



CSMA för backbone-nät

ARWID KOMULAINEN, JIMMI GRÖNKVIST OCH ULF STERNER

Arwid Komulainen, Jimmi Grönkvist och Ulf Sterner

CSMA för backbone-nät

Titel	CSMA för backbone-nät
Title	CSMA in backbone networks
Rapportnr / Report No.	FOI-R--4569--SE
Månad / Month	Februari / February
Utgivningsår / Year	2018
Antal sidor / Pages	29
ISSN	1650-1942
Kund / Customer	FM
Forskningsområde	4. Informationssäkerhet och kommunikation
FoT område	Ledning och MSI
Projektnr / Project No.	E722104
Godkänd av / Approved by	Christian Jönsson
Ansvarig avdelning	Ledningssystem
Exportkontroll	Innehållet är granskat och omfattar ingen information som är underställd exportkontrollagstiftningen.

Detta verk är skyddat enligt lagen (1960:729) om upphovsrätt till litterära och konstnärliga verk, vilket bl.a. innebär att citering är tillåten i enlighet med vad som anges i 22 § i nämnd lag. För att använda verket på ett sätt som inte medges direkt av svensk lag krävs särskild överenskommelse.

This work is protected by the Swedish Act on Copyright in Literary and Artistic Works (1960:729). Citation is permitted in accordance with article 22 in said act. Any form of use that goes beyond what is permitted by Swedish copyright law, requires the written permission of FOI.

Sammanfattning

I denna rapport undersöks hur väl ett CSMA-baserat accessprotokoll fungerar i ett semi-mobilt backbone-nät. De nät som undersöks upptar större ytor och inkluderar längre länkar än taktiska ad hoc-nät. Protokollen som används måste därmed anpassas och för CSMA innebär det huvudsakligen att väntetiderna i protokollet måste öka markant. En följd av de ökade väntetiderna är att nätet enbart presterar bra så länge paketen som skickas är stora. Nätverkssimuleringar används för att undersöka hur olika nätaspekter, trafikmodeller och parameter-
val påverkar vilken kapacitet för användartrafik som erhålls. Resultaten tyder generellt på att en kapacitet uppåt 20-30% av den totala bandbredden är vad som kan förväntas i de scenarier som undersökts. Kapaciteten kan dock variera mycket beroende på nodernas placeringar och fördelning av trafik i nätet.

Nyckelord: Backbone-nät, CSMA

Abstract

This report presents a study on the performance of a CSMA based access protocol in a semi mobile backbone network. The networks investigated cover larger areas and include longer links than what is typical for tactical ad hoc networks. The protocols used must therefore be adapted and for CSMA this mainly means that protocol wait times need to be significantly increased. When the wait times increase, data packet length also needs to increase in order for the protocol to perform well. Network simulations are used to determine how different network aspects, traffic models and parameter settings affect the capacity for delivering user traffic. The results suggest a capacity of up to 20-30% of the available bandwidth can be achieved in the evaluated scenarios. However, the capacity is greatly affected by the placement of nodes and the how traffic is distributed in the network.

Keywords: Backbone networks, CSMA

Innehållsförteckning

1	Introduktion	7
2	Bakgrund	9
2.1	CSMA för unicasttrafik	9
2.2	Konsekvenser av stora avstånd	10
2.3	Relaterat arbete	11
3	Scenario för simuleringar	13
3.1	Generering av nät	13
3.2	Trafik i nätet	15
3.3	Konfigurering av CSMA	15
3.4	Konfigurering av OLSR	16
4	Resultat	19
4.1	Beräkning av kapacitet	19
4.2	Nätstorlek och topologi	19
4.2.1	Nätstorlek och terräng	20
4.2.2	Spridning mellan nät	21
4.3	Trafikmönster	22
4.3.1	Paketstorlek	23
4.3.2	Trafikriktning	23
4.4	Parameterinställningar	24
4.4.1	OLSR-parametrar	24
4.4.2	Contention window	25
5	Slutsatser	27

1 Introduktion

Militära backbone-nät syftar till att upprätthålla kommunikation över långa avstånd. Dessa nät syftar typiskt till att upprätthålla kommunikation mellan olika bataljoner, kompanier och stabsplatser. Ett sådant scenario kan bestå i att upprätta kommunikation inom en brigad. Ytan som ett sådant nät måste kunna täcka motsvarar därmed ett område som en brigad förväntas verka inom. Nät över så pass stora ytor innebär andra utmaningar är taktiska nät och det är inte säkert att tekniker som fungerar väl i taktiska nät också gör det i ett backbone-nät, och vice versa.

I [1] undersöktes hur pass väl *Carrier Sense Multiple Access* (CSMA) fungerade som accessprotokoll i ett taktiskt nät. Resultaten pekade på att med broadcast-trafik som huvudsaklig typ av användartrafik och hög mobilitet så fungerade inte CSMA bra. I ett backbone-nät är trafikbilden annorlunda och utgörs i högre grad av punkt-till-punkt-trafik. Detta skulle kunna medföra att CSMA är mer lämpat att användas i dessa typer av nät. En fördel med att använda CSMA istället för *Time Division Multiple Access* (TDMA) i ett backbone-nät är att tekniken i stora delar är standardiserad; för TDMA-protokoll som hanterar trafikutjämning finns ingen standard som är accepterad i samma utsträckning. I CSMA är dessutom trafikutjämning till stor del inbyggt i protokollets grundfunktion. De huvudsakliga avseenden i vilka backbone-nät skiljer sig från taktiska nät är följande:

- När näten skall täcka större ytor krävs längre länkar mellan kommunicerande noder. Detta kan realiseras med hjälp av bland annat upphöjda antenner, mer avancerade antennkonstruktioner samt strategiska val i hur nättopologin byggs upp. Det sistnämnda kan handla om att med hjälp av planeringsverktyg välja ut nodplaceringar med fördelaktiga mottagningsförhållanden, exempelvis på höjder i terrängen.
- Backbone-nät är inte utsatta för samma höga mobilitet som taktiska nät. Att exempelvis resa en mast utrustad med en antenn tar tid och omgruppering bör därför ske relativt sällan. En följd av detta är att dessa typer av nät bör vara relativt statiska, i termer av att länkar sällan går upp och ner.
- Den typ av datatrafik som skickas i backbone-nät har andra egenskaper än trafiken i taktiska ad hoc-nät. I backbone-nät kan en större andel av trafiken antas vara av typen punkt-till-punkt (en sändare, en mottagare), och paketen är typiskt större än i taktiska nät. Tjänster som genererar den här typen av trafik kan till exempel vara ordergivning, filöverföringar, utbyte av lägesinformation.

De ovan beskrivna skillnaderna kan ha stor påverkan på hur kommunikationslösningar bör designas för backbone-nät. Framförallt långa kommunikationsavstånd är en egenskap som sällan undersöks i kontext av militära nät. I det här arbetet ligger fokus på kanalaccess och mer specifikt på att utvärdera hur väl en lösning baserad på CSMA fungerar i ett backbone-nät.

Utvärderingen baseras på nätverkssimuleringar för att undersöka hur prestandan hos CSMA påverkas av bland annat nätaspekter och användartrafik. Det bakomliggande kommunikationsscenarioet är kommunikation mellan bataljoner inom en brigad, mer specifikt kommunikation mellan brigadstab och bataljon eller kompani. Kommunikationen består i huvudsak av punkt-till-punkttrafik och nätet modelleras som snapshots av ett semimobilt nät.

Rapporten inleds med en beskrivning av hur CSMA hanterar punkt-till-punkttrafik och vad de långa avstånden har för påverkan på protokollet. Kapitel innehåller även en översikt av relaterat arbete. I Kapitel 3 beskrivs scenarioet som använts i simuleringarna för att utvärdera prestandan. Resultaten från simuleringarna presenteras i Kapitel 4 och rapporten avslutas med slutsatser kring resultaten i Kapitel 5.

2 Bakgrund

I detta arbete utgår vi så långt det är möjligt från den beskrivning av CSMA som ges för accessmetoden *Distributed Coordination Function* (DCF) i IEEE:s standard för lokala trådlösa nätverk (WLAN) IEEE 802.11. Eftersom huvuddelen av trafiken i WLAN är av typen punkt-till-punkt, finns det flera funktioner i standarden för att hantera den typen av trafik effektivt. Standarden är dock utvecklad primärt för korta avstånd vilket leder till att vissa parameter-justeringar är nödvändiga för att protokollet ska fungera i backbone-nät.

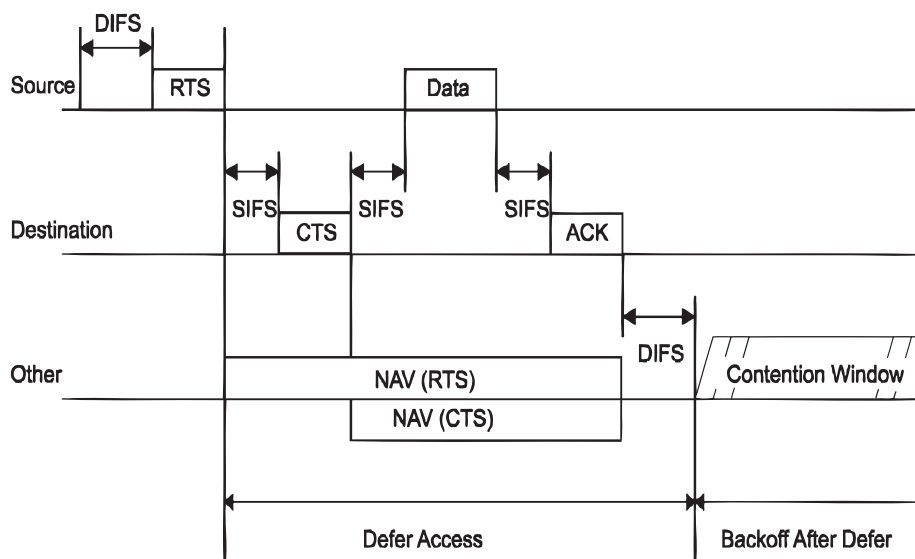
2.1 CSMA för unicasttrafik

Då vi i [1] fokuserade på broadcasttrafik kunde inte vissa tekniker användas, så som kanalreservering med *Request To Send* (RTS) och *Clear To Send* (CTS) och omsändningar av paket med hjälp av *Acknowledgements* (ACK). Meddelanden av typen RTS/CTS minskar risken för kollisioner i vissa fall och omsändningar leder till robustare paketförmedling i händelse av kollisioner och fädningsdippar.

I backbone-nät kan vi dock anta att en större andel av trafiken är punkt-till-punkt och då kan dessa funktioner användas. I Figur 2.1 illustreras hur kanallaccess typiskt sker för ett sådant fall. Källnoden börjar med att skicka ett RTS-meddelande efter att kanalen varit ledig en tid kallad *DCF Interframe Space* (DIFS). Den mottagande noden svarar med ett CTS-meddelande en kort tid efter att RTS-meddelandet mottagits, kallad *Short Interframe Space* (SIFS). Tiden kallad SIFS är kortare än DIFS vilket gör att CTS-meddelanden inte behöver konkurrera med andra noders datapaket om kanalresurser.

När källnoden tagit emot CTS-meddelandet kan den skicka sitt datapaket, varefter mottagande noden svarar med en ACK. Liksom CTS-meddelanden skickas också ACK-meddelanden med en kortare fördröjning för att undvika kanalkonkurrens med datapaket. Noder som hör RTS eller CTS får reda på den kommande sändningen och kan därmed undvika kolliderande sändningar. Notera att den schematiska bilden, från [2, s. 264], helt bortser från utbredningstider.

Genom att använda RTS/CTS minskar risken för problem orsakade av så kallade *hidden nodes*. Problem med hidden nodes uppstår när en grannod till den mottagande noden inte hör den sändande noden och därmed riskerar orsaka kollisioner hos den mottagande noden. Då den mottagande noden skickar ett CTS-paket nås typiskt denna nod och problem med hidden nodes minskar. En vidare fördel som följer av detta är att huvuddelen av alla kollisioner sker för RTS-paket. Då dessa paket typiskt är mycket mindre än datapaketerna innebär



Figur 2.1: Kanalaccess vid unicasttrafik. Bild tagen från [2, s. 264]

det att kanalen blockeras en kortare tid vid en kollision när RTS/CTS används.

2.2 Konsekvenser av stora avstånd

Med de stora avstånd mellan noder som uppstår i ett backbone-scenario följer några konsekvenser för hur CSMA fungerar. En central parameter för protokollet kallad *aAirPropagationTime* ska motsvara den maximala utbredningstiden, tur och retur, mellan två noder. Denna parameter garanterar bland annat att carrier sensing hinner utföras. Andra tider som styrs av denna parameter är hur länge noder väntar på CTS- och ACK-meddelanden. I typiska WLAN-nät är denna parameter ca 1 mikrosekund vilket motsvarar ett maximalt kommunikationsavstånd på cirka 150 meter. I backbone-nät, där länkar kan vara flera mil långa krävs att denna parameter är i intervallet 60-330 mikrosekunder (ca 1-5 mil maximalt kommunikationsavstånd).

Ju längre *aAirPropagationTime* är, desto sämre utnyttjas kanalen eftersom en större andel av tiden spenderas i passivt läge. I typiska scenarion där CSMA används, exempelvis WLAN, är dessa utbredningstider i stort sett försumbara i förhållande till paketlängderna. En konsekvens av detta är att man bör skicka väldigt stora paket i backbone-näten för att få vettig effektivitet i kanal användningen. Att öka datatakten på länken ger en relativt liten vinst, eftersom väntetiderna inte påverkas. Tvärtom, om datatakten ökar kommer sändningstiden för

ett paket att minska medan utbredningstiderna är oförändrade. Vissa funktioner i protokollet kan dessutom behöva stängas av om avstånden är långa och paketlängderna korta eftersom de då inte fungerar som tänkt. Ett exempel är fallet då en nod tar emot ett RTS-meddelande avsett för en annan nod. Nominellt kommer noden då blockera kanalen så länge som anges i RTS-meddelandet. Dock kan noden avblockera kanalen om den inte hör en påföljande paketsändning inom ett definierat kortare interval, *RTS-timeout*. Denna funktionalitet ska göra att noder kan komma åt kanalen snabbare. Dock kan *RTS-timeout* bli längre än den totala paketsändningstiden om paketen är korta och utbredningstiderna långa. I detta fall bör man stänga av möjligheten att använda *RTS-timeout*.

2.3 Relaterat arbete

Det finns ytterst lite publicerat om prestanda för CSMA i nät med långa utbredningstider. Vad gäller användning av CSMA i militära nät i allmänhet och backbone-nät i synnerhet finns i princip inga vetenskapliga publikationer. Det största användningsområdet för CSMA är som accessteknik i lokala trådlösa nät (WLAN) som en del av standarden IEEE 802.11. I och med detta är mycket av forskningen kring CSMA inriktad på just WLAN-scenarion där avstånden är korta och där kommunikationen i regel inte kräver mer än ett hopp.

Jobb har gjorts för att ta fram tillägg till 802.11-standarderna som är anpassade för längre avstånd. Tillägget kallat 802.11ah är framtaget för att användas under 1 GHz (typiskt kring 700-900 MHz) för bland annat sensornätverk och så kallad *long range WiFi*. Fokus ligger på låg energiförbrukning och stora nät med upp till tusentals sensorer. Kommunikationsavstånden sträcker sig upp mot ett par kilometer, jämfört med traditionella WLAN-nät där maxavståndet är ett par hundra meter [3]. Ett närbesläktat tillägg, kallat 802.11af eller *White-Fi*, är framtaget för att verka i oanvända TV-band, 54-698 MHz. I detta tillägg ligger tonvikten på kognitiva tekniker för att finna ledigt spektrum [4].

Ett par studier har gjorts som undersöker hur ökade utbredningsavstånd påverkar prestandan hos MAC-protokollet i 802.11, för ett scenario där 802.11 används för att leverera internetförbindelse till landsbygden. I [5, 6] studeras paketförlusten som en funktion av utbredningsavstånd för en länk som bär trafik i båda riktningar och som utnyttjar CSMA för kanalaccess. I båda studierna finner man att utbredningstiderna orsakar stora kapacitetsförluster, i huvudsak på grund av att en stor del av tiden går till att vänta på acknowledgements. Gemensamt för dessa arbeten är att de bara studerar enstaka länkar snarare än nät med multihopp-kommunikation. Även i [7] studeras hur långa länkar påverkar prestandan hos för MAC-protokollet i 802.11. Författarna lyfter fram vikten av att justera den maximala utbredningstiden vid långa avstånd samt

presenterar en teoretisk modell för att utvärdera långa länkar i ett 802.11-nät.

3 Scenario för simuleringar

Nätverkssimuleringar har använts för att analysera hur ett backbone-nät som använder CSMA fungerar samt vilka parametrar som påverkar prestanda som kapacitet och fördröjning. Simuleringarna är utförda med en paketbaserad nätverkssimulator utvecklad i C++ kallad Aquarius. I Tabell 3.1 sammanfattas de parametrar som används i simuleringarna.

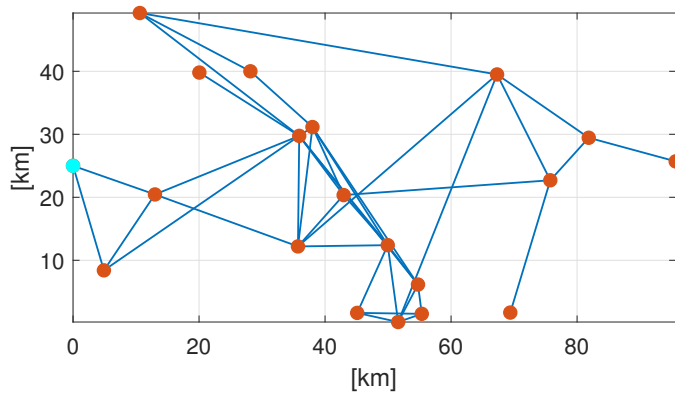
3.1 Generering av nät

Vi utgår från att området som skall täckas in har ett djup på 100 km. Två storlekar på nätet utvärderas, för det mindre nätet är bredden på nätet 50 km och i det större nätet 100 km. I det mindre nätet är antalet noder 20 noder och i det större nätet är antalet noder 40, antalet noder per ytenhet är alltså lika i båda näten. I båda fallen antas en stabsplats placerad i ena änden av nätet, i Figur 3.1 den turkosa cirkeln längst till vänster i bilden. Dessa nätstorlekar stämmer överens med nätstorlekar som används i bland annat [8, s. 5] och [9, s. 13] som båda berör sammanlänkning av brigad. Vidare undersöks två terrängområden där ett är lokaliserat kring Östergötland och det andra i Jämtland. Centerfrekvensen är vald till 1,35 GHz, densamma som RL371, och dataakten är 2 Mbit/s.

Vi utgår från att noderna inte kan kommunicera under förflyttning och simulerar därför endast statiska nät. Varje sådant statiskt nät kan ses som ett snapshot av ett semi-mobilt nät där vissa noder ibland omgrupperar sig. Noderna förutsätts ha upphöjda antenner med en höjd på 15 m och rundstrålande antenner med en antennvinst på 3 dB. Denna lösning kan tänkas motsvara att antennen placeras i en mast eller en mindre, ankrad UAV. I det senare fallet kan man inte räkna med att använda en riktningssärlig antenn, därmed antas antennförstärkningen vara låg.

För att binda samman ett nät över så stora avstånd som undersöks i detta scenario, med ett begränsat antal noder, krävs att noderna placeras ut på platser i terrängen med bra förutsättningar för kommunikation. En högt placerad position medger i regel fri sikt och därmed bra vågutbredningsegenskaper. Höjddata för de terränger som undersöks används för att reglera nodernas positioner till upphöjda platser. Utplaceringen av noderna sker enligt följande algoritm för att generera multipla nätrealisationer med sammanhängande nät.

1. Den totala ytan delas in i ett rutnät där varje ruta har en sidlängd på 5 km.
2. Till att börja med placeras en nod ut i varje terrängruta. Då en nod placeras ut i en terrängruta slumpas dess position bland de 5% högsta punkterna inom rutan. Vidare kontrolleras minsta avståndet mellan alla noder



Figur 3.1: Exempel på en nättopologi. Röda cirklar representerar kommunikationsnoder och den turkosa cirkeln motsvarar stabsp platsen.

så att det är större än 2,5 km.

3. När den första utplaceringen av noderna är klar väljs ett antal av dessa noder slumpmässigt ut som måste tillhöra nätet. Därefter reduceras nätet ner till rätt antal noder genom att stegvis eliminera noder från den delmängd som inte måste tillhöra nätet.
4. Kriteriet för att välja vilka noder som elimineras i varje steg är att de utvalda noderna från steg 3 är förbundna, samt att noden som elimineras har minst påverkan på avståndet till de noder som måste nås.
5. Endast de nät som är helt förbundna när nätet reducerats till sökt antal noder sparas.

Metoden är beräkningstung men ämnar att emulera ett avancerat nätplaneringsverktyg och samtidigt möjliggöra ett stort antal topologier. De nät som genererats är förbundna nät med stabila länkar och god variation av topologier. Totalt genereras 32 realisationer av respektive nätstorlek och terrängprofil. I Figur 3.1 illustreras ett exempel på ett nät som genererats med den ovan beskrivna metoden.

3.2 Trafik i nätet

All trafik som sänds från applikationsnivå är punkt-till-punkt-trafik. Paketstorleken varieras för att undersöka hur storleken på paketen påverkar systemets kapacitet. Dock är paketstorleken låst under en simulering, det vill säga alla paket antas ha samma storlek under en simulering. Vidare undersöks även hur trafikmönstren påverkar protokollet. I scenariot antas nod nummer noll motsvara en stabsplats. Denna nod är alltid placerad i utkanten av nätet. Vi har antagit att användartrafiken går från stabsplatsen till en nod i nätet eller vice versa. I det ena extremfallet är det alltid nod noll som skickar trafik och mottagarnoden slumpas bland resterande noder. I det andra extremfallet är det alltid nod noll som är mottagare och sändare slumpas bland resterande noder. Därutöver simuleras scenarion där trafik utgörs av olika blandningar av de två trafikmönstren.

I tillägg till trafiken från applikationen sänder även nätverkslagret kontrolltrafik. Denna trafik består av två typer av meddelanden: HELLO-meddelanden som skickas som broadcast ett hopp och TC-meddelanden som skickas som broadcast till alla noder i nätet. Alla noder skickar periodiskt bägge meddelandetyperna och beroende på hur ofta de skickas kan dessa påverka applikationstrafiken i olika stor grad.

3.3 Konfigurering av CSMA

I den mån det är möjligt används uteslutande standardparametrar från IEEE 802.11 för CSMA. Ett antal parametrar måste dock justeras med avseende på att utbredningstiderna är längre än i ett typiskt WLAN-scenarion. En central parameter i det här avseendet är *aAirPropagationTime*, som ska motsvara den maximala utbredningstiden, tur och retur, mellan två noder. I WLAN-nät har denna parameter ingen större påverkan, den är typiskt satt till att motsvara ett maximalt kommunikationsavstånd på 150 m, vilket förmodligen är i överkant för de flesta WLAN-nät. Parametern ska enligt standard styra ett antal andra parametrar i protokollet så som backoff-tider och timeout-perioder då en nod väntar på ACK eller CTS. Är air propagation time för lågt inställd kan det leda till kollisioner eftersom vissa noder då inte hinner detektera sändningar från andra noder som befinner sig långt bort. För låg air propagation time kan också leda till onödiga omsändningar om ACK-timeout och CTS-timeout, tiderna en sändande nod väntar på ACK respektive CTS, inte är tillräckligt långa. I de scenarion som studeras här behöver air propagation time ökas rejält för att kollisioner ska undvikas. Eftersom denna parameter har stor påverkan på protokollet har vi antagit att man i dessa scenarier har en uppfattning om länkarna i nätet och kan anpassa parametern till de gränsättande länkarna i det aktuella

fallet. Denna parameter sätts därmed individuellt för varje nätrealisation baserat på den längsta länken i det aktuella nätet.

För unicast används RTS/CTS för att uppnå effektivare kanalutnyttjande, åtminstone för stora paket. I simuleringarna utvärderas CSMA både med och utan RTS/CTS, då det inte är självklart att det ger någon vinst med de förhållanden mellan utbredningstider och paketstorlekar som är aktuella.

3.4 Konfigurering av OLSR

Vi antar att de backbone-nät som undersöks i denna rapport kan ses som relativt statiska nät. Förändringar i nätstrukturen kan ske i och med att noder förflyttas mellan två punkter men vi antar att dessa noder inte kommunicerar under förflyttning. Dessa nodrörelser antas ske i liten skala och däremellan kan nätet betraktas som statiskt. I ett scenario som beskrivs här kan man anta att en längre uppkopplingstid kan accepteras än i ett taktiskt ad hoc-nät. I ett semi-stationärt nät bör också förflyttningar ske relativt sällan och därmed bör antalet länkförändringar i nätet vara lågt.

Som nätverksprotokoll antas *Optimized Link State Routing* (OLSR) användas eftersom detta är ett välanvänt standardprotokoll för militära nät. Nätverksprotokollet bör ha relativt liten påverkan på resultaten sett till att näten som studeras är statiska. OLSR använder sig av två typer av kontrollmeddelanden för att bygga upp routingtabeller, HELLO-meddelanden och Topology Control-meddelanden (TC). HELLO-meddelanden skickas som broadcast ett hopp och används för att välja vilka noder som skall vidareända broadcasttrafik, så kallade MPR-noder. TC-meddelanden skickas som broadcast till hela nätet med hjälp av MPR-noderna och används för att bygga unicast-router. I och med att dessa pakettyper skickas som broadcast riskerar man få liknande problem som i [1], det vill säga inga ACK:ar, RTS eller CTS kan användas för dessa paket och därmed kan man inte ha ett variabelt contention window. I [1] visade vi att för att undvika konflikter för broadcast-paket krävs ett stort contention window. Eftersom de paket som genereras av OLSR utgör en liten del av den totala trafiken i nätet bör det dock inte leda till stora problem.

Det som kan påverka kapaciteten för nyttotrafiken är mängden kontrolltrafik som OLSR genererar. Vi har som grundinställning justerat tiderna i protokollet så att OLSR skickar kontrollpaket mer sällan än enligt standard eftersom snabba länkförändringar inte behöver hanteras. Därmed minskar OLSR:s inverkan på resultaten. En följd av detta är att uppkopplingstiderna blir längre, minuter snarare än sekunder, men det bedöms inte vara något problem i de scenarier som studeras. En känslighetsanalys genomförs dock, för att se hur ökad mängd kontrolltrafik från OLSR påverkar kapaciteten.

Tabell 3.1: Simuleringsparametrar. Värden markerade i fetstil är de som används som default om inget annat anges.

	Parameter	Värde	Enhet
Radiomottagare	Centerfrekvens	1,35	GHz
	Uteffekt	5	W
	Bandbredd	5	MHz
	Dataakt	2	Mbit/s
	Antennhöjd	15	m
	Antenn-gain	3	dB
	Känslighet	-121	dBW
Nätstorlek	Antal noder	20,40	-
	Yta	100*[50 ,100]	km
	Terräng	Östergötland, Jämtland	
OLSR	Hello-interval	2,10	s
	TC-intervall	5,25	s
CSMA	aCwMin	1,3,7,...,511	-
	aAirPropagationTime	varieras per nät	s
	RTS/CTS	av,på	-
Applikation	Paketstorlek	1,12	kbit

4 Resultat

Prestandan hos CSMA mäts i huvudsak i simuleringarna i termer av vilken kapacitet för nyttotrafik som ges. Vi börjar därför med att definiera vad som avses med kapacitet i det här sammanhanget samt illustrerar hur måttet beräknas och hur spridningen i kapacitet ser ut för olika nätrealisationer. Därefter undersöks hur terräng och nätstorlek påverkar kapacitet och fördröjning. Vidare undersöks hur egenskaper hos datatrafiken påverkar resultaten. Avslutningsvis illustreras hur ett antal protokollparametrar på nätverks- och MAC-lagret inverkar på kapaciteten.

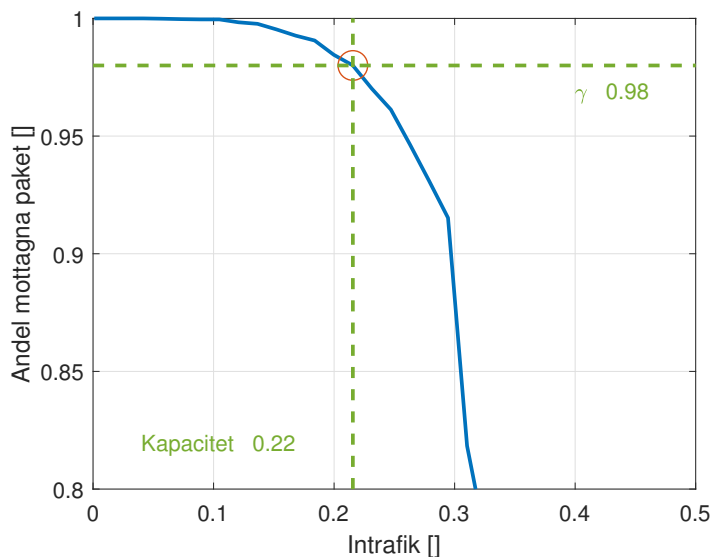
4.1 Beräkning av kapacitet

Ett mått på kapaciteten i ett nät bör spegla hur stor del av den tillgängliga bandbredden som kan utnyttjas till att skicka nyttotrafik. Vi definierar kapaciteten i nätet som den högsta intrafiklast, sett från applikationsnivå, för vilken andelen levererade paket överstiger en nivå, γ . Genomgående i simuleringarna används kravet $\gamma = 0,98$, det vill säga åtminstone 98% av alla sända paket måste komma fram för att nätet skall anses vara funktionellt. I Figur 4.1 visas hur andelen levererade paket varierar som en funktion av intrafiklasten. Intrafiklasten är normerad med den totalt tillgängliga bandbredden, den maximala kapaciteten är således 1. I det nät som visas i Figur 4.1 är kapaciteten 0,22 med kravet på 98% levererade paket. Som synes påverkar valet av η kapaciteten, dock är de trender som illustreras desamma så länge γ är större än cirka 0,95. Lägre trösklar än så är sannolikt inte relevanta för de applikationer som kan tänkas användas i backbone-nät. Vidare kan vi se att andelen mottagna paket minskar snabbt då intrafiklasten passerar den punkt då nätet blir överlastat.

Hädanefter illustreras kapaciteten i huvudsak som medelvärde av kapaciteten över de 32 nätrealiseringar som simulerats med undantag för avsnitt 4.2 som illustrerar spridningen i kapacitet mellan olika nätrealiseringar.

4.2 Nätstorlek och topologi

I det här avsnittet undersöks hur nätets storlek, topologi och terräng påverkar prestandan hos CSMA i termer av kapacitet och fördröjning. Fyra olika uppsättningar av systemparametrar undersöks och dessa konfigurationer inkluderar trafiktyp samt huruvida RTS/CTS används eller ej. Enligt IEEE 802.11 används typiskt RTS/CTS enbart för paket större än en viss storlek men i dessa simuleringar har alla paket samma storlek, därav antingen på eller av. De två trafiktyperna som undersöks är båda punkt-till-punkt, i ena fallet går all trafik från



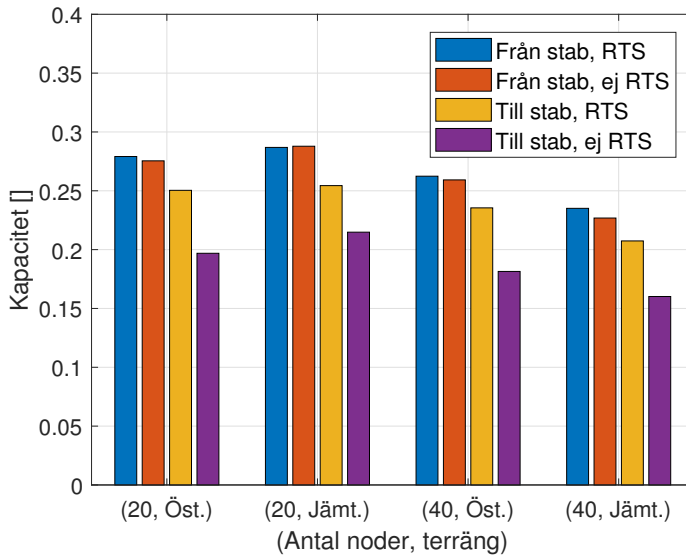
Figur 4.1: Exempel på kapacitetsberäkning för ett av de simulerade näten.

stabsplatsen ut i nätet och i det andra fallet går all trafik från nätet till stabsplatsen. I avsnitt 4.3 redovisas resultat för blandade trafiktyper, då trafik i olika proportioner går både i riktning till och i riktning från stabsplatsen.

4.2.1 Nätstorlek och terräng

Kapaciteten för fyra olika scenarior visas i Figur 4.2. De fyra scenarierna utgörs av två nätstorlekar, 20 respektive 40 noder, och två terrängprofiler, Östergötland och Jämtland. De fyra olika konfigurationerna rörande trafikriktning och RTS/CTS förhåller sig i stort sett likadant till varandra i alla fyra scenarierna. För de konfigurationer då trafiken går i riktning ut från stabsplatsen har det knappt någon påverkan på kapaciteten om RTS/CTS används eller inte. I det andra fallet, då trafiken går från nätet till stabsplatsen, är skillnaden desto större mellan att använda RTS/CTS och att inte göra det.

Vid jämförelse av de två terrängtyperna framgår att för den mindre nätstorleken har terrängtypen en marginell påverkan. Överlag är kapaciteten något högre för terrängprofil Jämtland vid den aktuella nätstorleken men skillnaden är maximalt ca 2 procentenheter. Skillnaden mellan de två terrängprofilerna är något större i det större nätet, dock är förhållandet mellan de två terrängprofilerna omvänt. Överlag är skillnaden i kapacitet 2-4 procentenheter i det stora nätet, till fördel för terrängprofil Östergötland.

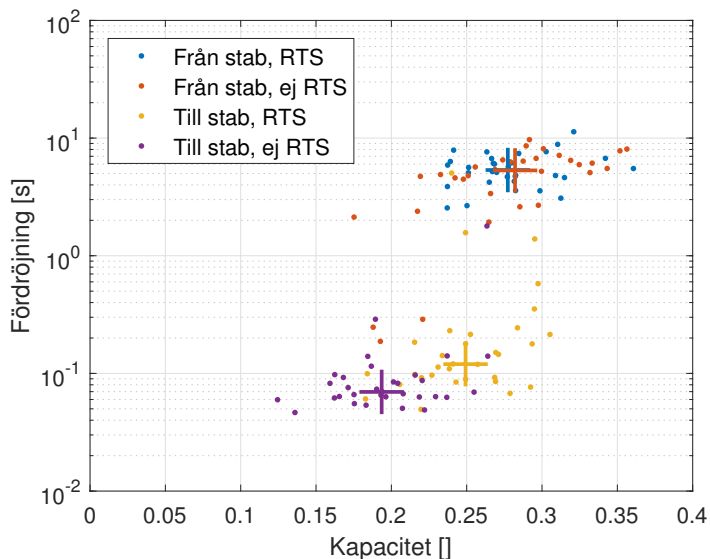


Figur 4.2: Inverkan av nätstorlek och terrängprofil.

Vid jämförelse av de två nätstorlekarna framgår att skillnaderna är relativt små, maximalt ca 2 procentenheter för Östergötland och maximalt ca 6 procentenheter för Jämtland. Sammantaget framgår att varken terrängprofil eller nätstorlek påverkar kapaciteten i någon större grad. Det bör också noteras att med tanke på de stora ytor som näten är spridda över (5x10 respektive 10x10 mil), är det svårt att hävda att terrängprofilerna är speciellt homogena för respektive område. De två terrängprofilerna bör snarare ses som två utfall av svensk terräng och ur den synvinkeln kan de små skillnaderna mellan terrängprofilerna tolkas som att de resultat som presenteras förmodligen är representativa för svensk landsbygd.

4.2.2 Spridning mellan nät

I Figur 4.3 illustreras hur kapacitet och fördröjning skiljer sig mellan olika nätrealisationer för ett givet nätskenario (20 noder, Östergötland). Resultaten illustreras med punktmoln för samma fyra konfigurationer som tidigare. För varje nätrealisation anges kapaciteten samt den genomsnittliga fördröjningen med en punkt och medianvärdet för respektive konfiguration anges med ett korstecken. Sett till fördröjningen är det skillnad mellan de två trafiktyperna. I fallet då all trafik går från nätet in till stabsplatsen är medelfördröjningen, med ett fåtal undantag, mindre än en sekund. I det andra trafikfallet är fördröjningen däremot



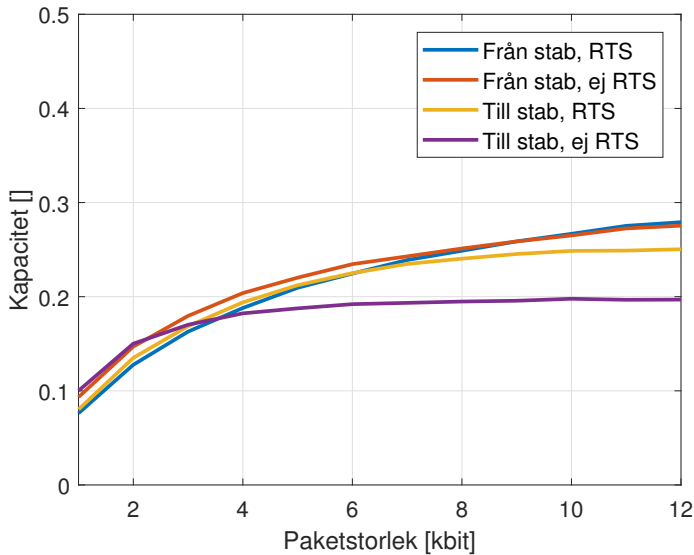
Figur 4.3: End-to-end fördröjning vid kapacitetsgräns. Punkterna visar genomsnittlig fördröjning vid kapacitetsgränsen för respektive nätrealisation. Kryssen anger medelvärde över alla realisationer.

större än 1 sekund i alla realisationer och medianvärdet är kring 6 sekunder. Eftersom fördröjningen är uträknad vid olika kapaciteter kan skillnaden mellan de två trafikriktningarna bero på att fördröjningen ökar i olika takt när trafiken närmar sig överbelastning.

Vidare framgår det av Figur 4.3 att det är en stor spridning i kapacitet mellan olika nätrealisationer. Den aktuella nättopologin har alltså en stor påverkan på vilken kapacitet som är möjlig att uppnå. Detta talar för att nätplanering i backbone-nät är av stor vikt, dock framgår inte från dessa resultat hur nätplaneringen bör genomföras för att maximera kapaciteten. Vi har undersökt om variationerna mellan olika realisationer kan förklaras i termer av medelantal hopp eller maximala länkvstånd. Båda dessa faktorer har viss påverkan men förklarar enbart en liten del av variationerna. Troligtvis är det en samverkan mellan flera faktorer, både nätmässiga och protokollmässiga, som ger de stora variationerna.

4.3 Trafikmönster

Här visar vi hur egenskaper hos datatrafiken påverkar vilken prestanda som erhålls i nätet. De egenskaper som undersöks är trafikmönstret (en sändare till olika mottagare kontra många sändare till en mottagare) samt paketstorleken.



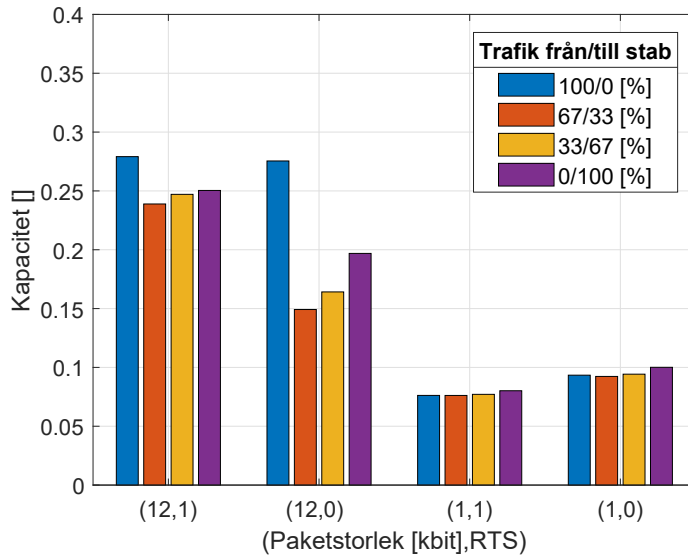
Figur 4.4: Inverkan från paketstorlek på kapacitet för nyttotrafik.

4.3.1 Paketstorlek

De resultat som presenterades i avsnitt 4.2 var baserade på paket med storleken 12 kbit, vilket motsvarar den maximala storleken för ett IP-paket. I Figur 4.4 visas hur en minskad paketstorlek inverkar på kapaciteten i nätet. Resultaten jämförs för de två trafikfallen då all trafik går antingen till eller från stabsplatsen samt huruvida RTS/CTS används eller ej. Rent generellt ger en större paketstorlek högre kapacitet upp till en viss gräns då kapaciteten planar ut. Kapaciteten minskar kraftigt då paketstorleken understiger ca 4 kbit och vid denna paketstorlek skiljer sig inte kapaciteten åt nämnvärt mellan de olika konfigurationerna. För större paketstorlekar är kapaciteten något högre i fallet då all trafik skickas i riktning från stabsplatsen.

4.3.2 Trafikriktning

I ett verkligt användningsfall är det rimligt att anta att all trafik inte går i en riktning utan att det snarare är en blandning av trafik till och från stabsplatsen. I Figur 4.5 illustreras hur kapaciteten förändras när trafikbilden går från att bestå av trafik i enbart en riktning till en blandning mellan trafik till och från stabsplatsen. Resultaten visas för paket som är 12 eller 1 kbit och om RTS/CTS används eller ej. I fallet med små paket skiljer sig inte de fyra olika trafikför-



Figur 4.5: Betydelse av trafikriktning.

delningarna sig åt nämnvärt. För stora paket visar sig dock att en blandning av trafik ger en lägre kapacitet jämfört med att all trafik går i samma riktning. Allra tydligast blir det när majoriteten av trafiken går från stabsplatsen och en mindre del av trafik går till stabsplatsen. I det fallet blir kapaciteten mycket lägre än fallet då all trafik går från stabsplatsen och även lägre än fallet då all trafik går till stabsplatsen. En trafikfördelning som innebär att en nod genererar en majoritet av trafiken, men inte all trafik, förefaller alltså leda till att bandbredden inte kan utnyttjas lika väl.

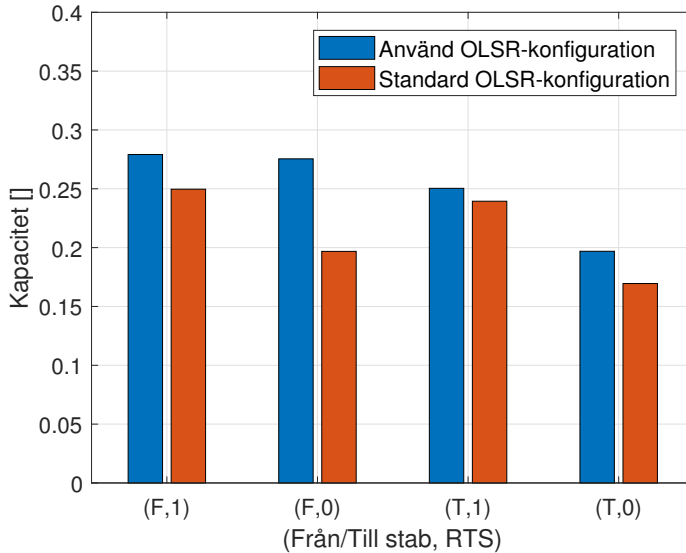
4.4 Parameterinställningar

Vi undersöker hur känsligt protokollet är för variationer i ett antal systemparametrar.

4.4.1 OLSR-parametrar

I [1] undersöktes hur väl CSMA och OLSR fungerade ihop i ett taktiskt ad hoc-nät med uteslutande broadcasttrafik. I det scenario som då undersöktes gjorde kollisioner på MAC-lagret att OLSR fungerade dåligt, vilket i sin tur ledde till ytterligare kollisioner på MAC-lagret.

För att se vilken inverkan kontrolltrafiken från OLSR har i ett backbone-

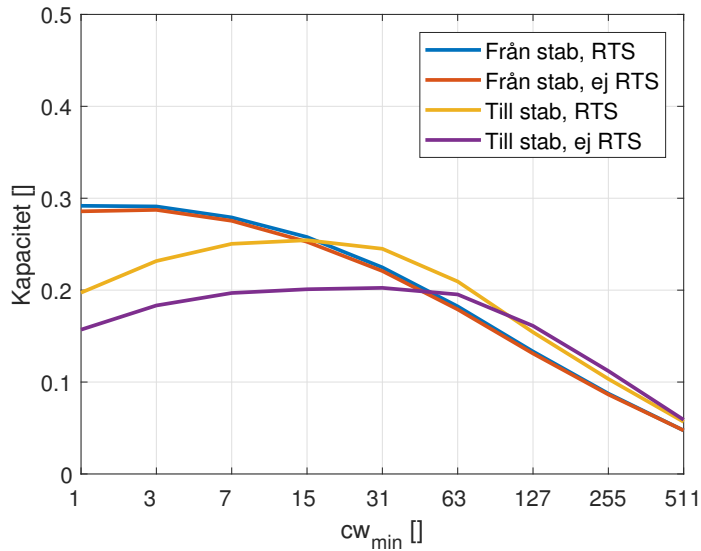


Figur 4.6: Tid mellan HELLO-meddelanden i OLSR.

scenario och vad det skulle innebära att köra med OLSR:s defaultparametrar har de två parametersättningarna jämförts. I Figur 4.6 illustreras hur kapaciteten påverkas av hur ofta OLSR sänder sina kontrollmeddelanden. De OLSR-inställningar som jämförs finns listade i Tabell 3.1. Det framgår från resultaten att kontrolltrafiken från OLSR har en viss negativ inverkan på kapaciteten, i synnerhet när trafiken går i riktning från staben. Genom att använda RTS/CTS minskar inverkan från OLSR-trafiken, förmodligen på grund av en minskad risk för kollisioner mellan datapaket och OLSR-paket. Att döma av resultaten kan en viss kapacitetsvinst erhållas genom att anpassa OLSR efter förutsättningarna i backbone-nätet men det är även möjligt att köra med defaultparametrar utan större kapacitetsförluster, åtminstone då RTS/CTS används.

4.4.2 Contention window

I CSMA används ett så kallat *contention window* för att avgöra vilken backoff en nod skall göra om kanalen är upptagen när noden försöker sända ett paket. Backoff-tiden räknas fram genom att slumpa ett antal tidluckor från intervallet $[0, CW]$ och multiplicera detta med tidluckelängden som används. Det maximala antalet tidluckor, CW , begränsas av två parametrar kallade aCW_{min} och aCW_{max} . Initialt och efter en lyckad sändning sätts CW till aCW_{min} , medan en detekterad kollision (utebliven acknowledgement) leder till att CW dubbele-



Figur 4.7: Min contention window

ras, så länge CW är mindre än aCW_{max} . Eftersom broadcasttrafik inte använder acknowledgements gäller för denna trafik att CW alltid är lika med aCW_{min} . Genom att öka aCW_{min} minskar därmed risken för kollisioner för paket som inte använder RTS/CTS, i huvudsak paket som skickas som broadcast.

I [1], där broadcast-trafik i taktiska nät med CSMA undersöktes, visade resultaten att aCW_{min} behövde ökas rejält, jämfört standardinställningar, då trafiken enbart bestod av broadcasttrafik. Som beskrivits tidigare genereras enbart unicast-trafik på applikationslagret i denna studie, dock skickas kontrolltrafiken från OLSR som broadcast.

I Figur 4.7 visas kapaciteten som en funktion av parametern CW_{min} . Från resultaten framgår att i det scenario som utvärderas i denna rapport krävs inte ett stort CW_{min} för att systemet skall fungera. Tvärtom, då CW_{min} överstiger 63 minskar kapaciteten markant i alla de undersökta fallen. Enligt 802.11-standarden är default-värdet för aCW_{min} 7, vilket ser ut att vara en bra kompromiss då det ger bra resultat för båda trafikriktningarna.

5 Slutsatser

I denna rapport studeras olika aspekter av att använda CSMA i ett semimobilt militärt backbone-nät. Denna typ av nät måste klara av att täcka stora ytor för att kunna användas till att binda ihop exempelvis en brigad. För att kunna täcka stora ytor med ett begränsat antal kommunikationsnoder krävs långa kommunikationslänkar. Detta kan åstadkommas bland annat med hjälp av nätplanering och upphöjda, riktantenner. Dessa antaganden leder till nättopologier som inkluderar länkar som är flera mil långa.

För att CSMA ska fungera i ett backbone-scenario måste väntetider i protokollet ökas rejält och detta begränsar vilken kapacitet som kan uppnås. En förutsättning för att CSMA ska fungera effektivt är att tiden det tar att bedöma om kanalen är ledig och genomföra backoff är kort i förhållande till tiden som används för att skicka datapaket. Då utbredningstiderna ökar till följd av långa kommunikationslänkar behöver datapaketerna vara stora för att kapaciteten inte ska bli minimal.

Vidare förstärks denna aspekt när datatakten på länkarna ökar. I denna rapport har en länkdatatakten på 2 Mbit/s använts medan nyare radiolänkar typiskt har stöd för högre datatakter, uppemot 16 Mbit/s. I och med att utbredningstiderna inte påverkas av datatakten krävs alltså ännu större paketstorlekar för att bibehålla nyttjandegraden av kanalen när länkdatatakten ökar, givet att länkarnas räckvidd är oförändrad.

Baserat på resultaten från simuleringarna kan typiskt 20-30 % av bandbredden utnyttjas till att skicka användartrafik när CSMA används i backbone-nät. Detta är klart bättre än i fallet då CSMA används för broadcasttrafik i taktiska nät. Det är inte troligt att kapaciteten skulle bli avsevärt högre med ett TDMA-baserat protokoll på grund av antalet hopp i nätet. Den variant av CSMA som utvärderats följer dessutom i stora drag befintlig standard, någon motsvarande industristandard för TDMA existerar inte.

Utöver paketstorlek är de två faktorer som påverkar kapaciteten mest nättopologin och trafikfördelningen i nätet. Samma nätstorlek och terräng kan ge vitt skilda resultat beroende på hur noderna placerats inom ytan. Detta antyder att nätplanering är viktigt för dessa typer av nät. Det är dock inte uppenbart från resultaten hur noder ska placeras för att optimera prestanda, då vare sig medelantal hopp i nätet eller maximala utbredningstider till fullo förklarar variationerna. Den andra faktorn som tydligt påverkar kapaciteten är hur trafikfördelningen ser ut. En praktisk följd av detta är att det vid utprovning av system som bygger på dessa tekniker är viktigt att mäta kapacitet då flera noder genererar trafik, annars finns det risk för att kapaciteten överskattas

Ett par faktorer som har stor betydelse för prestandan i taktiska ad hoc-nät

men som inte verkar ha samma betydelse i de scenarier som undersöks här är terrängtyp och antal noder. Att terrängen inte påverkar nämnvärt är en följd av att noderna placeras på höga punkter i terrängen med upphöjda antenner samt att terrängerna inte är homogena över så pass stora ytor.

Sammanfattningsvis ger CSMA bra prestanda i denna typ av nät om parametrar anpassas efter de långa räckvidderna och paketen som skickas är stora.

Referenser

- [1] A. Komulainen och U. Sterner. Analysis of CSMA broadcast performance in tactical ad hoc networks. Scientific Report FOI-R--4219--SE, FOI, Linköping, Jan 2016.
- [2] IEEE. IEEE std 802.11 - wireless LAN medium access control (MAC) and physical layer (PHY) specifications. Teknisk rapport, The Institute of Electrical and Electronics Engineers, New York, USA, 1997.
- [3] Evgeny Khorov, Andrey Lyakhov, Alexander Krotov och Andrey Guschin. A survey on IEEE 802.11ah: An enabling networking technology for smart cities. *Computer Communications*, 58(Supplement C):53 – 69, 2015. Special Issue on Networking and Communications for Smart Cities.
- [4] A. B. Flores, R. E. Guerra, E. W. Knightly, P. Ecclesine och S. Pandey. IEEE 802.11af: a standard for TV white space spectrum sharing. *IEEE Communications Magazine*, 51(10):92–100, Okt 2013.
- [5] A. Sheth, S. Nedeveschi, R. Patra, S. Surana, E. Brewer och L. Subramanian. Packet loss characterization in WiFi-based long distance networks. I: *IEEE INFOCOM 2007 - 26th IEEE International Conference on Computer Communications*, ss 312–320, May 2007.
- [6] M. Tanaka, D. Umehara, M. Morikura, N. Otsuki och T. Sugiyama. New throughput analysis of long-distance IEEE 802.11 wireless communication system for smart grid. I: *2011 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, ss 90–95, Okt 2011.
- [7] J. Simo Reigadas, A. Martinez-Fernandez, J. Ramos-Lopez och J. Seoane-Pascual. Modeling and optimizing IEEE 802.11 DCF for long-distance links. *IEEE Transactions on Mobile Computing*, 9(6):881–896, Jun 2010.
- [8] S. Örn Tengstrand och U. Sterner. Räckvidder för radiolänkar till upphöjd nod. Scientific Report FOI-R--3951--SE, FOI, Linköping, Okt 2014.
- [9] Ulrik Nylander. Slutrapport yttäckande samband. Teknisk rapport 15FMV1402-51:1, FMV AL Led/integration, Aug 2016.

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
164 90 Stockholm

Tel: 08-55 50 30 00
Fax: 08-55 50 31 00

www.foi.se