad hoc-nät. Till exempel kräver tal korta fördröjningar medan andra applikationer kräver höga datatakter utan att vara så fördröjningskänsliga. Att uppnå smartare protokoll kan göras på flera sätt, exempelvis genom så kallad lageröverskridande design (*cross layer*-design) och kognitiv radio.

Lageröverskridande design går ut på att man samtidigt försöker optimera funktioner i flera lager i en kommunikationsstack med avseende på en dimensionerande resurs, till exempel nätkapacitet eller kort fördröjning. Rätt använt kan lageröverskridande design leda till stora prestandavinster. Nackdelen är en begränsning i modulariteten. I projektet Tjänstekvalitet i ad hoc-nät har vi använt oss av lageröverskridande design

vid interaktionen mellan protokoll som styr tillträdeshantering, routing, *medium access control* (MAC) och länkdatatakt.

Kognitiv radio har potential att förbättra prestanda i radionät. Med kognitiv radio menar man oftast det fysiska lagrets förmåga att utnyttja spektrum på ett effektivt sätt, men trenden är att kognitiv radio har fått en bredare betydelse än vad det haft tidigare och att även smarta algoritmer/protokoll på nätverkslagret läggs i begreppet kognitiv radio. Tanken är att nätverkslagren momentant ska kunna anpassa sig efter till exempel trafik och mobilitet.

Ett annat område inom ad hoc-nätsforskningen som vuxit de senaste åren är multicast-routing. Detta är en mycket viktig funktion i ett militärt radionät eftersom många av de tjänster som används är multicasttjänster, dvs. informationen ska från en nod till flera andra noder i nätet. Den mesta forskningen inom routing i ad hoc-nät har varit fokuserad på *unicast*-trafik (punkt till punkt) och det finns idag flera välspecificerade och fungerande protokoll för detta. Effektiva routingprotokoll för *multicast*-trafik (en till många) i nät med hög dynamik är komplexa och kräver ofta högre datatakt på länkarna.

Ad hoc-nätsforskningen inom detta FoT-projekt har behandlat tillträdeshantering, broadcast-routing, stabil routing, konfliktfri access, MIMO och säkerhet. Rapporten är tänkt att ge en översiktlig sammanställning av resultaten.

1.2 Rapportens disposition

I kapitel 2 beskriver vi vilka problem som behöver hanteras i samband med tillträdeshantering. Kapitel 3 behandlar två problem inom routing: broadcast-trafik och stabil routing. I kapitel 4 beskriver vi status för vår utveckling av konfliktfria accessprotokoll. Kapitel 5 sammanfattar vår forskning inom MIMO för ad hoc-nät. Kapitel 6 beskriver problemområdet säkerhet i ad hoc-nät. Slutligen ger vi i kapitel 7 några översiktliga slutsatser utgående från projektets forskningsresultat. Referenslistan är uppdelad i två delar: en del med de publikationer som finansierats av projektet och en del med övriga referenser. Projektets referenser ges med sammanfattningar.

2 Tillträdeshantering

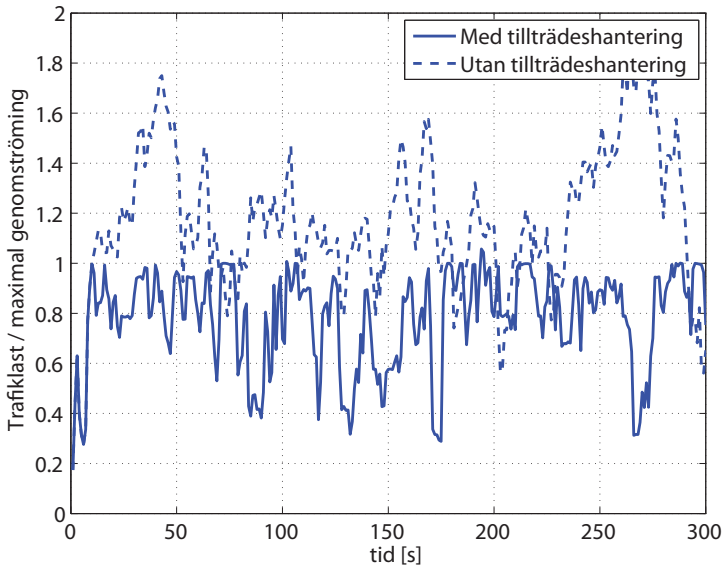
Metoder för att hantera trafik inkluderar policyhantering, tillträdeshantering (*admission control* på engelska) och trängselhantering (*congestion control*) samt de stödmekanismer som behövs för att tillträdeshantering och trängselhantering ska fungera tillfredställande. Policyhantering är appliceringen av regler för att bestämma huruvida tillträde till en specifik resurs ska tillåtas, i detta fall tillträde till nätverket. Detta är första steget för att bestämma om en användare överhuvudtaget ska få tillträde till nätverket, och om så är fallet med vilken trafik och under vilka förutsättningar. Tillträdeshantering bestämmer sedan om en godkänd trafiksession som söker tillträde till nätverket kan hanteras. För att bestämma det behöver de tillgängliga resurserna estimeras. Om resurserna är tillräckliga kan sessionen ges tillträde. Det finns således ett behov av att kunna estimera den nuvarande trafiken och kapaciteten i nätverket.

Förutsättningarna kan emellertid förändras sedan en session har getts tillträde. En session med högre prioritet kan söka tillträde till ett redan fullt lastat nätverk. Detta innebär att en session med lägre prioritet eventuellt måsta avslutas. Mobilitet kan också göra att kapaciteten i nätverket förändras. Att agera så att nätverket inte blir överbelastat, efter att sessioner har blivit insläppta i nätet, är uppgiften för trängselhanteringen.

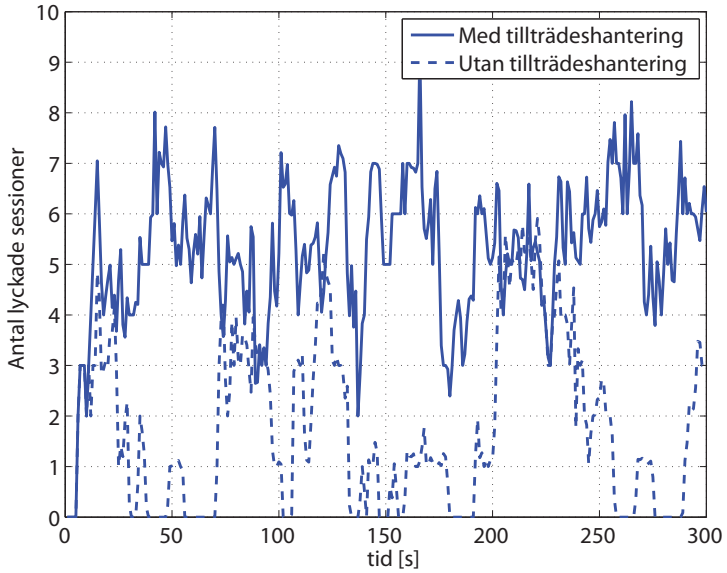
2.1 Tillträdeshantering i ad hoc-nät

För att undvika att nätet blir överbelastat vid dynamisk trafikhantering behövs först av allt någon form av tillträdeshantering (admission control). Notera att någon tillträdeshantering egentligen inte behövs om näten är överdimensionerade kapacitetsmässigt. De normala är dock att kapaciteten är en begränsad resurs och att nätet kan bli överbelastat utan tillträdeshantering. Om nätet blir överbelastat är det först den fördröjningskänsliga trafiken som får problem. Paket kommer att tvingas vänta i de olika noderna och hinner då inte levereras i tid till destinationsnoden. Det är avsevärt svårare att handskas med fördröjningskänslig trafik än med trafik med låga fördröjningskrav. I det senare fallet kan paketen lagras, antingen i sändarnoden eller i mellanliggande noder och sändas vid ett senare tillfälle då mer nätresurser är tillgängliga. I Figur 2.1 och Figur 2.2 ges ett exempel på vad som händer med fördröjningskänslig trafik då ett nät blir överbelastat. Exempelnätverket består av 32 noder och den trafik som söker tillträde till nätet består av förenklade talsessioner med fördröjningskravet 150 ms. Sändar- och destinationsnod väljs slumpmässigt för varje ny session och fler sessioner än vad som kan hanteras söker tillträde till nätet. I Figur 2.1 kan man se att trafikhanteringen reglerar trafiken så att nätet inte blir överbelastat, dvs. den normerade trafiklasten begränsas till ett. Detta medför att den trafik/session som släpps in också med betydligt högre sannolikhet lyckas då sessionens paket hinner levereras i tid till destinationen, se Figur 2.2.

Tillträdeshanteringen fattar beslut baserat på tillgängliga resurser. För att estimera dessa behöver dels kapaciteten i nätet, dels trafiken estimeras. Hur man estimerar kapaciteten hos ett ad hoc-nät är beroende på situation och hur nätet är designat, men det är mycket komplext i det generella fallet. Om nätet däremot är litet (få noder), relativt



Figur 2.1: Normaliserad trafiklast för exempelnätverket under 300 sekunder.



Figur 2.2: Antalet sessioner nätverket framgångsrikt kan hantera under 300 sekunder.

statiskt och länkarna har en fix datatakt blir det enklare. För att förenkla problemet kan man också dela in nätet i delar och bara lokalt estimera kapaciteten. Detta är något man framförallt behöver göra för stora ad hoc-nät. Det är egentligen först när nätet är specificerat, dvs. när man vet vilka protokoll som används, hur stort och dynamiskt nätet är, om länkkapaciteterna är fixa eller variabla etc. som det är meningsfullt att mera i detalj diskutera hur kapacitetsestimeringen ska göras.

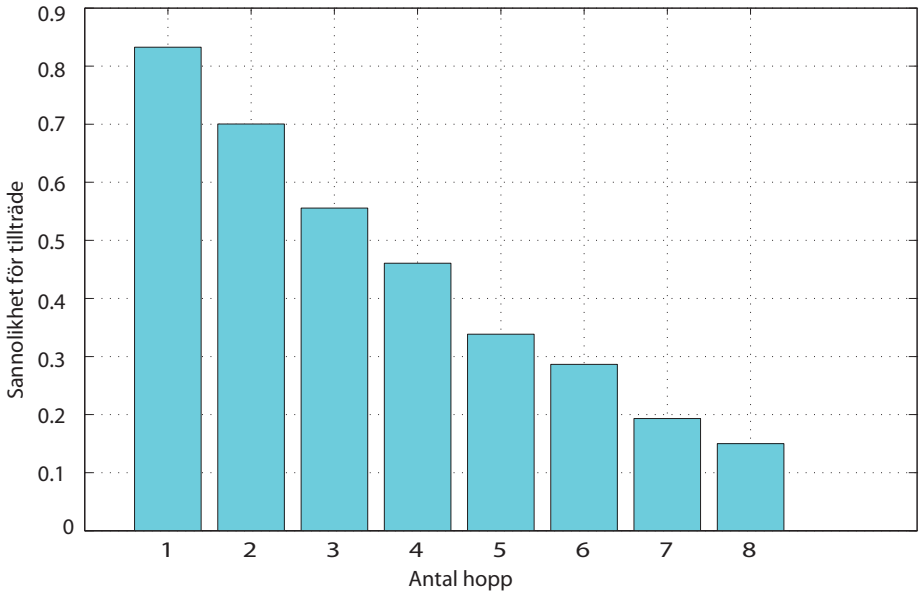
Trafikestimering kan göras på olika sätt beroende på hur mycket man vet om trafiken som ska estimeras. Det blir både lättare att utföra själva trafikestimeringen och bättre resultat om trafiktyperna är kända i förväg. Applikationer som man vet kommer att användas kan registreras i förväg i noderna. I bästa fall, då man har tillräckligt specificerad information om applikationerna, datatakt, QoS-krav etc., behöver man bara hålla reda på hur många sessioner/applikationer av en speciell typ som använder en länk för tillfället för att göra en trafikestimering. Alternativt kan man också packa upp pakethuvuden för att få mer information om applikationen, t.ex. vilken talkodare som används av en VoIP-applikation. Det finns således en mängd olika metoder som kan användas beroende på vad man vet i förväg och vad man eventuellt ytterligare kan få fram t.ex. via pakethuvuden. För icke känd trafik får dock en mer generell metod användas. Baserat på kölängder och pakets ankomstintensitet till noden kan dock trafiken estimeras med filterbaserade metoder, något som undersökts i [P8]. I det generella fallet då olika typer av trafik, inklusive i förväg icke känd trafik, ska kunna hanteras av nätverket, får en kombination av olika trafikestimeringsmetoder användas.

Tillträdeshantering fungerar normalt enligt följande princip: När en session söker tillträde till nätet beslutas om en rutt till destinationen. Sedan estimeras vilka resurser som krävs och vilka som finns tillgängliga för den valda rutten. Därefter används någon eller några beslutskriterier för att bestämma om resurserna är tillräckliga för att sessionen ska kunna tillåtas. För att kunna handskas med dynamiken i nätet kan det vara lämpligt att ha marginaler när man släpper in en session, dvs. lämna resurser så att inte all kapacitet används. I praktiken finns det alltid en fördröjning inblandad vid kapacitets- och trafikestimeringen vilket medför att estimaten speglar hur situationen såg ut i ett tidigare skede. T.ex. kan två olika noder på skilda ställen i nätet båda tillåta en session, baserat på samma estimerade tillgängliga resurser, vilket kan resultera i att nätet blir överbelastat.

I rapporten [P3] undersöks tillträdeshantering och dess robusthet, speciellt vilka marginaler som behövs vid tillträdeshanteringen för att åstadkomma robusthet mot trafikdynamiken i ett TDMA-baserat nätverk. En kombination av fördröjningskänslig och icke fördröjningskänslig trafik flyter i nätet. Vad som är tydligt är att hela nätkapaciteten *inte* bör nyttjas för fördröjningskänslig trafik. Hur stor marginal som behöver lämnas varierar men det viktiga är att resurserna som lämnas istället kan användas för icke fördröjningskänsliga trafik.

2.2 Rättvisa

I samband med tillträdeshantering och trafikhantering frågas ofta efter fairness", dvs. vad som är en rättvis resurstilldelning. De nätresurser som krävs för att leverera en



Figur 2.3: Sannolikheten att en session över olika antal hopp ges tillträde till exempelnätverket.

användares/nods trafik är beroende av var den är lokaliserad och hur bra förbindelser den har med övriga noder. En större andel av de tillgängliga nätresurserna krävs för att leverera trafik över dåliga än över bra förbindelser, och via flerhopp än via enkelhopp. Är det rimligt att en användare som råkar hamna i en ogynnsam position plötsligt inte längre ska få tillträde till nätet, eller bara mycket begränsat tillträde? Detta är en fråga som kan behöva vägas in i designen av olika trafikhanteringsmekanismer. Tillträdeshanteringen baserar normalt sitt beslut på behov i förhållande till tillgängliga resurser. En följd blir att en enkelhoppsession har större sannolikhet att tillåtas än en flerhoppssession. Ett exempel på detta illustreras i Figur 2.3, där det framgår att t.ex. en fyrahoppssession bara har hälften så stor sannolikhet att tillåtas som en enkelhoppsession. Vad som bedöms som rättvist varierar. Dock är det av intresse att ha metoder så att rättviseproblem kan hanteras på ett så enkelt sätt som möjligt när det behövs. I rapporten [P1] undersöks några metoder utifrån målet att sessioner ska hanteras rättvist oberoende av hopplängd.

3 Routing

Ad hoc-nätsrouting i allmänhet kan delas in i två typer, proaktiv routing och reaktiv routing. Proaktiv routing försöker hålla koll på nätet hela tiden, medan reaktiv routing bara letar reda på lämpliga vägar när de behövs. Proaktiv routing har fördelar när information om de flesta rutter behövs ofta (uppdateringar kan göras mer systematiskt), samt när uppkopplingstider måste hållas korta. OLSR (*Optimised Link State Routing Protocol*), baseras på proaktiv routing och beskrivs i internetstandarden [7]. Reaktiv routing är mer fördelaktig när bara ett fåtal flöden behöver upprätthållas samtidigt. AODV (*Ad hoc On-Demand Distance Vector Routing*) är ett populärt reaktivt protokoll, [6].

Eftersom behov av positionsinformation och allmän statusinformation normalt är viktigt gör detta ofta proaktiva metoder fördelaktiga i militära nät. Ett av de mest studerade (och närmast standardiserade) proaktiva routingprotokoll är OLSR som bygger upp en databas över länkarnas status och använder denna vid routing av paket i nätet. För att effektivisera processen något skickas inte information om alla länkar utan bara om en delmängd. Dessutom effektiviseras själva utsändingen av länkinformationen genom en effektiv algoritm för broadcast som kallas multipoint relay (MPR) flooding.

OLSR utnyttjar två typer av administrativa meddelanden för att skicka ut routinginformation: *hello-meddelanden* för sprida lokal information samt *topology control-meddelanden* (TC) för information om länkar längre bort. OLSR utnyttjar MPR-flooding för att minska antalet återsändningar av meddelanden som ska nå alla noder i nätet jämfört med flooding. Varje nod väljer ut en delmängd av sina grannoder. Dessa noder brukar kallas för MPR-noder och är de enda noder som återutsänder meddelanden. Varje nod väljer sina MPR-noder så att alla två-hopps grannar nås om MPR-noderna återsänder ett meddelande. För att reducera mängden genererad trafik i nätet distribueras enbart information om länkar till MPR-noder. Den informationen sprids med TC-meddelanden via MPR-flooding. I OLSR används MPR-flooding för att skicka ut administrativ trafik, men användas för att skicka vilken broadcasttrafik som helst.

3.1 Broadcasttekniker

Broadcasttrafik (en till alla) samt multicasttrafik (en-till många) är i allmänhet sett som mycket viktigt i militära scenarier. Detta till en mycket högre grad än i motsvarande civila tillämpningar. Ett problem är dock att design av ad hoc-nät för att hantera multicasttrafik är mycket svårare än motsvarande design för unicasttrafik (punkt-till-punkt)

Det mesta arbete som gjorts om ad hoc-nät har av denna anledning gjorts för unicasttrafik och lösningar för multicast och broadcast har huvudsakligen gjorts tillägg och/eller utökningar till dessa. I detta kapitel kommer vi studera broadcastproblemet och redovisa det som gjorts inom projektet.

Man kan dela in broadcastrouting i två typer av tekniker. Den första tekniktypen går ut på att utnyttja floodingäv meddelanden genom nätet, dvs. alla noder återsänder ett meddelande som de hör. Detta kan sedan effektiviseras genom att bara en del av noderna återsänder meddelandena, exempelvis genom MPR beskrivits ovan. Den andra

tekniktypen är att skapa en trädstruktur i nätet, dvs. ett antal sammanhängande noder som når alla noder i nätet.

Den första av dessa kräver lite eller ingen (ren flooding) information om nätet, medan den sistnämnda kräver mycket information. I praktiken flyter metoderna ihop, t.ex. kan man skapa gemensamma trädstrukturer utgående från MPR-noder.

Hur effektiva olika former av broadcasttekniker är kan bland annat mätas med hur många återsändningar av ett meddelande som behöver göras för att nå alla noder i nätet. I vanlig flooding kommer alla noder återsända meddelandet, medan i MPR-flooding kommer enbart MPR-noderna att återsända det. Med mer information kan antalet återsändande noder minskas ytterligare.

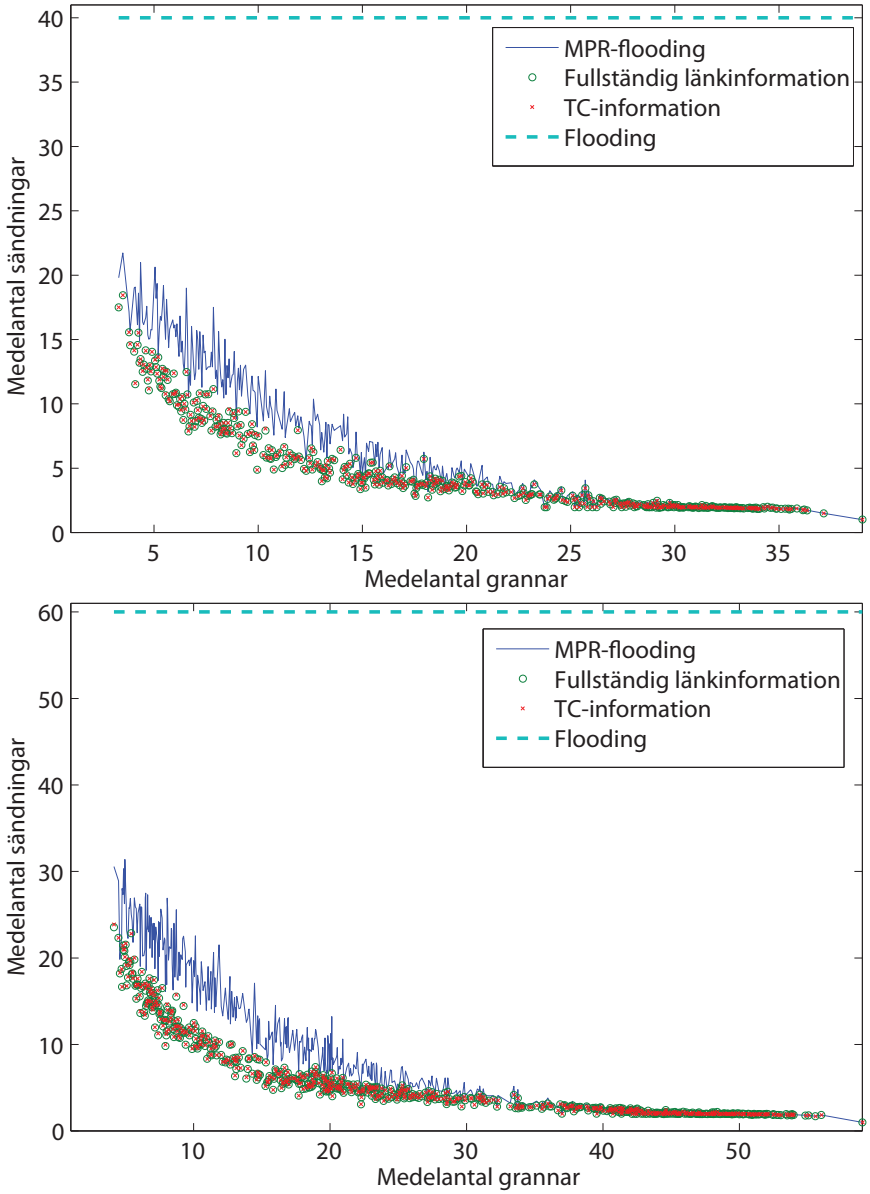
I [P5] har bland annat effektiviteten hos olika routingmetoder för broadcast studerats. Flooding och MPR-flooding har jämförts med trädbaserade metoder baserade på fullständig information om länkarna i nätet samt baserad på den begränsade information man får från TC-meddelanden. Detta visas i Figur 3.1, som visar hur många gånger ett meddelande måste återsändas som funktion av förbundenheten i nätet. Som synes kommer antalet återsändningar för flooding att vara oberoende av graden av förbundenhet. För de övriga metoderna minskar återsändningarna dock med graden av förbundenhet. För hög förbundenhet blir det inga eller mycket få omsändningar, både för MPR-flooding och trädbaerad broadcast baserad på fullständig information. Ett skäl till detta är att i sådana fall blir hela nätet lokalt. Det kommer att vara högst ett par hopp mellan noder i nätet. För lägre förbundenhet är resultaten intressantare. MPR-flooding ger vettiga resultat och är ganska okänsligt för mobilitet. Trädbaserade metoder ger bättre resultat men kräver mer information och att utnyttja TC-meddelanden ger i stort sett lika bra resultat som att ha all information. I praktiken är den reduktionen av nätinformation inte speciellt stor så det resultatet inte överaskande.

3.2 Variabel datatakt

Datatakten som används på de enskilda länkarna har stor påverkan på ett ad hoc-näts prestanda. Högre datatakter kan leda till mer kapacitet i nätet men räckvidden för enskilda länkar minskar. Valet av datatakter är en viktig designparameter vid specifikation av nät. I de flesta arbeten inom området har problemet ignorerats och en fast datatakt antagits given. Om datatakten kan anpassas på länkarna, speciellt om det kan ske lokalt, kan stora vinster potentiellt göras i kapacitet och/eller räckvidd.

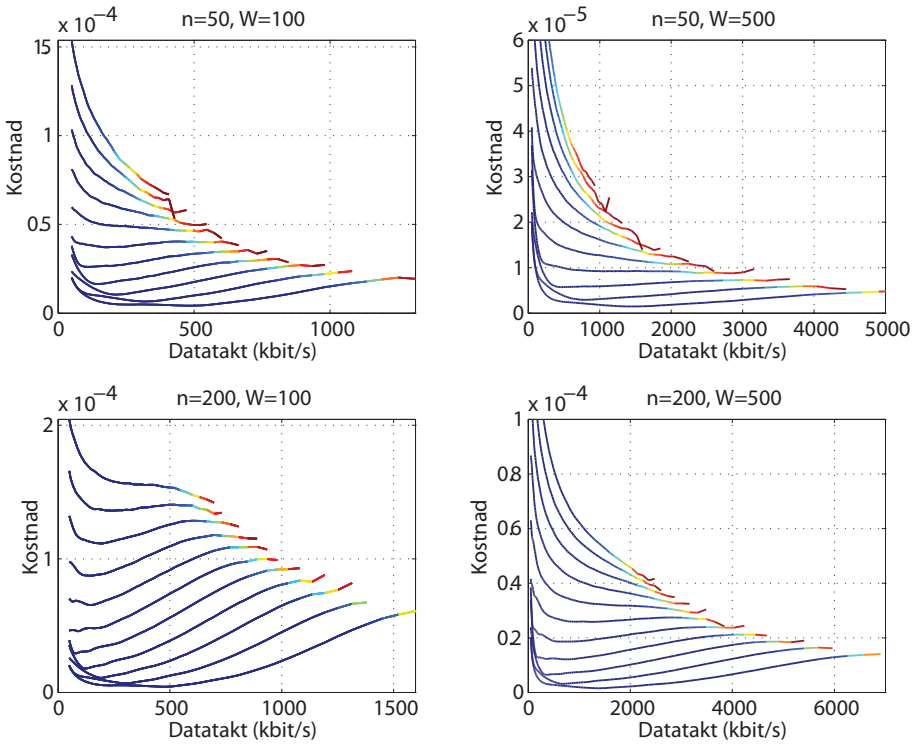
För unicasttrafik kan den variabla datatakten ganska enkelt hanteras genom att hantera viktfunktioner i den routingmetrik som används, men för broadcast- och multicasttrafik är problemet mycket besvärligare och inga enkla lösningar existerar.

I projektet har en första studie har gjorts, [P2], som studerat problemet givet att en *gemensam* datatakt har använts i nätet. Dock har denna tillåtits att vara dynamisk så den kunnat anpassas till topologi och trafikkrav. För unicasttrafik ökar nätverkskapaciteten med ökad datatakt så länge nätet är någorlunda förbundet. Vid tillräckligt hög datatakt blir inte nätet längre förbundet och nära denna gräns kan ibland trafik tvingas gå långa omvägar i nätet. Däremot varierar inte användarkapaciteten speciellt mycket beroende på datatakten om man inte väljer en alltför låg datatakt.



Figur 3.1: Jämförelse mellan olika broadcasttekniker för 40-nodsnät (ovan) och 60-nodsnät (nedan). Notera att resultaten för träd baserade på TC-information samt träd baserade på fullständig länkinformation nästan helt överensstämmer.

För broadcasttrafik är situationen något annorlunda. Beroende på en rad nätparametrar kan man få mycket olika resultat. I vissa fall kan man se ett kraftigt minimum för låga datatakter. Minimat ligger nära den datatakt där en central nod just kan nå alla andra noder i nätet. Trafiken liknar då trafiken i en mobiltelefonicell med en basstation i mitten. I andra fall minskar kostnaden med ökad datatakt.



Figur 3.2: Simuleringsresultat för $L = 5, 7, \ldots, 25$, där L är ytan som nätet är spritt över. Ökande L leder till ökande kostnadsnivåer. Där kurvorna är blå är alla nät förbundna, grön så är 50% förbundna och röd innebär att nästan inga nät är förbundna. Andelen förbundna nät är strikt avtagande.

I Figur 3.2 kan vi studera fyra olika fall där vi kan se dessa skillnader. Det som varierats här är bandbredd (W), nätstorlek (n) samt ytan som nätet täcker (L). Som kan ses har specifikt nät med låg bandbredd och hög noddensitet (litet område eller många noder) tydliga minimum vid en relativt låg datatakt. I övriga fall får vi oftast en minskning av av kostnaden för ökad datatakt.

3.3 Stabil routing

Ett problem som kan uppstå i samband med routing är att en vald rutt blir instabil, vilket innebär att rutten mellan sändande och mottagande nod växlar mellan likvärdiga vägar. Detta kan förekomma i många typer av nät, men blir extra besvärande i mobila ad hoc-nät med hög rörlighet. Routingstrategier som enbart försöker hitta den kortaste vägen mellan noderna tenderar dessutom att föredra länkar mellan noder på långt geografiskt avstånd från varandra. Risken att sådana länkar bryts är stor jämfört med länkar mellan näraliggande noder.

Det finns en stor potentiell vinst i att välja stabila rutter och länkar i nätet. Paket som skickas genom nätet utan att nå fram orsakar en onödig belastning och ruttbyten kan i sig orsaka extra administrativ trafik, både från routing och access. Speciellt måste trafikadaptiva accessprotokoll anpassa kanalresurserna dynamiskt efter hur trafiken i nätet omfördelas. I kommunikationsnät med begränsade resurser och varierande trafik är trafikadaptivitet önskvärt för att undvika överbelastning i flaskhalsar i nätet.

Ett sätt att förbättra ruttstabiliteten i en routingstrategi är att införa *hysteresmarginaler* för routingbesluten. Detta innebär att en ny rutt väljs först när minskningen i ruttkostnad, jämfört med den gamla rutten, är större än en given tröskelnivå. I [P10] har vi undersökt om hysteres vid ruttbyten kan reducera administrativ trafik i trafikadaptiva accessprotokoll baserade på tidsdelning (TDMA) eller sådana baserade på frekvensdelning (FDMA). De routingstrategier vi har analyserat är *kortaste väg* (ruttkostnad: antal hopp) och för variabel datatakt *lägst total transmissionstid* (ruttkostnad: $\sum_i 1/R_i$, där R_i är datatakten på länk i i rutten). Vi visar att små hysteresmarginaler för routingbesluten minskar overheadtrafiken för accessalgoritmen mer än ruttkostnaden ökar. För stora hysteresmarginaler överväger dock nackdelarna med att de rutter som används i nätet blir långa.

4 Konfliktfria accessprotokoll

Inom projektet har arbetet med att utveckla accessprotokoll tagit vid efter det arbete som utfördes i [2]. Fokus för arbetet har fortsatt varit på att utveckla ett distribuerat STDMA protokoll. STDMA är ett konfliktfritt accessprotokoll utvecklat för ad hoc-nät. STDMA står för *spatial reuse* TDMA och innebär, liksom TDMA, att kanalresursen delas upp i tidluckor som fördelas mellan noderna. För att öka kapaciteten försöker dock protokollet att återutnyttja tidluckor genom att låta flera noder simultant utnyttja samma tidluckor, vilket är möjligt om noderna befinner sig tillräckligt långt från varandra.

En tidluckebaserad accessmetod har flera fördelar framför andra accessmetoder såsom CSMA som är vanligt förekommande i ad hoc-näts-sammanhang. För QoS-trafik kan resurser reserveras och därmed möjliggöra fördröjningsgarantier (i den mån sådana är möjliga i ad hoc-nät), vilket är viktigt för många militära applikationer.

4.1 Utmaningar och möjligheter

Utmaningen med STDMA är att ta fram sändningsscheman som säger när en viss nod får sända. Förutom att schemat ska vara konfliktfritt vill vi ofta att de ska ha andra egenskaper, som att noder med mycket trafik ska få fler tidluckor än andra noder.

För att kunna avgöra hur sändningsschemat ska se ut behövs information om hur trafiken i nätet ser ut samt hur noderna påverkar varandra då de sänder. Givet denna information kan vi avgöra vilka noder som kan använda samma tidluckor och utifrå detta generera hela sändningsschemat. Rör noderna sig finns dock en risk att noder som tidigare kunnat sända samtidigt utan att störa varandra inte längre kan det, vilket leder till att schemat måste ändras, se [4].

Skapandet och förändrandet av schemat kan antingen ske centralt eller distribuerat. En fördel med att skapa schemat centralt är att schemat kan optimeras bättre. Risken är dock stor att schemat redan är inaktuellt när det når ut till noderna. Vidare är det inte en särskilt robust lösning eftersom en utslagning av den centrala noden får stora konsekvenser. För att öka robustheten har vi därför valt att generera våra scheman distribuerat i nätet. Vid genereringen tar vi dessutom bara hänsyn den lokala omgivningen, vilket minskar kostnaden att aggregera den information som behövs för att skapa schemat. En nackdel med denna metod är att algoritmen blir mer komplex.

Förutom bättre förmåga att hantera QoS-trafik erbjuder ett STDMA-protokoll en bra grund för att introducera mer komplexa nätfunktioner såsom tillträdeshantering, se Kapitel 2, och routing med hänsyn till datatakten, se Kapitel 3. I allmänhet kan tekniker på andra lager i kommunikationsstacken enkelt fås att fungera väl ihop med STDMA-protokollet, något som ofta är nödvändigt för att nya tekniker på dessa lager ska kunna öka effektiviteten hos nätet. Att exempelvis addera variabel datatakt på länkarna om inte högre lager såsom routing väljer att utnyttja detta är normalt meningslöst.

Med hjälp av en generell distribuerad STDMA-algoritm kan avancerade funktioner stegvis introduceras så att ett mycket anpassningsbart och modulärt ramverk för ad hoc-nät skapas, där extra funktionalitet enkelt adderas på ett evolutionärt sätt. Problemet är

dock att en sådan generell distribuerad STDMA-algoritm saknas. Inom tidigare projekt [2] har ett första arbete utförts i syfte att skapa en sådan algoritm. Det är dock ett komplext problem och flera förenklingar gjordes.

4.2 Ny version av algoritmen

Vid designen av den STDMA-algoritm som tagits fram i detta projekt har huvudmålsättningen varit att skapa en mindre idealiserad algoritm än den som togs fram inom projektet Heterogena Ad Hoc-nät [2]. Förutom huvudmålet har även delmålet att skapa en algoritm som kan användas och byggas vidare på i framtida projekt varit styrande. Fokus för designen har därigenom främst varit att skapa en fungerade felhantering som kan hantera förlorade meddelanden och inkonsistenser i nodernas uppfattning om nätet och det aktuella sändningsschemat. Vidare har algoritmens förmåga att hantera både allokering av länkar och noder i samma sändningsschema samt mängden trafik algoritmen genererar varit viktiga designparametrar.

Felhantering

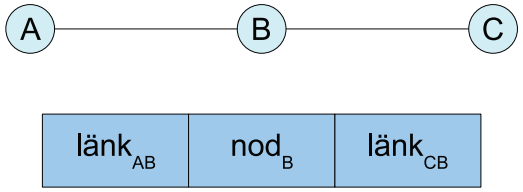
En distribuerad-STDMA algoritm behöver information om både nätstruktur och det aktuella sändningsschemat för att kunna fungera väl. För kunna hålla nere kostnaden för att överföra denna information måste dock algoritmen kunna hantera att den inte har aktuell information om allt i nätet. Då risken för paketförluster inte kan ignoreras i ett radionät måste algoritmen även kunna hantera att meddelanden inte kommer fram.

Den tidigare algoritmen kunde hantera att informationen om länkarna inte var helt korrekt men kunde få problem om informationen om trafikbelastningarna och sändningsschemat inte var korrekt [2]. Överföringsproblem för den förhandlingstrafik som hanterar allokering och avallokering av tidluckor riskerade också att leda till problem som algoritmen inte kunde lösa.

Den nya algoritmen kan i princip hantera alla dessa typer av problem. Inkorrekt länkinformation hanteras som i den tidigare algoritmen genom att marginaler skjuts in in länkberäkningarna. Problem med trafikbelastningsestimaten samt felaktigheter hos nodernas uppfattning av sändningsschemat hanteras genom att de inblandade noderna synkroniserar sina databaser. Tappade paket vid allokering hanteras genom att algoritmen efter en stunds väntan ignorerar den icke svarande noden under en tid och istället går vidare med andra allokeringar. Får en nod inte svar då den begär att en annan nod ska släppa en tidlucka på grund av in interferens- eller trafiksituationen går noden efter en stunds väntan själv vidare med avallokeringen.

Nod- och länkallokering

Beroende på vilken trafik som ska sändas är olika typer av tidluckor mer eller mindre lämpliga att använda. Vill vi kunna sända trafik från en nod till godtycklig granne,



Figur 4.1: Exempel på ett schema med både länkar och noder. I tidlucka 1 kan nod A sända till nod B. I tidlucka 2 kan nod B sända till både nod A och B medan i tidlucka 3 kan nod C sända till nod B.

eller kanske till alla grannar, är en så kallad nodtidlucka lämpligast. I en nodtidlucka garanterar vi att alla grannar kan ta emot ett paket. Vill vi däremot bara sända trafik till exakt en granne är det ofta bättre att allokera en så kallad länktidlucka. I en länktidlucka garanterar vi bara att den aktuelle grannen kan ta emot ett paket. Fördelen med en länktidlucka är vi att kan få en högre grad av spatiell återanvändning då antalet noder som ska kunna ta emot ett paket är färre.

Är trafiken i nätet unicastrafik är således länktidluckor oftast att föredra medan om det är multicasttrafik är nodtidluckor lämpligast. I många fall består dock trafiken av en mix av unicast- och multicasttrafik. Det är därför fördelaktigt att en algoritmen kan allokera både länktidluckor och nodtidluckor så att radiokanalen kan användas så effektivt som möjligt [2]. Den nya algoritmen kan hantera båda dessa typer av tidluckor så att ett sändningsschema kan bestå av en lämplig mix av nod- och länktidluckor, se Figur 4.1.

En möjlig vidareutveckling av algoritmen är att låta en nod med flera länktidluckor med lågt trafikflöde slås samman dessa till en eller flera nodtidluckor så att utnyttjande graden av tidluckorna maximeras. Hur en sådan sådan omfördelning av trafiken ska ske är dock i sig en forskningsfråga som behöver studeras vidare.

Trafikbelastning

En av de stora designmässiga utmaningarna med en distribuerad STDMA-algoritm är att minimera den trafik som algoritmen genererar då det aktuella sändningsschemat genereras. Denna trafik består dels av information om nätet, dels av information rörande det aktuella sändningsschemat. Då det underliggande STDMA-sändningsschemat är deterministiskt till sin natur är det ur effektivitetssynpunkt fördelaktigt om den trafik som ska sändas är så deterministisk som möjlig. Den nätdata som ska överföras tenderar dock att genereras mycket slumpmässigt i tiden. För att sänka kostnaden för att överföra den i grunden stokastiska informationen om nätet aggregerar därför algoritmen information och sänder ut den vid i förväg bestämda tidpunkter. För att ytterligare sänka kostnaden för informationsöverföringen sänds informationen bara ut till närliggande noder. Vilka noder som anses vara närliggande beror på vilken typ av information som sänds ut. Att aggregera informationen och bara sända ut den till en mindre del av nätet innebär dock samtidigt att antalet felsituationer för algoritnmen riskerar

att öka. Då lösande av fel också innebär en kostnad i form av extratrafik och sämre sändningsschema så är det en avvägning hur mycket informationsmängden som distribueras kan minskas. Exakt vad som är lämpligt här är därför en framtida forskingsfråga då algoritmen helst själv borde anpassa sig till den rådande situationen.

Vidare kan den rena förhandlingstrafiken minimeras ytterligare. Ett första steg är att låta noder allokera mer än en tidlucka åt gången. Ett sådan förfarande riskerar visserligen att försämra algoritmen ur rättvisesynpunkt, men då många av de tänkta applikationerna inte kommer kunna fungera utan att de får en viss begärd resursmängd så är detta allokeringssätt troligen mer lämpligt.

En annan utvecklingsmöjlighet för att minska förhandlingstrafiken är att försöka utnyttja den interna informationen om övriga noders resursbehov bättre. Speciellt fallet då en nod släpper tidluckor samtidigt som resursbrist råder resulterar idag i att flera noder initialt försöker allokera den fria resursen. I slutändan kommer den nod som har störst behov att få tidluckan, men dagens algoritm tenderar att generera mer trafik än vad som antagligen skulle behövas om den interna informationen utnyttjades bättre.

5 MIMO

Kommunikationssystem där både sändare och mottagare är utrustade med flera antenner kallas normalt (Multiple-Input-Multiple-Output) MIMO-system. Sådana flerantennsystem är en lovande teknik när det gäller möjligheten att kunna öka datatakten och robustheten i trådlösa taktiska kommunikationssystem. MIMO system har studerats flitigt under senaste åren och det existerar ett stort antal olika MIMO-algoritmer med varierade prestanda och komplexitet. MIMO-tekniker brukar grupperas i tre klasser/moder utifrån vilka principiella vinster de tillför systemet. Vid lobformning är målet att öka signalstyrkan och/eller undertrycka interferenser. Rumsdiversitet gör att fädning kan motverkas. Spatiell multiplexing gör det möjligt att öka datatakten. Användande av MIMO-system ger alltså många möjligheter att förbättra prestanda. Vilken mod av dessa som ska användas beror på situation och man kan tänka sig ett avancerat MIMO-system som kan byta mod mellan spatiell multiplexing, diversitet och lobformning.

5.1 MIMO i ad hoc-nät

Införande av MIMO i ad hoc-nät kräver en översyn av nätprotokollen som ska användas då de flesta nätprotokoll är konstruerade under antagandet att antennerna är rundstrålande. Speciellt viktigt blir detta vid lobformning och utnyttjande av den spatiella domänen. Protokollen för schemaläggning, detektering av grannar, nätinitialisering och konfigurering behöver inkludera mekanismer för att handskas med den spatiella domänen. Vägval (routing), flödeskontroll, och andra högre lagers protokoll kan möjligen också tjäna på att utnyttja den spatiella domänen. Om däremot endast spatiell multiplexing och diversitet används behöver inte så omfattande protokollmodifieringar göras. De viktigaste är då att protokollen kan hantera variabel datatakt på de olika länkarna. Detta kan dock kräva modifieringar i MAC- och routingprotokoll.

Ett avanserat adaptivt MIMO-systems prestanda beror på hur väl kanalen är känd inte bara hos mottagaren utan också hos sändaren. En viktig frågeställning blir därför hur sändaren ska kunna skapa sig bra kanalestimat. Bra kanalestimat hos sändaren kräver återkoppling från mottagaren. Detta kan behöva vägas in i protokolldesignen, speciellt i MAC-protokollet. T.ex. kan man i ett TDMA-schema allokera början av en tidslucka till återkopplingen, dvs. den avsedda mottagaren skickar först en pilotsignal för att den avsedda sändaren ska kunna estimera kanalen.

5.2 Möjliga kapacitetsvinster i ad hoc-nät med MIMO-system

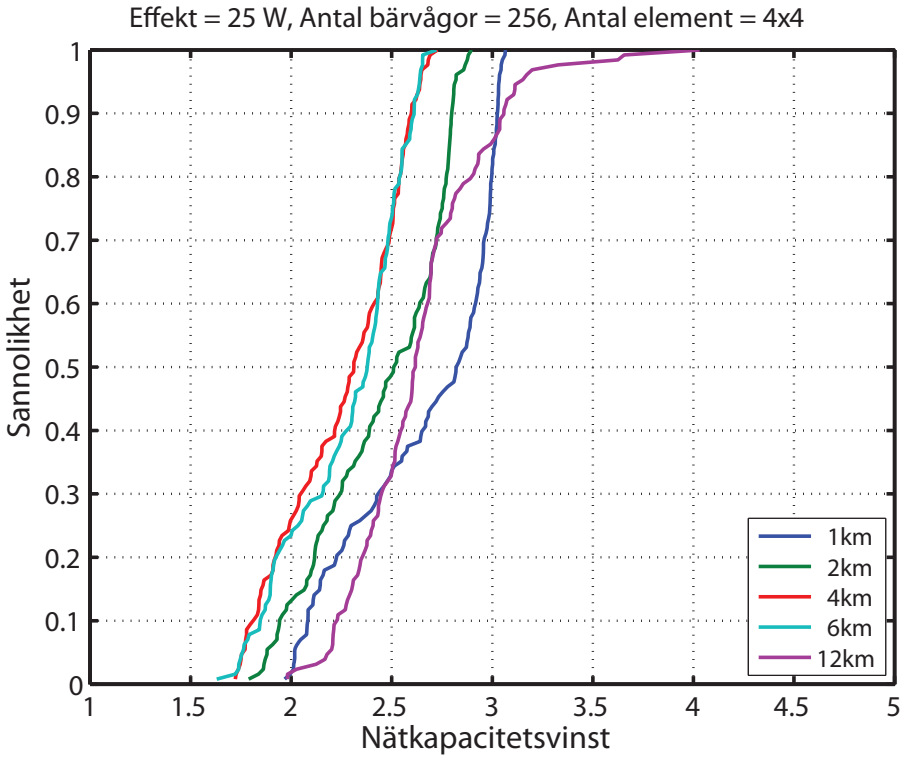
Spatiell multiplexing är som tidigare nämnts ett sätt att öka datatakten. Hur mycket datatakten kan ökas beror på egenskaperna hos flervägsutbredningen. Teoretiskt, om vi antar ett högt SNR och oberoende rayleighfädning så blir den maximala medel vinsten

med MIMO och spatiell multiplexing jämfört med SISO (Single Input Single Output) $min(n_{Tx}, n_{R_x})$. Beteckningarna n_{Tx} och n_{R_x} står för antal sändar- respektive mottagarantenner. Ett 4x4 MIMO-system skulle alltså ge en datataktsvinst på 4 gånger jämfört med SISO. Försök och experiment visar dock att den vinsten inte uppnås i medel för kanaler i verklig miljö och att den dessutom varierar kraftigt mellan olika kanaler.

I [P4] har vi undersökt möjliga länk- och nätkapacitetsvinster med MIMO vid 300 MHz i stadsmiljö. Två olika kanalmodeller för stadsmiljö har använts, en strålbaserad kallad RPS och en geometribaserad stokastisk kanalmodel. Med dessa modeller, speciellt med RPS som använder en digital karta över stadsbebyggelsen, fås representativa kanalöverföringsfunktioner som kan användas för att beräkna länkdatatakter både med MIMO och med SISO. Med hjälp av RPS undersöks ett stadsscenario bestående av 23 noder. Med ett 4x4 MIMO-system fick vi en median MIMO vinst jämfört med SISO på ungefär 2,2 för de cirka 100 länkarna som undersöktes medan vinsten för en enskild länk varierade mellan 1,3 och upp till nästan 4. Med fler antennelement på sändare och mottagare sidan kan vinsterna ökas men systemkomplexiteten och kostnaden ökar också. Kostnaden för sändare och mottagare ökar ungefär linjärt med antal antennelement. Vinsterna som går att uppnå praktiskt ökar dock inte riktigt lika mycket. Att använda ett 4x4-MIMO-system kan därför vara en bra kompromiss mellan prestanda och kostnad.

För att kunna skapa sig en bild av vinsterna på nätnivå krävs det att många nät genereras och undersöks. På grund av den höga beräkningskomplexiteten med RPS användes i stället den stokastiska kanalmodellen. I Figur 5.1 ges ett exempel på vilka nätkapacitetsvinster som kan fås. Vad som visas är fördelningsfunktionen för nätkapacitetsvinsterna som fås då ett 4x4-MIMO-system kombineras med ett OFDM system bestående av 256 underbärvåger. Att kombinera MIMO med OFDM ger att antal fördelar som underlättar vid en praktisk realisering av systemet. Vi kan se att vi får nätkapacitetsvinster med MIMO jämfört med SISO mellan ungefär 1,7 och 3. Storleken på näten påverkar också resultaten. De olika nät som undersökts har bestått av 32 slumpmässigt utspridda noder på en kvadratisk yta med sidlängd mellan 1 km och 12 km. För varje storlek har 128 olika 32 noders nät genererats. Resultaten för det största nätet (12 km) ska tolkas med försiktighet då SISO näten som jämförelsen görs mot får lite för dåliga länkar. Om vi bortser från det största nätet ser vi att kapacitetsvinsterna med MIMO är störst för små nät för att sedan minska något när näten blir större. Ett litet nät medför korta länkar och ett högt SNR i medel vilket ger stora MIMO kapacitetsvinster från spatiell multiplexing. Det kan påpekas att också nättopologin påverkas av MIMO. En närmare underökning som gjordes i [P4] visade att för små nät minskades antalet använda länkar i näten med MIMO. Detta medför att medelhopplängderna ökade. För stora nät var situationen den omvända.

Sammanfattningsvis kan konstateras att det finns betydande vinster att göra med ett införande av MIMO i ad hoc nät. Teoretiskt finns möjligheten att mångfaldiga kapaciteten men det återstår att noggrannare undersöka vilka prestandavinster som går att praktiskt åstadkomma i ett verkligt system.



Figur 5.1: Nätkapacitetsvinst med ett 4x4 MIMO system.

6 Säkerhet i ad hoc-nät

Trådlös kommunikation är relativt lätt att störa och avlyssna om den inte skyddas. Jämfört med fasta nät kan man säga att förutom att de flesta säkerhetsrisker i fasta nät även är relevanta i mobila ad hoc-nät så tillkommer ytterligare specifika säkerhetsrisker för mobila ad hoc-nät som specifikt behöver hanteras.

6.1 Hotbild

I ett fast nät är viktiga noder (t.ex. brandväggar, servrar och routrar) ofta inlåsta. Till övriga noder finns vanligen någon typ av behörighetskontroll (t.ex. tjänstekort för åtkomst till lokalen). Mobila noder har sämre fysisk säkerhet än fasta, konventionella noder. En radio kan tas över genom stöld, att användare av radion kidnappas eller att fordon slås ut men radioutrustningen klarar sig.

Möjligheter till passiva och aktiva attacker är störrre i trådlösa nät än i fasta nät. En passiv attack innebär att avlyssna nätverket för att få kännedom om dess innehåll. En aktiv attack innebär att aktivt modifiera något. Exempel på aktiva attacker är att modifiera meddelanden, kasta meddelanden, sprida falska meddelanden, skicka mycket meddelanden för att åstadkomma kollisioner samt att en nod utger sig för att vara en annan nod.

En fungerande och autenticerad radio kan användas till att avlyssna eller till att sända vilseledande eller störande legal trafik (DoS attack). Till exempel finns det ett taktiskt värde i att avlyssna eller störa positions- och statusinformation. Ett annat motiv är att försöka plocka ut kryptonycklar ur radion för att ta sig vidare in i radionätet.

En mer avancerad säkerhetsattack är att installera skadlig mjukvara i radion. Detta kan göras i en övertagen radio eller en egentillverkad kompatibel radio. I ett radiosystem med svagt skydd kan en virusattack via radiogränssnittet ge samma resultat.

Några specifika egenskaper som ökar hotet mot ad hoc-nät är följande:

- Distribuerad funktionalitet, vilket innebär att noder antas samarbeta. Ad hoc-nätsalgoritmer är baserade på ett distribuerat samarbete. Elaka noder kan enkelt ställa till stora problem genom att inte följa protokollen.

- Initiering och konfigurering ska vara automatisk, med så lite förplanering som möjligt. Detta innebär att nya noder kan tillkomma utan att nätet har tillgång till en central server.

- Mobila noder har ofta en begränsad beräkningskapacitet. Dessutom, med den begränsade kapacitet som finns i ad hoc-nät behöver trafiken från alla förhandlingar och utbyten mellan noder hållas till ett minimum.

6.2 Skydd

Säkerhetsmekanismer i fasta nät omfattar bl.a. autenticering, integritet och sekretess. De bygger ofta på centraliserad funktionalitet. Exempelvis innehåller de flesta nyckelhanteringssystem centraliserad funktionalitet. Andra exempel är centraliserade intrångsdetekteringssystem och databaser med loggar. Denna typ av centraliserade säkerhetslösningar kan vara svåra att anpassa till ad hoc-nät.

Nätverkstopologin ändras kontinuerligt eftersom noderna är rörliga. Det kan därmed vara svårt att övervaka nätet och avgöra om noder inte uppträder på korrekt sätt.

Medlemmarna i nätet ändras också då noder ansluter eller lämnar nätet. Vissa noder, som identifieras som elaka, kan också tvingas att lämna nätet. Nätet kan även förändras då noder tappar eller återfår kontakten med varandra. Ett dynamiskt nät ställer speciella krav på säkerhetsmekanismerna. En statisk säkerhetslösning, vilket ofta används i fasta nät, kan aldrig uppfylla säkerhetskraven. Det är också viktigt att en nod autenticeras då den ansluter till nätet.

Ytterligare en metod kan vara att regelbundet autenticera användare. Detta är dock opraktiskt att göra mot en central punkt i nätet på grund av den extra trafik det medför och nätets topologiförändringar.

Ett sätt att skydda kommunikationen är att dela in nätet i säkra och icke säkra domäner. I fasta nät kan det ofta göras på ett naturligt sätt. Exempelvis kan det interna nätet utgöra den säkra domänen, medan Internet utgör den icke säkra domänen. Mellan den säkra och icke säkra domänen placeras diverse säkerhetsmekanismer t.ex. brandvägg och intrångsdetekteringssystem. I ett mobilt ad hoc-nät finns inte någon naturlig indelning av säker och icke säker domän. Det finns ingen plats i nätet där all trafik passerar.

Nyckelhantering är ytterligare ett problem som måste ha speciella lösningar. Om en viss förplanering är möjlig, kan nycklar förinställeras i enheterna, eller laddas ner vid kontakt med en fast server. Ett ad hoc-nät behöver emellertid också kunna fungera utan koppling till ett fast nät och hur initiering och uppdatering av nycklar ska kunna ske i sådana fall är oklart. Ett ytterligare problem är revokering av nycklar.

6.3 Skydd mot interna attacker

En intern attack innebär att kommunikationen störs av en obehörig användare som är autenticerad i nätet. Det finns många exempel på enkla interna attacker som är baserade på att missbruka de protokoll som används i nätet. Det förutsätter dock att man har tillgång till en radio där legal programkod har ersätts med modifierad mjukvara. Till exempel kan en stulen och manipulerad radio användas för detta. För att mobila ad hoc-nät ska kunna fungera utan central funktionalitet används distribuerade protokoll. Protokollen bygger på principen att noderna samarbetar. Med små modifieringar i protokollen kan samarbetet utnyttjas för att störa kommunikationen i nätet. Om en intern attack lyckas så blir funktionsstörningarna ofta stora. Därför är det viktigt att kunna detektera interna säkerhetsattacker och om möjligt mildra deras skadeverkningar.

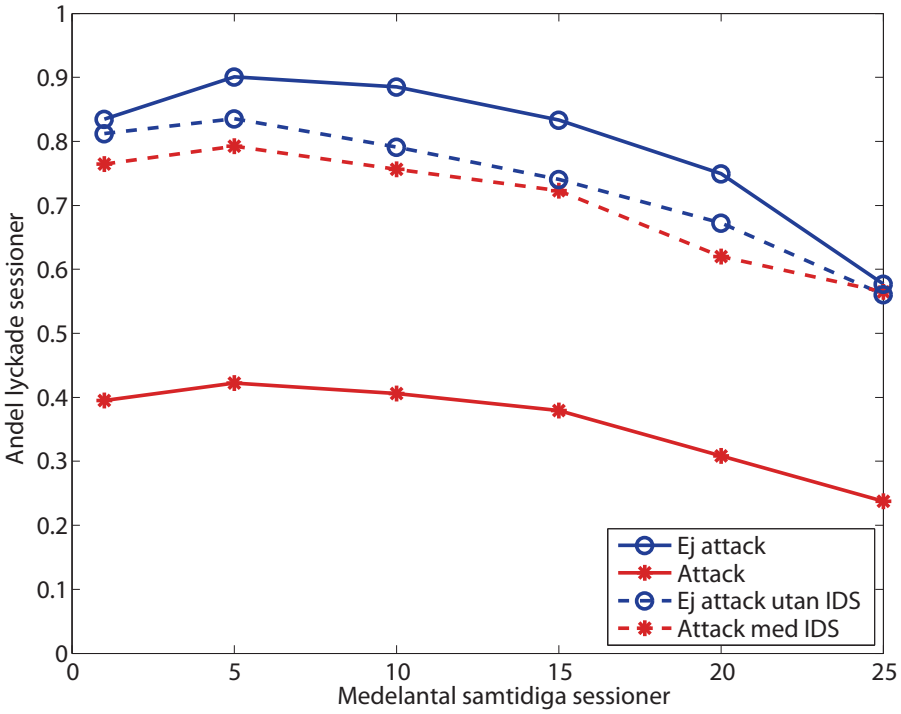
När det gäller interna attacker har vi valt att studera två routingprotokoll, AODV

(*on demand distance vector routing*) och OLSR (*optimised link state routing protocol*). Båda dessa protokoll har funnits som standarder under lång tid och representerar två grundtyper av routingprotokoll: reaktiva (AODV) och proaktiva (OLSR).

I [P7] utvärderar vi effekten av interna attacker mot routingprotokollet AODV. Arbetet finansierades även av projektet Säkerhet i ad hoc-nät. Utvärderingen visar att interna attacker kan slå ut kommunikationen i en stor del av nätet. För att erhålla en acceptabel nivå på säkerheten behövs avancerade säkerhetslösningar. En effektiv variant är att använda policybaserad intrångsdetektering, speciellt när den kombineras med traditionella kryptolösningar. Genom att ignorera felaktiga paket kan vår policy-baserade intrångsdetekteringsmetod ta bort i stort sett all effekt av dessa attacker, till priset av en liten kostnad i form av minskad tillgänglig kapacitet vid normal drift.

I Figur 6.1 ser vi hur en intern attack påverkar antalet lyckade sessioner i ett ad hoc-nät, med och utan intrångsdetektering. Attacken som vi har simulerat är en *rush attack*, vilket innebär att den elaka noden modifierar tidsstämplingen i de routingpaket som den vidarebefordrar. Mottagande noder kommer då att föredra routinginformationen i dessa paket, eftersom de paketen verkar vara nyare än de legala routingpaket som kommer från andra noder. Den intrångsdetektering vi har implementerat detekterar attacken och noderna ignorerar då felaktiga routingpaket. Som vi kan se i figuren, så kan attackens verkan reduceras kraftigt med hjälp av intrångsdetektering. Dessutom påverkas nätets prestanda ganska lite av intrångsdetekteringen.

Effektiv routing för multicasttrafik och broadcasttrafik är svårare att realisera än routing för unicasttrafik. Detta gäller även när routingen ska skyddas mot interna attacker. I [P5] har vi undersökt om det är praktiskt genomförbart att skydda routingmeddelandena i OLSR med hjälp av autenticering. Den metod vi har valt att analysera kallas *advanced signatures* och beskrivs i [5]. Den visar sig orsaka en mycket hög andel administrativ trafik och det krävs mer utvecklingsarbete för att metoden ska vara praktiskt användbar. En möjlig förbättring är att endast skydda en delmängd av de routingmeddelanden som skickas i OLSR. Lokalt informationsutbyte är enklare att säkra med signaturer, vilket kan utnyttjas för MPR-flooding. Resultaten visar att MPR-flooding kan ge en god balans mellan kapacitet, säkerhet och robusthet i mobila ad hoc-nät.



Figur 6.1: Diagrammet visar hur medelandel lyckade sessioner beror av trafikbelastningen, när nätet utsätts för en intern attack. Som jämförelse visas även samma system utan attack samt med och utan intrångsdetektering.

7 Slutsatser

Hur väl ett ad hoc-nät fungerar är starkt kopplat till dess kapacitet och förmåga att kunna hantera olika typer av tjänster, samt till nätets pålitlighet; det vill säga om man kan lita på att tjänsterna fungerar också under svåra förhållanden. Att åstadkomma detta är en utmaning då ett ad hoc-nät karakteriseras av dynamisk topologi, intermittent konnektivitet, varierade säkerhetskrav, opålitliga länkar samt brist på bandbredd och fast infrastruktur. Dessutom ska dynamisk trafik med varierande tjänstekvalitetskrav och prioritet kunna hanteras.

Första generationens taktiska nätverksradio finns idag tillgänglig men det återstår mycket forskning och utveckling innan näten blir så självkonfigurerande som skulle vara önskvärt. Det finns ett fundamentalt problem som behöver adresseras: det krävs för mycket mänsklig inblandning vid hanteringen och driften av dagens nät och arbetet behöver utföras av erfarna nätoperatörer. För att minska behovet av mänsklig inblandning behövs dynamiska, automatiserade mekanismer som styr näten. Framförallt behöver näten själva kunna konfigurera sig efter mobilitet och varierande trafik. En anpassning efter rådande förhållanden gör också att nätens prestanda kan förbättras. Dessutom finns det som alltid ett behov av att kunna öka datatakten på länkarna i nätet. Förutom att näten kan göras robustare och mer data kan överföras blir det då också lättare att hantera olika dynamisk skeenden, t.ex. genom att lämna marginaler vid resurstilldelningen.

För att kunna tillgodose behovet av att dynamiskt kunna hantera nya trafikflöden och deras krav avseende tjänstekvalitet behövs förbättrade trafikhanteringsmekanismer. Så länge det finns mer kapacitet tillgänglig än vad som efterfrågas, eller om trafiken är så predikterbar att resurser kan tilldelas i förväg, kan dagens metoder användas. I framtiden vill man dock att trafiken ska kunna hanteras dynamiskt. För att undvika att nätet blir överbelastat vid dynamisk trafikhantering behövs först och främst någon form av tillträdeskontroll, (*admission control*). Överbelastning i nätet är speciellt destruktivt när trafiken är fördröjningskänslig. Dessutom bör man lämna vissa marginaler och inte lasta nätet fullt ut med fördröjningskänslig trafik. Resurserna som lämnas kan då istället användas till icke fördröjningskänslig trafik. Notera att förutom tillträdeskontroll behövs också många andra mekanismer, t.ex. trängselhantering för att på ett tillfredställande sätt dynamiskt kunna hantera olika trafikklasser.

Mycket av trafiken i taktiska nät är av broadcast- eller multicasttyp, det vill säga en till alla, eller en till flera. Hur denna typ av trafikflöden ska distribueras effektivt är långt ifrån så väl utforskat som unicasttrafik (punkt till punkt). Eftersom en stor del av trafiken förväntas vara av broadcast/multicast-typ finns också betydande vinster att göra med en effektiv distribution av denna trafiktyp. Frågorna inkluderar routing, val av noder som återutsänder trafiken och vilken datatakt som ska väljas. Användande av hög datatakt innebär att ett mindre område (färre noder) nås jämfört med användande av låg datatakt då ett större område (fler noder) nås. Robusthet och tillförlitlighet är två viktiga egenskaper hos ett ad hoc-nät. Robusthet återkommer på olika nivåer i nätstyrningen och vid routing vill man ha robusta länkar med hög kapacitet i sin rutt. Detta kan vara viktigare än att momentant maximera kapaciteten på en länk. Det är snarare medelkapaciteten över tiden på en länk som är viktig. Om en länk högst tillfälligt får

hög kapacitet är det inte säkert att den förbättrade länkkapaciteten kan utnyttjas då det tar tid att fördela om trafiklaster till en ny länk. Det finns dessutom normalt en kostnad inblandad, på grund av kontrolltrafik, vid byte av rutter i nätet. Slutsatsen blir att man vid routing förutom kapacitet också bör försöka väga in robusthet och stabilitet, det vill säga hur lång tid en given rutt kommer att fungera.

Dynamisk hantering av tjänster och mobilitet kräver ett dynamiskt MAC-protokoll. En lämplig struktur hos ett dynamiskt MAC-protokoll är att vissa delar av protokollet använder konflikthanterande allokering såsom CSMA och resten reservationsbaserad allokering såsom TDMA. Dessa två allokeringsmetoder har var och en sina för och nackdelar, vilket gör en kombination fördelaktig. Sedan kan man dynamiskt, beroende på situationen, variera hur stor andel av protokollet som använder vardera metoden. Det finns också en stor potential i att använda spatiell TDMA (STDMA) där samma tidlucka kan användas av geografiskt separerade noder. När TDMA-baserade protokoll används, eller delar av protokollet baseras på TDMA, behöver tidluckor kunna allokeras både dynamiskt och distribuerat. Att kunna göra det utan att behöva införa för mycket kontrolltrafik är ett forskningsområde där det fortfarande återstår betydande arbete. Det finns dock föreslagna och fungerande metoder idag för att göra dynamisk allokering av tidluckor, men det finns definitivt utrymme för förbättringar och flera olika lösningar/metoder behöver undersökas.

Flerantennsystem, så kallade MIMO-system (*Multiple Input and Multiple Output*), är en lovande teknik när det gäller möjligheten att förbättra kapaciteten, dvs datatakterna, och robustheten vid trådlös kommunikation. Vid ett användning av MIMO i mobila ad hoc-nät finns också ett antal viktiga frågeställningar som har med mobiliteten att göra. Dock finns det uppenbara möjligheter att förbättra prestandan i ad hoc-nät genom införande av MIMO. Eftersom komplexiteten också ökar med ett MIMO-system krävs olika avvägningar avseende när och hur MIMO-tekniker ska införas. För statiska nät, och vid låg mobilitet, finns möjligheten att mångfaldiga kapaciteten. Det återstår dock att noggrannare undersöka vilka prestandavinster som går att åstadkomma vid högre mobilitet.

Säkerhet i kommunikationsnät är ett komplext problemområde. För mobila ad hoc-nät tillkommer ytterligare ett antal säkerhetsfrågeställningar. Radiogränssnittet erbjuder i sig möjligheter till olika säkerhetsattacker och om ett intrång skulle lyckas, så är ad hoc-nätsprotokollen känsliga för störningar eftersom de baserar sig på samarbetande radionoder. I projektet har vi fokuserat på intrångsdetektering, men vi konstaterar att det finns många andra viktiga säkerhetsproblem för mobila ad hoc-nät.

Publikationer inom projektet

[P1] J. Nilsson och U. Sterner. *Admission control in wireless multihop networks*, MILCOM. San Diego, USA, 17–19 november 2008.

Sammanfattning

Admission control is an essential part of a traffic management system. Overloading the network will only lead to congestion and performance degradations. The paper investigates how to design admission control in wireless TDMA-based multihop networks. Key components are the estimation of the available resources and how to coordinate the usage of these resources among the nodes. To increase robustness we use a resource margin to deal with uncertainties in the resource estimates. The traffic consists of a mix of two types: prioritized delay-sensitive traffic and background traffic. The investigation focuses on the robustness of different admission control methods. Fairness is also included. In particular, we consider how well the delay-sensitive traffic sessions over different path lengths are served. Moreover, we propose a method so that traffic sessions can be supported fairly when they have different path lengths.

[P2] J. Löfvenberg, J. Grönkvist, M. Sköld och A. Hansson. *Broadcast with variable data rates in mobile ad hoc networks*, Vetenskaplig Rapport FOI-R--2582--SE, Totalförsvarets Forskningsinstitut, Linköping, oktober 2008.

Sammanfattning

Vi utvärderar transmissionskostnaden för broadcast-trafik i ad hoc-nät med multipoint relay-flooding (MPR-flooding) och variabel datatakt. Mobila trådlösa ad hoc-nät består av ett antal noder, som bildar ett robust radionät utan fast infrastruktur och centraliserade funktioner. Militär mobil kommunikation genererar ofta en stor andel trafik av typen multicast (en-till-många) och broadcast (en-till-alla). Som exempel kan nämnas distribution av statusinformation, positionsinformation och gruppsamtal. Variabla datatakter på länkarna i nätet har potential att öka kapaciteten samt minska risken att tappa radionoder med svaga länkförbindelser. Rutterna i nätet blir också mer robusta om de ingående länkarna tillåts att gradvis försämras, snarare än att plötsligt försvinna, under ett visst signal-brus-förhållande. I analysen antar vi att alla noder i nätet använder en och samma datatakt och att de simultant kan variera denna datatakt för att förbättra nätets prestanda. Anledningen är att vi vill hitta uppslag till bra strategier för att hantera broadcast i nät med multipla datatakter. Som referens utvärderar vi också transmissionskostnaden för unicast-trafik (en-till-en) med variabel datatakt. I detta fall verkar det vara en bra strategi att sträva efter så hög datatakt som möjligt utan att nätet delas. I broadcast-fallet är det svårare att formulera en likartad generell strategi. För nät med låg bandbredd och hög nod-täthet ligger emellertid minimum för transmissionskostnaden nära den datatakt som motsvarar att centralt belägna noder når alla andra noder i nätet. I dessa nät kan det alltså vara en god strategi att välja en datatakt som

möjliggör ”tvåhopps-broadcast”: ett hopp in till en central nod och därifrån ett hopp ut till övriga noder i nätet. Detta påminner om transmissionsbeteendet i cellulära bas-stationsnät, vilket vi normalt inte brukar förknippa med ad hoc-nät.

[P3] J. Nilsson och U. Sterner. *Admission Control in Wireless Multihop Networks*, Vetenskaplig Rapport FOI-R--2384--SE, Totalförsvarets Forskningsinstitut, Linköping, december 2007.

Sammanfattning

Inträdeskontroll är en viktig komponent i ett trafikhanteringssystem. Att tillåta mer trafik i nätet än vad som kan hanteras leder endast till överbelastning i nätet och att nätets prestanda försämras. I rapporten behandlas inträdeskontroll i trådlösa flerhoppsnät. Näten har distribuerade funktionalitet och är baserade på TDMA. Ingen central nod med full kunskap, om resurstillgängligheten i nätet, kan ta besluten. Besluten tas istället distribuerat i all noder. Detta innebär då också att det inte existerar någon sammanslagen och synkroniserad information, avseende resurstillgängligheten. Vi undersöker först hur fördröjningskänsliga trafiksessioner med olika ruttlängder betjänas med och utan inträdeskontroll. Resultaten visar på vikten av att inträdeskontroll. Därefter föreslår och undersöker vi hur inträdeskontroll kan modifieras så att trafiksessioner betjänas rättvisst när de har olika ruttlängder.

[P4] J. Nilsson, O. Tronarp, G. Eriksson, P. Holm, E. Löfsved och J. Rantakokko. *Link and network capacity gains in ad hoc networks utilizing MIMO-techniques*, MILCOM, p. 1–8. 29–31 oktober 2007, Orlando, FL, USA. FOI-S--2676--SE.

Sammanfattning

Multiple-Input Multiple-Output (MIMO) antenna systems is a promising technique for achieving substantially increased capacities and robustness in future tactical wireless networks. The purpose of this work has been to investigate the theoretical link and network capacity gains that can be achieved by employing MIMO-techniques in wireless ad hoc networks. We study these gains from a theoretical viewpoint and derive a closed-form expression of the network capacity for a reservation based MAC protocol that utilizes traffic adaptation. The link and network capacities are thereafter examined in urban environments, using two different MIMO channel models. Furthermore, the effect of utilizing MIMO-systems on the mean route lengths and the number of used links are investigated.

[P5] J. Grönkvist, A. Hansson och M. Sköld. *OLSR broadcast security in mobile ad hoc networks*, Vetenskaplig Rapport FOI-R--2323--SE, Totalförsvarets Forskningsinstitut, Linköping, september 2007.

Sammanfattning

Ett mobilt trådlöst ad hoc-nät består av ett antal noder, som bildar ett robust radionät utan fast infrastruktur och centraliserade funktioner. I dessa sammanhang är sårbarhet för attacker och säkerhetsfrågor viktiga problem att lösa. I militära scenarier brukar multicast-trafik och broadcast-trafik anses viktiga. Ad hoc-nät som kan hantera sådan trafik är dock mycket svårare att realisera än motsvarande nät som bara hanterar unicast-trafik. ”Advanced signatures” är en metod att höja säkerheten i OLSR. I denna rapport visar vi att andelen administrativ trafik blir mycket hög och detta kräver vidare utveckling. Lokalt informationsutbyte är enklare att säkra med signaturer, vilket kan utnyttjas förMPR-flooding. Vi har också jämfört olika broadcasttekniker som utnyttjar varierande mängd information och studerat deras effektivitet. Resultaten visar att MPR-flooding kan ge en god balans mellan kapacitet, säkerhet och robusthet i mobila ad hoc-nät.

[P6] T. Holmberg, J. Grönkvist, J. Nilsson och M. Sköld. *Traffic estimation in mobile TDMA-based ad hoc networks*, 6th Annual Mediterranean ad hoc networking workshop., p. 85-91. 12-15 juni, 2007, Corfu, Grekland. FOI-S--2587--SE.

Sammanfattning

A traffic estimator is developed and thereafter used to do the slot assignment in a traffic adaptive TDMA scheme. The traffic estimation is made packet-by-packet and locally in the nodes. The purpose of the work is to investigate the efficiency of such traffic estimation. To do that we compare traffic-adaptive TDMA, using our traffic estimator, to non traffic-adaptive TDMA and ”optimal” TDMA, i.e., a centralized scheme having complete knowledge about the traffic situation. The introduced traffic estimator uses two steps in order to predict the traffic over the links in ad hoc networks. At first, an exponential filter is used to generate an estimate based on the size and the intensity of arrival of the transmissions. The estimation error of the exponential filter is further reduced by a multiplication of a function that considers queuing times in the links. The assessment of the traffic estimator and traffic adaptive TDMA is made for traffic sessions with delay constraints. Simulation results show that adding our traffic estimation to TDMA-based mobile ad hoc networks yields a significantly higher ratio of successfully transmitted sessions compared to the case without traffic estimation.

[P7] J. Grönkvist, A. Hansson och M. Sköld. *Evaluation of a specification-based intrusion detection system for AODV*, 6th Annual Mediterranean ad hoc networking workshop., p. 121-128. 12-15 juni, 2007, Corfu, Grekland. FOI-S--2586--SE.

Sammanfattning

A mobile ad hoc network consists of wireless nodes that build a robust radio network without any preexisting infrastructure or centralized servers. However, these networks have inherent vulnerabilities that make them susceptible to malicious attacks. In order to secure ad hoc networks advanced techniques must be used, one efficient solution is to use specification-based intrusion detection, especially when combined with traditional cryptographic methods.

In this paper, we study attacks on realistic networks to see what effect they have on communications. We show that some of the well known attacks on AODV do have a significant effect, preventing more or less all nodes from communicating. However, as we also show, our specification-based Intrusion Detection System removes almost all of the effects of the attacks by discarding detected incorrect packets. This can be done with very little cost in terms of overhead and false alarms.

[P8] T. Holmberg. *Trafikestimering i mobila ad hoc-nät*, Teknisk Rapport FOI-R--2242--SE, Totalförsvarets Forskningsinstitut, Linköping, februari 2007.

Sammanfattning

För att minska sårbarheten i försvarets kommunikation eftersträvas system utan fast infrastruktur. Ad hoc-nät har en dynamisk struktur och saknar funktionsavgörande enheter. I ad hoc-nät färdas information från startdestination till slutgiltig destination genom att förmedlas via mellanliggande enheter. Ett betydande problem vid användning av ad hoc-nät, i synnerhet mobila, är hur nätets kapacitet ska fördelas. I denna forskningsstudie undersöks möjligheten att utnyttja trafikestimering för att fördela mobila ad hoc-näts resurser. Den introducerade trafikestimatorn uppskattar trafiken över nätets länkar i två steg. Först skapas ett estimat utgående från datasändingarnas storlek och ankomstintensitet. I ett andra steg reduceras estimeringsfelet genom hänsyn till datapaketens kötider. När trafikestimatorns uppskattningar används vid resurstilldelning i TDMA-baserade mobila ad hoc-nät förbättras andelen lyckat genomförda talsessioner betydligt.

[P9] J. Nilsson, J. Rantakokko och O. Tronarp. *Ad Hoc network capacity utilizing MIMO-techniques*, Teknisk Rapport FOI-R--2167--SE, Totalförsvarets Forskningsinstitut, Linköping, december 2006.

Sammanfattning

Flerantennsystem (MIMO) är en lovande teknik när det gäller möjligheten att avsevärt kunna öka kapaciteten och robustheten i trådlösa taktiska kommunikationssystem. Syftet med arbetet har varit att undersöka de möjliga

nätvinsterna för trådlösa ad hoc-nät vid användande av MIMO-tekniker. Vi har studerat vinsterna utifrån ett teoretisk perspektiv och härlett ett slutet uttryck för nätkapaciteten. Dessutom har nätkapaciteten också undersökts, med hjälp av två olika kanalmodeller avsedda för stadsmiljöer. Resultaten visar på att MIMO länkkapacitetsvinsterna, för de länkar som används, överförs till liknande nätkapacitetsvinster. Nättopologin påverkar dock kraftigt den möjliga nätkapacitetsvinsten. För de undersökta kompakta näten är MIMO länkkapacitetsvinsten i medel avsevärt mindre än för de glesa näten.

[P10] E. Johansson, A. Hansson, J. Grönkvist och U. Sterner. *Routing hysteresis impact on traffic adaptation*, Teknisk Rapport FOI-R--2166--SE, Totalförsvarets Forskningsinstitut, Linköping, december 2006.

Sammanfattning

Vid taktiska operationer är kapaciteten i mobila ad hoc-nät av stor vikt. Nätets resurser måste därför utnyttjas effektivt samtidigt som kommunikationstjänster i nätet ska erbjudas med god kvalitet. För att öka kapaciteten, anpassar trafikadaptiva accessprotokoll resursallokeringen så att länkar med hög belastning kompenseras med mer kanalresurser. På grund av mobiliteten förändras rutterna i nätet, vilket medför att resursallokeringen måste anpassas till de nya trafiklaster som uppkommer. I samband med detta genereras overhead-trafik. Om rutterna ändras för ofta så kan overhead-trafiken orsakad av trafikadaptionen bli onödigt stor. Genom att införa hysteresströsklar i routingalgoritmen kan rutterna göras mer stabila till priset av rutter med lägre kapacitet. Vi tar fram ett effektivitetsmått för trafikadaptionen och beräknar detta för simulerade nät med fast och variabel datatakt på länkarna. Näten har slumpmässig mobilitet och olika storlekar. Vi visar även att små tröskelvärden i routingprotokollet möjliggör en högre nyttotrafik i de nät vi simulerat.

[P11] H. Tullberg. *Cross-layer design i kommunikationssystem - en översikt*, Teknisk Rapport FOI-R--2069--SE, Totalförsvarets Forskningsinstitut, Linköping, oktober 2006.

Sammanfattning

De senaste åren har cross-layer design (lageröverskridande design) rönt starkt intresse inom kommunikationsforskningen. Vid cross-layer design genomför man samtidig optimering av funktioner i flera lager i en referensmodell med avseende på en systemkritisk dimensionerande resurs, t ex nätkapaciteten eller batterilivslängden. Rätt använt kan cross-layer design leda till stora prestandavinster medan felaktig användning kan medföra en oavsiktlig begränsning i modulariteten. Rapporten behandlar olika aspekter av cross-layer design och dess inverkan på effektiva kommunikationssystem. I rapporten inventeras pågående forskning om cross-layer design för kommunikationssystem. Vi diskuterar definitioner och olika tolkningar av cross-layer design. Vi föreslår en definition enligt följande: Cross-layer design är när man avviker från en specifik referensmodell, genom extra informationsflöde eller på annat sätt, i syfte att optimera prestanda med

hänsyn till en specificerad kritisk resurs för ett väl avgränsat system. Vi konstaterar även att det behövs en ny radioreferensmodell som tar hänsyn till utbredningsegenskaper och behov av flexibilitet i radionära signalbehandling men ändå ger tillräcklig struktur för modularitet. Slutligen ger vi exempel på områden där cross-layer design är av intresse för militär kommunikation och pekar på nya möjligheter inom taktiska radionät och sensornät.

[P12] S. Linder. *Evaluation of a method based on the impulsiveness ratio to estimate the communication performance*, EMC Europe 2006, p. 470-474. 4-8 september 2006, Barcelona, Spanien. FOI-S--2290--SE.

Sammanfattning

Determining the impact on digital communication systems from electromagnetic interference often requires complex analyses or computations. Therefore, there is a need for lowcomplexity approximate methods. A commonly used approximation is to treat the interference as additive white Gaussian noise (AWGN), when estimating the resulting bit error probability (BEP). In this paper we investigate a quality measure to improve the AWGN approximation. The method uses the impulsiveness correction factor (ICF) based on the impulsiveness ratio to correct the AWGN approximation. The conclusion is that the ICF is useful for different kinds of pulsed signals. For other types of signals the ICF is often to low. However, when the interference is a mix of pulses signals the result from the ICF is often better than the result from only using the AWGNapproximation.

[P13] J. Grönkvist. *Novel assignment strategies for spatial reuse TDMA in wireless ad hoc networks*, Wireless networks, vol. 12, no 2, mars 2006, p. 255-265. FOI-S--2449--SE.

Sammanfattning

Spatial reuse TDMA has been proposed as an access scheme for multihop radio networks where real-time service guarantees are important. The idea is to increase capacity by letting several radio terminals use the same time slot when possible. A time slot can be shared when the radio units are geographically separated such that small interference is obtained. In reuse scheduling, there are several alternative assignment methods. Traditionally, transmission rights are given to nodes or to links, i.e., transmitter/receiver pairs. We present a comparison of these two approaches and show that both have undesirable properties in certain cases, e.g. link assignment gives a higher delay for low traffic loads but can achieve much higher throughput than node assignment. Furthermore, we propose a novel assignment strategy, achieving the advantages of both methods. Simulation results show that the proposed method can achieve the throughput of link assignment for high traffic loads as well as the lower delay characteristics of node assignment for low traffic loads.

Övrga referenser

[1] Editor: Mattias Sköld. *Mobila ad hoc-nät – Utmaningar och möjligheter*, User Report FOI-R--1799--SE, Swedish Defence Research Agency, Linköping, December 2005.

[2] Editor: Jan Nilson. *Ad hoc networks – Routing and MAC design*, Technical Report FOI-R--1801--SE, Swedish Defence Research Agency, Linköping, december 2005.

[3] Websida, kontaktperson: Thorbjörn Ericson, FMV. *GTRS nulägesdemo 7 - 9 oktober i Enköping*, Försvarsmakten.

[4] Jimmi Grönkvst. *Interference-Based Scheduling in Spatial Reuse TDMA*, PhD thesis, KTH Electrical Enginering, september 2005.

[5] D. Raffo, C. Adjih, T. Clausen och P. Mühlethaler. *An Advanced Signature System for OLSR*, Proc. of the 2nd ACM Workshop on Security of ad hoc and Sensor Networks, SASN 2004, vol. 2, oktober 2004.

[6] C. Perkins, E. Belding-Royer och S. Das. *Ad hoc On-Demand Distance Vector (AODV) Routing*, RFC 3561, juli 2003.

[7] T.Clausen och P.Jacquet. *Optimised Link State Routing Protocol (OLSR)*, RFC 3626, oktober 2003.