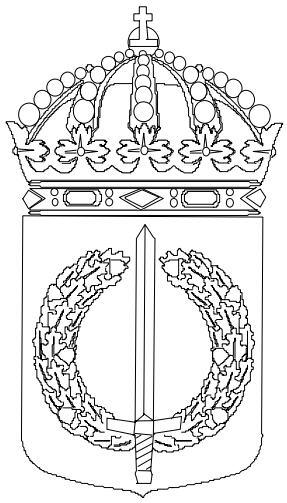


FÖRSVARSHÖGSKOLAN

C-UPPSATS

Författare	*Förband*	*Kurs*
Mj Tore Reinhold	Amf 4	ChP T 00-02
FHS handledare		
Prof Anders Lundberg		
Uppdragsgivare	*Ämnets beteckning*	
FHS MTI	19 100:2056	

AD HOC-NÄT – NÅGOT FÖR MOBILA ENHETER I NBF?

SAMMANDRAG

Ett syfte med nätverksbaserat försvar är att erhålla snabbare reaktionstider i ledningssystem. Ad hoc-näten utgör en framtida möjlighet att erbjuda taktiskt rörliga enheter uppkoppling i nätverk även under förflyttning. Det kan på sikt inkludera de funktioner som har krav på liten fördröjning i uppkopplingarna. Exempel på en sådan funktion är sensorintegration genom sensornät. Ett av problemen i ad hoc-nätverksutvecklingen ligger i att de dataprotokoll som ska utnyttjas för att erbjuda en kompabilitet mot den fasta nätstrukturen, inte har den funktionsduglighet som krävs i ett ad hoc-nät. För att ge snabb överföring krävs en utvecklad variant av de nätverksprotokoll (TCP/IP) som hanterar uppkomna fel på förbindelsen. Detta är avgörande för ad hoc-nätverkens funktionsduglighet. Det skulle resultera i minskade fördröjningar och därmed ökad kapacitet. Mycket talar för att snabbheten kommer att bli så stor att multisensordatafusion kan realiseras i ad hoc-nät.

Nyckelord: ad hoc-nätverk, sensorintegration, protokoll

INNEHÅLL:

Inledning **4**

Bakgrund *4*

Syfte *6*

Problemformulering *6*

Uppsatsens struktur *7*

Underlag *7*

1 Krav på informationsöverföring i nätverk **8**

1.1 Stridens krav *8*

1.2 Acceptabel fördröjning *9*

2 Fördröjning i nätverk **11**

2.1 Nätarkitektur *11*

2.2 Förmedlingsprinciper *12*

2.3 Metoder för att skicka data i nätverk *13*

2.4 Kanaldelning *14*

2.5 Routing-principer *15*

2.6 Databaser *15*

2.7 Protokoll *16*

2.8 Resulterande fördröjning *18*

3 Ad hoc-nätens möjligheter **20**

3.1 Bakgrund *20*

3.2 Utveckling av ad hoc-nätverksteknologin *20*

3.2.1 Nät med och utan hierarki 20

3.2.2 Ad hoc-nätets arkitektur 21

3.2.3 Protokollutmaningen i AHN 21

3.2.4 QoS 24

3.2.5 Standarder för ad hoc-nät 25

3.2.6 Ad hoc-nätverk i praktiken 26

3.2.7 Trender kring begreppet AHN 27

3.3 AHN och tidskraven *27*

4 Sensorintegration i ad hoc-nät 29

4.1 Bakgrund 29

4.2 Källan till måldata: sensorer 29

4.2.1 Sensorstyrning 29

4.2.2 Bearbetning av sensordata 29

4.2.3 Informationsfusionering 30

4.3 Sensorintegration 30

4.3.1 Datafusion 30

4.3.2 Trender inom ”sensor-networking” 31

4.3.3 Multisensordatafusion 31

4.4 AHN – ett led i sensorintegrationen 33

5 Sammanfattning 34

Avslutning 37

Referenser 38

Tryckta källor 38

Övriga källor 38

Figurförteckning 39

Bilagor:

Bilaga 1 Förkortningsförteckning

Bilaga 2 Genomförda intervjuer och samtal

Inledning

Bakgrund

Nätverksbaserat försvar

Teknikutvecklingen inom telekommunikation och databehandling har resulterat i att nya former av nätverkslösningar blir möjliga, där olika enheter kan samverka med varandra på nya sätt. Detta är grunden för nätverkscentrisk krigföring, som internationellt kallas *Network Centric Warfare* (NCW)[1]. För svenskt vidkommande har detta omsatts till konceptet *Nätverksbaserat Försvar* (NBF). I det sammanhanget är det intressant att belysa hur rörliga enheter kan vara delar i ett nätverk och bilda egna mobila nätverk oberoende av uppgift, taktiskt läge eller rumslig placering. Rörliga enheter har inte hittills ständigt kunnat vara en del av nätverken, i och med att deras mobilitet medför att förbindelserna kopplas ner emellanåt. Det är i dessa situationer som självupprättande mobila nätverk kan komma att fylla en funktion, eftersom de kan erbjuda nätverkslösningar ad hoc – därav termen ”ad hoc-nätverk”. *Det självupprättande mobila nätverket skall tillse att noderna ständigt kan vara nätverksanslutna. En förutsättning för diskussionen i uppsatsen är därför att självupprättande mobila nätverk eftersöks inom NBF-konceptet.*

Ad hoc

Det latinska uttrycket ad hoc betyder ”för detta”. I nätverkssammanhanget anger det företrädelsevis att något är improviserat. Det skall tolkas som att ett *ad hoc-nät* är ett nät som förändras kontinuerligt, anpassas till terrängen och situationen, m.a.o. att det förändras ”för detta” ändamål. Ett Ad hoc-nät[2] består enbart av mobila delar utan att det behövs någon central enhet, d.v.s. det krävs inga basstationer. I den nätverksbaserade striden kan ad hoc-nät användas där inte infrastruktur finns eller där radionät ständigt behöver vara etablerade p.g.a. den taktiska situationen. *Utmaningen med ad hoc-nät består i att nätets struktur ändras kontinuerligt då enheterna rör sig vilket leder till avbrott på förbindelser. Informationen måste därför automatiskt kunna finna nya vägar i nätet då avbrott uppstår.* Fortsättningsvis kommer förkortningen *AHN* att användas för ”Ad Hoc-Nätverk”.

Nätverkets lägesuppföljning

I ett nätverksbaserat ledningssystem med en mängd aktiva eller passiva sensorer i olika våglängdsområden uppstår behovet av att kunna jämföra data från olika sensorsystem. Rådata från sensorer kan förädlas och erhåller därmed en kvalitetsmässigt högre nivå. Förädlingen bygger i stort på en jämförelse av information från olika sensorer. Denna jämförelse syftar till att öka säkerheten i lägesangivningen och klassificeringen av målet och därmed höja det totala värdet av måll ägesinformationen. Jämförelsen skall kunna genomföras inte bara på en plattform med flera sensorer utan även som en automatiserad process i det nätverksbaserade

[1] Alberts S, Garstka J, Stein F, *Network Centric Warfare*, Library of Congress Cataloging-in-Publication Data, 1999, s 2
[2] Persson K, *TCP/IP i taktiska ad hoc-nät*, Teknisk rapport, Totalförsvarets Forskningsinstitut, 2002, s 11

ledningssystemet. Detta syftar bland annat till att skapa ett underlag för en så kallad *gemensam mållägesbild* för aktörerna i ledningssystemet.

Realtid – acceptabel fördröjning
I datorsammanhang används begreppet realtid eller som också sägs ibland ”nära realtid”, vilket innebär att datasystemet kontrollerar en pågående process och bearbetar data tillräckligt snabbt, för att i tid avge nödvändiga resultat.[3] I denna uppsats kommer begreppet realtid eller nära realtid att undvikas – istället riktas del av resonemanget in mot vilka omständigheter som orsakar tidsförluster. Skälet till detta är att det bedöms som väsentligare att ha en uppfattning om var, i vilka system, och när, i vilka typsituationer som en *fördröjning* uppstår.

Sensorintegration
Nyttan av sensorer, i syfte att skapa en bild av stridsfältet, ökar i takt med den tekniska utvecklingen. Främst rör det den utveckling som lett till större rörlighet hos de stridande enheterna vilket i sin tur ökat fragmentiseringen av stridsfältet. Morgondagens förbandsenheter är allsidigt sammansatta, flexibla och uppträder med stor manöverförmåga på stort djup. Förbanden i den nätverksbaserade striden kommer att uppträda dygnet runt och verka med högt tempo och stor eldkraft. Det medför krav på att tiden från upptäckt till bekämpning förkortas. – särskilt om man strävar efter att komma ”innanför motståndarens beslutscykel”.[4] Sensorn är den första länken i underrättelsekedjan. Sensorutvecklingen går mot allt bättre prestanda genom multifunktionssystem och miniatyrisering, vilket medger en ökad förmåga att verka oberoende av tidpunkt och väder.[5] Sensorplatformar kan integreras i nätverk och man kan nå vidare till en *multisensordatafusion*. Denna fusion har hittills kunnat genomföras inom en plattform med sensorer i olika våglängdsområden. *Sensorintegrationen* kan också utföras med sensorer på olika plattformar, men hittills har detta enbart utförts på forskningsnivå. En utmaning består i att kunna utföra sensorintegration i ad hoc-nätverk.

Mobila nätverksuppkopplingar
Sensorernas måldata skall kunna utnyttjas för de vapenplattformar som är aktörer i nätverket. De fasta nätverkslösningar som NBF bygger på är i huvudsak baserade på kommersiell teknologi som knyts till Internet. En fråga är om nuvarande nätverkslösningar svarar mot de krav som rör *acceptabel fördröjning och säkerhet*, eller om modifikationer av dessa lösningar behövs för att säkerställa snabbhet och tillförlitlighet i de mobila nätverken? Nuvarande lösningar grundar sig på krav och specifikationer för stationära nät, men frågan är om de också kan appliceras på *militära mobila nätverk, med krav på snabba, tillfälliga men tillförlitliga uppkopplingar*. Sådana uppkopplingar kan exempelvis vara de mellan sensorer i s.k. sensornätverk. En nätverksteknologi som i framtiden kan komma att erbjuda dessa tillfälliga mobila uppkopplingar är AHN.

---

[3] En definition på realtid och realtidssystem är: det faktiska tidsförloppet då en process pågår. Begreppet har sitt ursprung i engelskans *real time*, Nationalencyklopedin (NE)
[4] Den egna tiden för OODA-loopen (Observation, Orientation, Decision, Act) i förhållande till motståndarens tid från observation, orientering till beslut och handling.
[5] *Tekniska utvecklingstrender*, Försvarets Materielverk, 2001, s 120

Protokoll
Som en grund för vårt resonemang kring AHN ska vi titta närmare på de protokollsystem[6] som de flesta maskinvaru- och programvaruplattformar använder idag och som också utgör stommen i Internet. Information som sänds över ett nät måste behandlas och tolkas. Idag används ett antal olika protokoll som tar hand om data för att dels få fram den information man är ute efter, dels få informationen dit man vill. Man kan jämföra *protokollen* med *en samling regler för hur data ska tas om hand*. Protokollen har olika ansvarsområden och egenskaper, t.ex. adressering och kodning. Två av de vanligaste protokollen är *Transmission Control Protocol* (TCP) och *Internet Protocol* (IP). (se kap. 2.7)

Syfte

Uppsatsen är skriven med syftet att översiktligt beskriva ad hoc-nätverksteknologin som den ser ut idag och åt vilket håll utvecklingen går, särskilt med tanke på AHN-teknikens möjligheter. Läsaren antas känna till sådana begrepp som bandbredd, kanalkapacitet, sensorintegration etc. En tänkt målgrupp består av de som ska fatta beslut om inriktningen av forskning och utveckling på nätverksområdet.

Problemformulering

Det nätverksbaserade försvaret bygger på TCP/IP-baserade protokoll med sina begränsningar i att skapa uppkopplingar med konstant tidsfördröjning i nätverk. Den framtida ad hoc-nättekniken erbjuder nya möjligheter för mobilitet genom sina självkonfigurerande mobila nätverkslösningar. Det syftar till att åstadkomma en bättre tillgänglighet i nätverken för de deltagande enheterna. Frågan är om AHN kommer att kunna svara mot de behov och krav som den nätverksbaserade striden ställer på tillfälliga mobila uppkopplingar. Det kan också röra sig om nya sätt att nå sensorintegration. Det skulle kunna innebära att mobila sensorer kan integreras på nya sätt. Uppsatsens tidsperspektiv sträcker sig från vad dagens nätverksteknik erbjuder till dess att de ad hoc-tekniker som nu finns på forskningsnivå kan komma att finnas vid förband, uppskattningsvis 2007-2010. Uppsatsens problemområde handlar i grunden om huruvida det finns möjligheter att med framtida ad hoc-nätverk skapa tillräckligt snabba och säkra uppkopplingar i nätverken. Detta mynnar ut i följande tre huvudfrågor:

- Vilka krav på nätverk måste ställas för att ge erforderliga förbindelser mellan rörliga enheter?

- De fasta nätverkens protokoll skapar okontrollerbara fördröjningar när de utnyttjas i mobila radionätverk. Kan ad hoc-nät erbjuda en lösning på problemet?

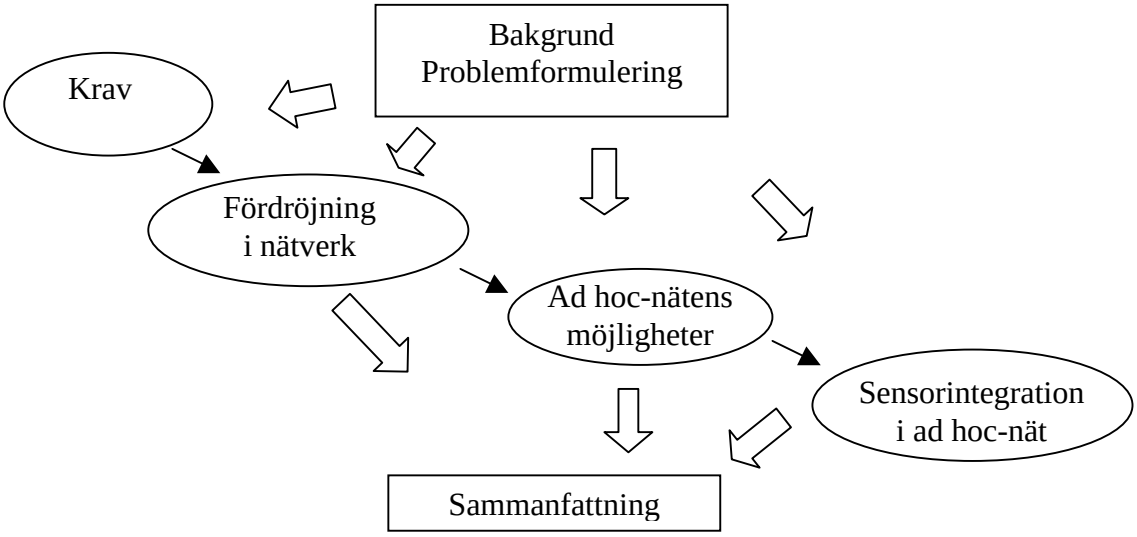
- Kan ad hoc-nätverken erbjuda vägar för sensorintegration med tillräcklig kapacitet och snabbhet?

[6] Protokoll eller kommunikationsprotokoll**,** en uppsättning regler för kommunikation mellan olika enheter i ett datorbaserat kommunikationssystem. Reglerna gäller t.ex. felövervakning, sekvenskontroll, start- och avslutningsprocedurer, NE

Uppsatsens struktur

I kapitel 1, *Krav på informationsöverföring i nätverk*, förs ett resonemang kring krav på snabbhet i nätverk. I kapitel 2, *Fördröjning i nätverk*, diskuteras hur tidsförluster uppkommer i nätverk. I kapitel 3 redovisas *Ad hoc-nätens möjligheter*. Kapitlet utmynnar i frågan om AHN kan erbjuda en lösning på fördröjningsproblematiken. I det fjärde kapitlet, *Sensorintegration i ad hoc-nät*, förs diskussionen vidare mot frågan om vilka möjligheter AHN kan ge vad gäller sensordatafusion.

De olika kraven och möjligheterna från kapitlen sammanfattas i det femte kapitlet. Resonemanget fokuseras på de sammanvägda krav som bör kunna ställas på överföring av information i AHN. Uppsatsens struktur åskådliggörs i figur 1.



Figur 1 Uppsatsens struktur

Underlag

Den bakgrund som tecknas är i mångt och mycket baserad på de robusta kurser inom informationssystem och sambandsystem som Totalförsvarets Forsknings Institut (FOI) genomfört för ChP T ledning/telekrig. I övrigt har litteratur använts för att teckna de olika hot som finns mot den nätverksbaserade striden. För att nå ett större djup inom specifika teknikområden och för att kunna föra ett resonemang kring frågorna, har även tekniska rapporter från FOI använts. För att besvara frågeställningarna har rapporter och studier från FOI, Försvarsmakten och Försvarets Materielverk (FMV) samt den tekniska syntes som Chefsprogrammets Tekniska kurs 00-02 vid Försvarshögskolan (FHS) genomförde under 2001 använts som underlag. För att få kunskap om de senaste trenderna inom de olika teknikområden som rör AHN, genomförde jag intervjuer och samtal med representanter för FOI, industri, Försvarsmakten och FMV. Dessa intervjuer finns redovisade i bilaga 2 och refereras till genom fotnoter.

1 Krav på informationsöverföring i nätverk

I detta kapitel behandlas i korthet de krav på informationsöverföring i nätverk som är nödvändiga för genomförande av strid, i synnerhet vid snabba stridsförlopp med mobila enheter.

1.1 Stridens krav

Chefer i strid har oavsett nivå två huvuduppgifter. Den första är att tidigt fastställa målbilden för verksamheten. För att utöva ledning erfordras en sammanställd *gemensam lägesbild* tillgänglig, detta är en huvudpunkt i den nätverksorganiserade striden. Chefen skall också genom personlig närvaro på stridsfältet följa utvecklingen och undanröja de hinder som upptäcks, främst genom att samordna resurser, vilket därmed är den andra huvuduppgiften. Chefens placering på fältet är främst beroende på vilken lägesuppfattning som finns presenterad. Inom ett nätverk är det möjligt att erhålla många stridsfältsintryck, genom de olika *informationskanaler* som finns *tillgängliga* i ledningssystemet. Då kan det handla om allt från sensordata som fusionerats till att video presenteras för chefen. Båda dessa huvuduppgifter ställer grundläggande krav på att informationen som presenteras är *aktuell, korrekt och tillgänglig*.

Beslutsfattare som är sammankopplade med verkanssystem och sensorer får därigenom bättre och snabbare beslutsunderlag för insats. Det leder till bättre förutsättningar för att sätta in *rätt verkan*, på *rätt plats* och i *rätt tid* d.v.s. för att "komma innanför motståndarens beslutscykel"[7], vilket är ett av målen för NBF. Tillräckligt korta reaktionstider är en förutsättning för att detta ska lyckas.

Ledningssystemen är en väsentlig del i den nätverksorganiserade striden. De skall kunna designas och fungera i en klassisk högintensiv konflikt och erbjuda en ändamålsenlig funktion i andra lägre krisnivåer. *Nätverket skall kunna stå emot påverkan* i hela ledningskedjan från underrättelseinhämtningen till bekämpningen. Kommunikationen i nätverken kan drabbas av yttre *störning* och datornätverken kan utsättas för *intrång*, vilket kan utgöra allvarliga hot mot nätverkstriden.

Tekniskt har NBF blivit möjlig genom att datorerna integrerats inom Internet samt genom datorernas roll som medier för presentation och interaktion. Den drivande faktorn är utvecklingen av datorerna med sina processorer som hittills medgett en kapacitetsökning inom kommunikationsområdet enligt Moores lag.[8]

En motståndare kan möta det nätverksbaserade försvaret med asymmetriska medel, som exempelvis intrångsförsök. Det finns därför tydliga krav på att *intrångsskydd* behövs i NBF. Kryptering används för att ge skydd, det kan ske på olika sätt. Men man kan alltid nå erforderlig säkerhet på en förbindelse om man tar tillräckligt lång tid på sig. För att inte erhålla för stor tidsförlust på förbin-

[7] OODA loopen, se not nr 4

[8] Beträffande teknikutvecklingen refererar man sedan 1965 till Moores lag: var 18:e månad fördubblas kapaciteten och halveras kostnaden för en given integrerad krets, Jönsson L m fl, *Informationsfusion i den taktiska underrättelseprocessen*, Försvarets Forskningsanstalt, Linköping, 1998, s 118

delsen är det troligt att överlagringskrypto används för att skydda informationen. Nätverkens kommunikationslösningar måste även kunna begränsa störning.

En förutsättning för NBF är att den taktiska kommunikationen är *sömlös*. Det innebär att användarna, trots de dynamiska förändringarna i kommunikationsnäten, har tillgång till de ledningssystemtjänster de behöver. Frågan är om NBF genom tekniken bakom Internet – TCP/IP – har den potential som krävs för att kunna uppfylla dessa krav. En nackdel är att TCP/IP-protokollen utvecklats för fasta nät med hög kapacitet. Det har medfört att det saknas funktioner för att garantera kvaliteten på dataöverföring i mobila nätverk.

1.2 Acceptabel fördröjning

För att ett nätverk ska ge ett tillfredsställande stöd för en strid krävs sålunda att informationsöverföringen i nätverket är tillräckligt *snabb*, ha tillräcklig *intern säkerhet* och goda *störningsskydd*.

Snabbheten beror på såväl hårdvara som programvara. Den kan anges i form av fördröjningen, d.v.s. tiden från en signals källa (t.ex. en sensor) till dess adressat (t.ex. styrorganen i en robot).

Den interna säkerheten, vilken bl.a. kräver korrigering av bitfel och andra fel, ger också upphov till fördröjning. Likaså kan störningar, och skydd mot sådana, uttryckas i form av fördröjningar, t.ex. genom behov av redundans och genom den tidsförlust som förorsakas av frekvenshopp.

De olika kraven på informationsöverföringen kan därför sammanfattas som *största acceptabla fördröjningen*. Denna tid är självfallet olika i olika moment av strid och stridsledning. Särskilt stort torde kravet på snabbhet vara i slutskedet av ett anfall. Med följande enkla räkneexempel kan vi få en grov uppfattning om storleksordningen av den fördröjning som kan accepteras i en sådan situation.

Vi betraktar en robot (rb) som avfyrats för att bekämpa ett anfallande flygplan (fpl). För enkelhetens skull antar vi att rb styrts in på samma rätlinjiga bana längs vilken fpl rör sig, men i riktning rakt emot fpl. Från senaste tillgängliga sensordata har tid och plats för träffen räknats fram. Vidare antar vi att fpl har medel att detektera rb och har inbyggda mekanismer för att göra lämpliga undanmanövrer.

Vid tiden t före beräknad träff inleder fpl en undanmanöver. Den består i en acceleration av storleken a vinkelrätt mot banan. Om t är så kort att rb inte hinner reagera på undanmanövern, kommer fpl att befinna sig på avståndet s från den predikterade träffpunkten då rb når denna. Det avståndet ges av formeln

$$s = \frac{at^2}{2}.$$

För enkelhetens skull antar vi att krevaden äger rum i den predikterade träffpunkten. Antag att fpl klarar sig utan skador om $s = 100m$. Antag vidare att piloten tål en acceleration av ca $8g$. Det betyder att $a \approx 80m/s^2$. Därav erhålls $t \approx 1{,}6s$.

Exemplet är extremt, men inte helt orealistiskt. Det leder till att roboten inte har möjlighet att bekämpa fpl om det tar mer än 1-2 *s* för roboten att få data om undanmanövern. Befinner sig sensorn inte i rb utan, utan förmedlas data till rb via ett nätverk, finner vi att *en fördröjning i nätverket på mer än 1-2 s inte är acceptabel i bekämpningens slutskede*.

Detta är detta krav på nätverket som minst bör ställas i en situation där kraven på prestanda är som allra störst. Är det möjligt att konstruera nätverk med sådana prestanda? Det är den frågan vi ska försöka besvara i de följande tre kapitlen.

2 Fördröjning i nätverk

I detta kapitel går vi igenom de viktigaste principer och processer i ett nätverk som orsakar fördröjning. Kapitlet mynnar ut i en lista på *fördröjningsfaktorer* i ett nätverk och en kort diskussion av hur stora fördröjningar de kan åstadkomma.

2.1 Nätarkitektur

I nätverket utgör de olika deltagande enheterna och plattformarna noder. Kommunikationssystemen vid varje nod bildar *länkar* i nätet till andra noder. En nod är därmed en del i ett nätverk[9] och har hittills i fasta nätverk kunnat uppträda semiautonomt. Det innebär att en nod både kan uppträda i nätverket och självständigt. Nodens datorsystem är därmed inte beroende av ett ständigt fungerande nätverk. Det har gett en flexibilitet för rörliga enheter att kunna vara en del i de fasta nätverken när de har grupperat. Det har dock medfört att noden inte kunnat vara en del av nätverket fullt ut under rörelse, vilket resulterat i låg tillgänglighet och tillförlitlighet.

Ett resultat av informationsteknikutvecklingen är att nya former av nätverkslösningar kan realiseras. Detta skapar basen för den nätverksbaserade striden. Det resulterar i informationsnätverk som utgörs av sammanbundna noder, vilka kan utbyta information med hjälp av olika typer av kommunikationsnät. En nod kan utgöras av allt ifrån exempelvis en soldat med vapen till sensorer och vapen på olika typer av plattformar.[10] Notera att informationen i nätverket inte behöver vara knuten till någon specifik nod utan finnas tillgänglig för dem som behöver den.

Den fasta nätverksstrukturen utgör stommen i ett nätverksbaserat försvar ner till den taktiska nivån. På den taktiska nivån och nedåt finns behov av mobila nätverkslösningar. Men först en bakgrund kring den generella nätverkssstrukturen med tonvikt på de tekniker och lösningar som utgör kopplingar mot mobila enheter.

Stommen i nätverksvärlden är *Wide Area Network* (WAN), vilket är ett datornätverk som kan sträcka sig över ett land, en kontinent eller hela världen. Ett bra exempel på ett gigantiskt WAN är Internet, i vilket även många *Lokal Area Network* (LAN) ingår.

Det lokala nätverket kan konfigureras på sätt som svarar mot användarnas behov. Ett exempel på detta är *Virtuella LAN* (VLAN). Med virtuell menas att man åstadkommer separata nätverk genom konfigurering och erhåller därmed en segmenterad nätstruktur. Fysiskt är det fortfarande ett LAN men användarna uppfattar det som om de har varsitt LAN.[11]

Detta är en teknik som kan omsättas till hur nätverk i ett nätverksbaserat försvar kan konfigureras. Man kan tänka sig olika virtuella nättyper för användarna, som allt ifrån logistik och stridsledning till sensordatanät. Virtuella LAN är ett sätt att öka prestanda och säkerhet i nätverk. Det nätverksbaserade försvaret borde ha en

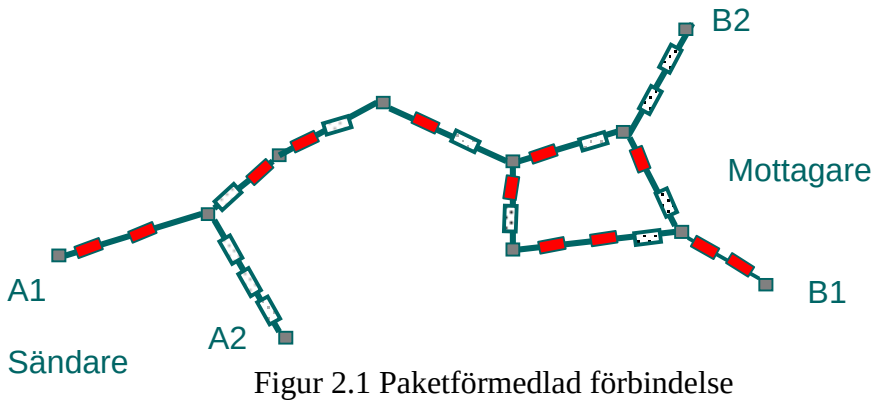
[9] Hellman A, *Att förstå Telekommunikation*, Ericsson Telecom, Telia studentlitteratur, 1996, s 22
[10] *FM idé och målbild*, rapport 5, Försvarsmakten
[11] Zettersten, KTH, föreläsning, Datakommunikation, 2000-11-15

väl utvecklad VLAN-struktur för att kunna hantera olika typer av datatrafik och därmed även kunna förenkla prioriteringar. Förenklas prioriteringarna ökas kapaciteten och tidsförlusterna blir därmed mindre.

2.2 Förmedlingsprinciper

För att två noder i ett nät ska kunna skicka information mellan varandra behövs någon form av princip för att upprätta en förbindelse. Principerna som finns innebär stora skillnader för vilka tidsmässiga garantier som erhålls. Skillnaderna i resurstilldelning beror främst på hur snabbt kommunikationsbehoven förändras.

Paketförmedlat nät
Vid paketförmedling bestämmer nätet i varje tidsögonblick vilken väg trafiken ska ta. Det paketförmedlande nätet skickar data uppdelat i paket, där varje paket har en adress som talar om vart det ska och har information om vilken nod som skickade den, men inte hur den ska ta sig dit. Data skickas i nätet enligt principen lagra och skicka vidare. Nätets resurser delas dynamiskt (dynamisk tilldelning beskrivs i 2.4 Access) av alla som använder nätet, vilket syftar till att nätet skall utnyttjas optimalt. Vägen som paketen tar i nätet är inte bestämd utan kan variera med tiden. Detta beror på att varje nod väljer väg i nätet för paket som kommer in (kallas även routing vilket beskrivs närmare i avsnitt 2.5).



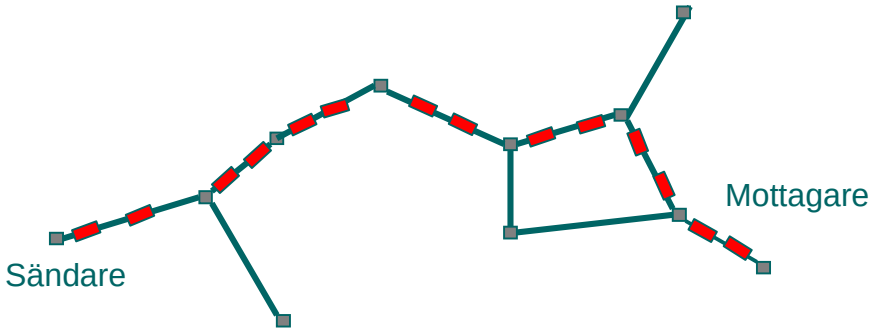
Figur 2.1 Paketförmedlad förbindelse

Det finns många sätt att välja väg i ett nät, se figur 2.1. Man kan välj väg enligt principen:

- Kortaste väg, dvs. minst antal hopp. Det förutsätter att man känner till hur hela nätet ser ut.
- Snabbaste väg i nätet. Det förutsätter att man känner till hur hela nätet ser ut samt vilka noder som har hög belastning.
- Skicka vidare fortast möjligt åt något håll som inte är samma som paketet kom ifrån.
- Skicka paketet i ungefärligt korrekta riktningen.

I det paketförmedlade nätet är det svårt att ge garantier för överföringshastigheter. Ett pakets tid från en viss nod till en annan kan variera beroende på nätets belastning och tillstånd i övrigt.

Kretskopplat nät
Kretskopplade nät förmedlar inga data förrän nätet har etablerat en väg till mottagaren. Vägen står uppställd under hela överföringen, se figur 2.2. Kretskopplingen kräver ofta att det finns en central nod med kunskap om hela nätbilden. Den centrala noden är en del i en kontrollhierarki.



Figur 2.2 Kretskopplad förbindelse

I den kretskopplade förbindelsen kommer data i samma ordning som de skickas. Mottagaren lägger ihop paketen i den ordning de kommer och kan på det sättet återskapa det sända.

För kretskopplad överföring gäller allmänt att när man har fått access till kanalen så disponerar man den så länge man använder den. När förbindelsen är etablerad, varierar inte överföringstiden som den kan göra vid paketförmedling, utan en viss maximifördröjning kan garanteras. Men själva uppkopplingen kan ta avsevärd tid. Vid hög belastning blir det *blockering* i nätet. (Så fungerar exempelvis GSM.)[12]

En fråga är hur man kan beräkna kapaciteten i ett paketförmedlat nätverk. Det är svårt när det rör sig om komplexa nätverk. Det går att komma en bit med matematiska beräkningar, därefter måste det till erfarenhet. En tumregel är att belastningen i ett nätverk eller en förbindelse inte skall vara högre än 80%. När denna belastning uppnås är det dags att uppgradera. Det är flaskhalsarna i nätet som måste identifieras. När en flaskhals identifierats och bytts ut skapar man därefter förutsättningar för nästa flaskhals.[13]

Som synes har var och en av förmedlingsprinciperna både för- och nackdelar. I mobila nätverk är paketförmedling vanligen att föredra, eftersom kanalbandbredden är mer begränsad än i ett fast nätverk och ett bättre utnyttjande av kanalen krävs.

2.3 Metoder för att skicka data i nätverk

Det finns tre metoder för att skicka data i ett nätverk, de kan karaktäriseras enligt följande:

- *Unicast*: en avsändare skickar till en mottagare.
- *Broadcast*: en avsändare skickar till alla.
- *Multicast*: en avsändare skickar till flera mottagare.

[12] Hansson A, FOI, föreläsning Kommunikationsnät, 2001-04
[13] Tummala M, McEachen J, NPS, föreläsning Advances in High Speed Networking, 2001-05

Dessa olika trafiktyper hanteras i *switchar*. En switch fungerar som en växel. När en switch får ett datapaket adresserat till en mottagare, kontrolleras först vilken port som är aktuell för mottagaren, varefter paketet skickas dit. Om switchen inte känner till adressen, skickas datapaketet till alla portarna. Detta är principen för unicast. Om en switch får ett datapaket som är av typen broadcast skickas en kopia ut på varje port, eftersom det är avsett för alla stationer som är anslutna till switchen.[14]

Adresseringsmetoden multicast används bland annat för multimediaapplikationer som video. Ett problem är att en switch hanterar multicastpaket på samma sätt som broadcast, dvs. de skickas ut på alla portar, oavsett om det finns någon station på den porten som vill se videoströmmen. Eftersom videoströmmar ofta kan kräva upp till flera Mbps bandbredd kan en mottagare som tar emot en videoström kraftigt försämra prestanda för alla på nätverket. Detta kan medföra stora tidsförluster, inte minst inom ett nätverk med mobila radiokanaler.

För att lösa det problemet kan man använda sig av VLAN. Det innebär att videoströmmen begränsas till det VLAN som vill ta emot multicast. Fortfarande kommer dock alla i samma VLAN att drabbas av prestandaförsämring. Videoströmmen kan istället enbart skickas ut på de portar som har en intresserad mottagare. *Group Membership Protocol* (GMP), som är ett protokoll som åstadkommer detta. När en mottagare anmäler sig hos videoservern för att ta emot video kommer GMP ihåg på vilken port multicastadressen sitter.[15] Detta medför att olika typer av datatrafik kan styras direkt till de delarna i nätverket de skall till. Detta medför vinster för det totala utbytet av information över nätverket. Ett nätverk inom NBF bör därför ha denna utvecklade multicast-förmåga för att undvika fördröjningar i och med att variationerna i olika datatyper är stor, allt från tal och målinformation till lägesbilder och video.

2.4 Kanaldelning

När flera användare ska skicka information i samma *kanal* i ett nät krävs en metod för att låta användarna dela på den begränsade resursen. Man säger att det råder *multiple access* när flera användare får tillgång till en sådan gemensam resurs.

Användaren av en förbindelse behöver inte resursen hela tiden. Det resulterar i att *trafiken uppträder sporadiskt.* Man brukar säga att trafiken kommer i form av ”*skurar*” eller ”*meddelanden*”. Kanaldelning används därför för att ge användarna ett bättre utnyttjande av kanalens kapacitet. Vid hög belastning finns dock en risk för överlast och köbildning med fördröjningar som följd.

Avsändarna i ett nät använder accessalgoritmer för att bestämma när de skall sända trafik i nätet. Det finns två grundprinciper för kanaldelning eller *access*; *fast tilldelning* och *dynamisk tilldelning*. I system med fast tilldelning delas den gemensamma kanalresursen upp i ett antal kanaler. En fast tilldelning innebär en låg medelfördröjning vid låg intensitet. Vid hög intensitet står få kanaler oanvända vilket resulterar i ett effektivt utnyttjande av kanalresursen. Användaren disponerar inte en större kanalresurs än den som är tilldelad.

[14] Zettersten, KTH, föreläsning, *Datakommunikation,* 2000-11-15
[15] VLAN: virtuella LAN, Cisco systems, *Produkter och lösningar,* 2002-10

Ett mobilt nät kan ha fast eller dynamisk tilldelning av kanalresursen. Dynamisk tilldelning kan fungera bra i ett nät med lite trafik, men är det för hög trafik kan det bli för mycket "krockar" med fördröjning som resultat. Fast tilldelning är däremot bra om man har mycket trafik i ett nät, men är det låg trafik finns risken att inte resurserna utnyttjas och man får onödigt stor tidsförlust.[16] I alla moderna mobila kommunikationssystem strävar man efter att åstadkomma en dynamisk tilldelning av kanalkapaciteten.

Vid dynamisk tilldelning utnyttjar användarna hela kanalresursen efter behov. Vid låg intensitet blir kollisionerna begränsade och man har ett effektivt utnyttjande av kanalen. Vid ökad intensitet växer problemen med kollisioner och omsändningar med ökad fördröjningen som resultat. Exempel på dynamisk access är *Carrier Sense Multiple Access* (CSMA). Sändaren lyssnar på kanalen för att kontrollera om den är ledig.[17]

2.5 Routing-principer

Att välja väg, *rutt*, i ett nät kallas, som nämnts i avsnitt 2.2, *routing*. En *routing-algoritm* har till uppgift att finna mottagarens adress samt de länkar och nätverksresurser som behövs för uppkopplingen. Det finns två övergripande principer för routing.

Proaktiv routing: kontinuerlig uppdatering av rutter. När en rutt behövs finns den tillgänglig omedelbart. Det kräver en stor apparat för hantering av alla rutterna. Denna lösning slösar med kanalresurserna, eftersom den kräver en stor overhead.

Reaktiv routing: rutter skapas endast då de behövs. Detta spar minnesutrymme och beräkningskapacitet. Tiden för upprättande av rutt blir längre än vid den proaktiva routing-metoden, ty den reaktiva metoden innebär att nätet avsöks globalt för att hitta en rutt. Det ger såväl långsamma som dåliga rutter. [18]

Särskilt i mobila nätverk är valet av routing-algoritm viktig. Mobiliteten medför förändringar på kanalen, med uppdateringar som följd. Det gäller att hitta den kortaste vägen mellan sändare och mottagare, för att få så liten tidsförlust som möjligt.

2.6 Databaser

En databas är i stort en mjukvara som presenterar lagrade data på ett logiskt sätt. En fråga är vilka av databasteknikerna som passar i mobila radionät och kan erbjuda en bättre strukturerad information. *Databashanteraren* står för den systematiserade hanteringen av data gentemot alla användare. Det är användarens tillämpning på databashanteraren som styr valet av hanterare. Faktorer som påverkar tillämpningen är bl.a. *åtkomsttiden, datatyper, samtidiga användare och dataskydd*.[19] Här följer några exempel på olika databastekniker:[20]

---

[16] Bilaga 2, s 10
[17] Söderqvist I, *Kommunikationsnät*, Totalförsvarets Forskningsinstitut, 2001, s 9
[18] Ibid, s 10
[19] Neider G, FOI, föreläsning Databasteknik, 2000-11-24
[20] *Tekniska utvecklingstrender*, FMV, s 174

- *Hierarkiska databaser* är väl etablerade och bygger på att de bara är designade för den applikation som använder databasen. Därmed är de inte helt lämpliga i ett mobilt radionät.
- *Relationsdatabaser* utgör en teknik som består av tvådimensionella tabeller som i sig är lätta att förstå. Tekniken[21] baserar sig på ett specifikt sätt, att ställa frågor till databasen.
- *Objektorienterade databaser* kan via en godtycklig struktur användas för att lagra, söka och presentera data. Det är en princip som används mer och mer i dagens läge på grund av sin ökade flexibilitet. Deras principer för flexibel access till information i databaserna är lämpliga för mobila radionät.[22]

En annan databastillämpning är *data-warehousing*, som bygger på att data mellanlagras och ges ett innehåll med utgångspunkt i olika modeller och arkitekturer för olika plattformar.[23] Denna modell har beståndsdelar som är intressanta att implementera i mobila nätstrukturer, där enheterna skall kunna ”vandra in och ut” ur det dynamiska självkonfigurerande nätverket. Data-warehousing innebär att olika plattformar lätt kan anslutas i nätverket om deras nätverksprofil är fördefinierad med en minskad tid för uppkoppling som resultat.

Databasreplikering
När militära enheter med egna databaser ska uppträda rörligt i en fast nätstruktur, uppstår situationen att olika enheters databaser skall jämföras med varandra, när de åter blir anslutna i ett nätverk. Detta kallas att databaserna replikerar varandra. Frågan uppstår då vilken information i respektive databas som har den *högsta förädlingsnivån* eller *är mest aktuell*. Tidsmärkning kan utnyttjas som en särskiljare, men det behöver inte vara så att den senaste tidsmarkeringen på informationen är den mest relevanta eller den informationen som har störst förädlingsvärde. Dock är det alltid så vad gäller rådata från en sensor, att där är den senaste tidsmarkeringen den mest aktuella.

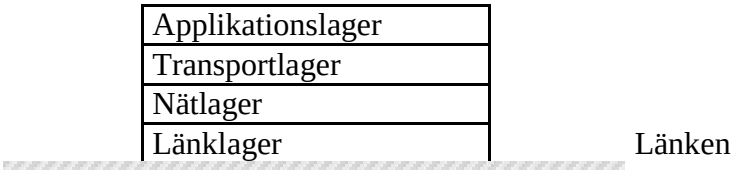
Mot bakgrund av att cirka 60 % av all nättrafik i dagens läge går åt till databasreplikering, är det en adekvat åtgärd att försöka minska detta effekt- och tidskrävande arbete. Tendensen är dock tvärtemot; att dator-dator-trafiken som syftar till att uppdatera, replikera databaser ökar. En trend som kan motverka databasreplikeringen är de s.k. distribuerade databaserna i kombination med en s.k. databasagent.[24] Dessa två företeelser beskrivs i kap 3.2.3.

2.7 Protokoll

Informationen som sänds över nätverk skall behandlas och tolkas. Idag används flera olika protokoll som tar hand om dataflöden. Protokollen kan liknas vid en samling regler för hur data ska tas om hand. TCP/IP protokollen har olika ansvarsområden och egenskaper, t.ex. adressering och kodning, och delas upp i olika lager i den sk. *stacken*. TCP/IP-stacken började utvecklas under 1960-talet

[21] SQL standarden
[22] Neider G, FOI, föreläsning Databasteknik, 2000-11-24
[23] *Tekniska utvecklingstrender*, FMV, s 174
[24] Tummala M och McEachen J, NPS, föreläsning Advances in High Speed Networking, 2001-05

och har idag nått långt över förväntningarna. En stadig utveckling och förnyelse av protokollen har skett under åren. Det är viktigt att förstå hur protokollstackens funktioner och egenskaper passar in i de nya nätarkitekturerna. TCP/IP-stacken har fyra lager eller nivåer som kommunicerar uppåt och neråt, enligt figur 2.3.[25]



Figur 2.3 TCP/IP-stacken

TCP
TCP ansvarar för att informationen som skickas från sändaren tas emot korrekt av mottagaren, och sänder om information som tappats bort. Eftersom AHN mestadels ska ha förbindelse med den fasta nätstrukturen inom NBF gör det att TCP måste användas. I fasta nät med låg bitfelssannolikhet uppstår bara en bråkdel av felen p.g.a. tappade paket eller avbrott på förbindelsen. De mobila trådlösa näten är känsliga för yttre störningar och har därmed relativ hög bitfelssannolikhet.[26] Felen beror dessutom ofta på att länkar försvinner och nya upprättas. Ibland bryts kontakten helt. Det innebär att kapaciteten inom ett mobilt radionät varierar och att trafiklasten därför måste anpassas hela tiden för att inte överbelasta nätet.

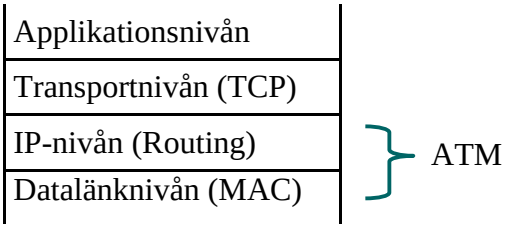
TCP skiljer tyvärr inte på fel som beror på överbelastning och fel som uppkommer p.g.a. hög bitfelssannolikhet eller avbrott, utan reagerar genom antagandet att felen beror på överbelastning. TCP sänker därför datatakten. Detta är mycket olämpligt eftersom det innebär att överföringen på kanalen blir mindre.[27] Detta resulterar i att de krav som ställs på kapaciteten hos radionät inte uppfylls.

ATM
Asynkron Transfererings Mod – ATM – är ett hybridprotokoll som kan utnyttjas för dataströmmar med höga tidskrav. ATM i förhållande till TCP/IP-stacken redovisas i figur 2.4.[28] Principen för ATM är att all information delas upp och packas i celler av fast storlek. Cellernas väg genom nätet bestäms före transporten och är den samma under hela sessionen. Detta ger följande egenskaper:
- Celler med fast storlek medger snabb hantering
- Fast väg genom nätet, cellerna kommer fram i rätt ordning. De behöver inte buffras eller sorteras.
- Uppdelningen i celler medför att bandbredden blir skalbar, dvs. få celler liten bandbredd. Det medför att bandbredden kan utnyttjas mer effektivt.

Men det finns problem också. Överföringshastigheten förväntas vara hög, vilket ställer krav på infrastrukturen. ATM har den stora fördelen att kunna hantera begränsad bandbredd. ATM kan ge en högre garanti för *Quality of Service* (QoS) (se

[25] Bilaga 2, s 8
[26] Persson, *TCP/IP i taktiska ad hoc-nät*, s 15
[27] Ibid, s 22
[28] Bilaga 2, s 8

vidare i 3.2.4). ATM:s styrka är att den klarar av att växla olika typer av trafik. Den är flexibel på bekostnad av effektivitet. ATM kommer att finnas som bärartjänst i publika höghastighetsnät eller i nätverk med krav på hög tjänstekvalité. Dock behövs inte ATM i nät som enbart skall förmedla data av enhetlig art.[29]



Figur 2.4 ATM i förhållande till TCP/IP-stacken

Datalänknivån
Eftersom enheterna i ett mobilt radionät påverkar varandra mycket mer än i ett fast nät blir datalänknivån med sitt MAC-protokoll (Medium Access Control-protokoll) viktigt att följa upp, se figur 2.4. En nod vet inte när prioriterade paket finns i grannoderna, vilket innebär att prioriteringar i noden inte räcker för att sända reserverade paket i trådlösa nät. Någon form av QoS-garanterande MAC-protokoll på länknivån blir därför nödvändigt.[30]

Det har visat sig att TCP/IP får problem när protokollet används i trådlösa nät. Den främsta orsaken till det är förekomsten av fel i överföringen, som är en källa till fördröjning. Bedömningen är att IP kommer att utvecklas mot att få en funktionsduglighet som liknar ATM. Det utvecklas också routingprotokoll som på sikt kan komma att göra IP lika snabbt som ATM.[31] (Tänkbara lösningar på TCP/IP:s problem finns beskrivna i kap 3.)

2.8 Resulterande fördröjning

Utöver fördröjningarna i nätverk finns förluster i källan, t.ex. en sensor, och i adressaten, t.ex. en vapenplattform. Fördröjningen i ett system har många olika orsaker. Om man utgår från fallet att ett mål skall bekämpas och målet har en given första position och listar olika tekniska källor till fördröjning enl. följande:

- Sensorn skall detektera målet. Beroende på sensor, aktiv eller passiv uppstår olika gångtidsskillnader för den elektromagnetiska strålningen från eller till och från målet.
- Sensorn i sig har en inbyggd fördröjning; svephastighet, processorberäkningsfaktorer.

Sensorinformationen skall sedan förmedlas över en förbindelse i nätverket med en varierande grad av fördröjning beroende på;

- *nätets transmissionsmedia; optofiber, kabel, radio eller satellitlänk*
- *olika typer av förmedling, krets- eller paketförmedlat. Där också själva uppkopplingen av förbindelsen tar olika lång tid.*

[29] Söderqvist, *Kommunikationsnät*, s 15
[30] Bilaga 2, s 9
[31] Tummala M, McEachen J, NPS, föreläsning Advances in High Speed Networking, 2001-05-02

- *att informationen kan ta olika långa vägar i nätverket vid paket-förmedlad överföring och IP vilket sammantaget ger olika fördröjning beroende på gångtidsskillnader*
- *olika typer av routingprinciper som också påverkar uppkopplingstiden.*

- Sensorinformationen skall integreras med annan sensorinformation för att exempelvis klassificera målet, en process som är automatisk, men som tar mer eller mindre lång tid.
- Vid vapnet finns också fördröjningar; beräkning av framförhållningspunkt, inbyggd fördröjning i inriktningsmaskineri, skillnader i flygtid för olika bekämpningssystem.

Under ett stridsförlopp finns även mänskliga faktorer som bidrar till fördröjning:

- I ledningssystemet skall befattningshavare fatta beslut om bekämpning. Alternativet är att vi har en autonom bekämpningssituation utan beslut.
- Bekämpningen skall bekräftas av en befattningshavare på vapenplatt-formen eller någon annanstans i systemet.

Beroende på ledningsdoktrin kan det finnas olika behov av mänsklig medverkan. Varje mänsklig medverkan innebär att fördröjningen ökas med åtskilliga sekunder. Vi studerar skeden av striden, där kraven på snabbhet är stora, och utgår från att processerna i ett sådant skede är automatiserade. Därför bortser vi här från de mänskliga fördröjningsfaktorerna.

Av de nu listade rent tekniska fördröjningarna, är det främst de som härrör från nätverkets olika funktioner som är dominerande. Vid fasta nätverk med TCP/IP-protokoll får man räkna med fördröjningar, jämförbara med dem vid användning av Internet. Vi kan därför referera till våra egna erfarenheter från e-post, sökning på Internet m.m. Redan en så enkel sak som ett kort e-postmeddelande i ett LAN kan ta flera sekunder om nätet har hög belastning. Själva överföringen i nätet kan alltså ta betydligt längre tid än den gräns på 1-2 sekunder, som vi uppskattade i exemplet i kap. 1.

För mobila enheter tillkommer tiden för uppkoppling i nätet varje gång kontakten har brutits. Slutsatsen blir att koppling till fast nätverk inte är en acceptabel lösning för mobila enheter i snabba stridsförlopp. Frågan är om ad hoc-nät i framtiden kan erbjuda en lösning på det problemet.

3 Ad hoc-nätens möjligheter

Vi har funnit att, i de skeden av en strid då kraven på snabb överföring är som störst, är fördröjningarna i de fasta näten för stora. Frågan är därmed om AHN-teknologin gör det möjligt att konstruera ett nätverk med erforderliga prestanda.

3.1 Bakgrund

När radio används i ett taktiskt ledningssystem är det ett medel för att upprätta förbindelser över avstånd, dels för att ge mobila användare access till den fasta nätstrukturen, det s.k. *accessnätet*, dels för att åstadkomma lokala radionätverk. Enheternas kommunikationssystem tillsammans med den upprättade kanalen utgör uppkopplingen, d.v.s. det vi kallar *länken*. (se kap 1.2)

Mobilitet och snabbhet i taktiska nätverk är avgörande i den nätverksbaserade striden. Frågan är hur de framtida systemlösningarna skall kunna anpassa till mobila enheter med hänsyn till de bandbreddsbegränsningar som finns på radio-förbindelser. Utmaningen med ett AHN består i att själva nätets struktur ändras kontinuerligt i och med att enheterna rör sig. Det leder till avbrott i förbindelsen mellan enheterna. Informationen måste därmed automatiskt finna nya vägar i nätet då avbrott uppstår.

3.2 Utveckling av ad hoc-nätverksteknologin

3.2.1 Nät med och utan hierarki

Ett nät kan vara *platt*, d.v.s. sakna hierarki, eller vara *hierarkiskt* med minst två nivåer. Ett exempel på hierarkisk nätstruktur är GSM. I GSM-nätet utförs all uppkoppling av trafik via de högre nivåerna, eftersom det är där det finns information om nätstruktur och noder (abonnenter).

Nät med hierarki – cellbaserat
I ett s.k. cellbaserat nät finns en *basstation* som täcker in de användare som befinner sig inom radioräckvidd från basstationens sändare. Användarna tillsammans med basstationen bildar *cellen*. Varje radiosändare inom cellen är hela tiden aktiv mot basstationen. Information om signalstyrka skickas till andra angränsande basstationer. Basstationen hanterar en eventuell överföring till en annan cell, en sk. ”handover”. All trafik till radiostationerna eller mobilerna i ett nät som GSM sker via basstationer. Både i upprättandefasen och i signaleringsfasen av sändningen sker datatrafik till det hierarkiska nätets högsta nivåer. Sätts de högre nivåerna ur spel kan inte basstationen fungera autonomt längre.

Nät utan hierarki – AHN
I ett nät utan hierarki krävs en omsorgsfull nätplanering. I och med att nätet inte har någon *centralnod* måste trafik reläas mellan radioenheter som ligger inom täckningsavstånd från varandra. Detta, att ingen nod agerar som centralnod, som vidaredistribuerar routingprotokoll och har kännedom om nätstrukturen, utgör en stor utmaning för den som ska konstruera ett AHN. Alla noder innehåller därför logik för att nätet ska kunna organisera sig, distribuera protokoll och ha information om den rådande nätstrukturen. Eftersom nätet förändras fortlöpande måste protokollen vara robusta och effektiva, samtidigt som de måste reagera

snabbt på omvärldsförändringar. AHN beskrivs därför även som ett *trådlöst distribuerat flerhoppsnät.*[32]

Begreppet *sömlöshet,* d.v.s. att användarna har tillgång till nätet trots förändringar i kommunikationen(enl kap 1.1), används i samband med mobila trådlösa nätverk. Det man syftar på är en sömlös yttäckning som består av ett stort antal trådlösa överlappande nät, sammanbundna av kommersiella och försvarsunika kärnnät.[33] Sömlöshet avser alltså inte bara AHN. Utan det rör sig om helheten – NBF – med sin kombination av fast infrastruktur och trådlösa mobila nätverk.[34]

3.2.2 Ad hoc-nätets arkitektur

I ett nät med flerhoppsfunktion kan alla stationer fungera som relästationer, informationen kan ofta finna ett flertal vägar eller rutter från sändarnod till mottagarnod. Detta i sig ger en robust arkitektur där meddelande snabbt kan hitta nya vägar. Länkarnas förbindelseavstånd är kort i förhållande till det cellulära nätet. Det medför även att mängden utstrålad energi kan hållas nere i förhållande till ett cellulärt nät. Nätstyrningens funktionssätt är dock mycket mer komplicerad. Detta beror på att den är distribuerad till alla noder som ingår i AHN.[35] Sammanfattningsvis kan man säga att:

Cellbaseratnät;	Flerhoppsnät;
- är sårbart	- är robust
- har långa länkar	- har korta länkar
- använder hög uteffekt	- använder låg uteffekt
- har enkel logik för nätstyrning	- har komplicerad logik för nätstyrning

Bluetooth[36] *– ett AHN?*
Bluetooth – sägs ibland vara ett AHN. Men det är inte ett renodlat AHN eftersom det bygger på en master-enhet och upp till sju stycken slavenheter som bildar ett piconät. Med andra ord är Bluetooth i grunden ett cellulärt nät. Systemet använder sig av bandspridning genom frekvenshopp. Det som gör att Bluetooth kan karaktäriseras som ett AHN, är den dynamiska tilldelningen.[37] Det finns dock ett mellanting, s.k. scater nets där två olika piconät kan länkas samman [38]. En uppkoppling av typ *”master-slav-master”* är då upprättad. Dock har denna lösning inte AHN:s totala flexibilitet.

3.2.3 Protokollutmaningen i AHN

Routing i AHN
Varför är ”routing”-resonemanget intressant i ett mobilt nätverk? Det är i alla sammanhang frågan om att hitta den kortaste vägen mellan sändare och mottagare med mindre förluster som mål. Mobiliteten i sig ger hela tiden förändringar på

[32] Söderquist, *Kommunikationsnät,* s 11
[33] Persson R, FMV, föreläsning Försvarsmaktens telekommunikationer i framtiden, 2001-02-23
[34] Bilaga 2, s 13
[35] Söderquist, *Kommunikationsnät,* s 14
[36] *Bluetooth* – en de facto-standard för trådlös korthållkommunikation mellan inledningsvis mobiltelefoner och bärbaradatorer. Systemet komunicerar på 2,4 GHz bandet. Syftet är att eliminera de skrymmande kablarna mellan olika enheter.
[37] Söderquist, *Kommunikationsnät,* s 26
[38] Bilaga 2, s 9

kanalen, med täta uppdateringar som följd. En fördel med ”routing”-protokoll är att de inte kräver en stor kontinuerlig information om nätet.[39] Det innebär att det inte krävs en stor överföring av information för att ha en uppdaterad bild om nätverket.

AHN och databastekniker
Var kommer databaserna in i AHN-resonemanget?

- Primärt kan det röra sig om att *lagra* allt från måldata, vapendata, underrättelser, meddelandehantering, etc. Databaserna kan vara såväl *centrala* som *lokala* eller *distribuerade*.

Sekundärt är det frågan om att *integrera* data, som är uppbyggda av olika beståndsdelar. En ny teknik för detta är s.k. medlare eller ”mediators” mellan databaserna och tjänsterna i nätverket. Medlardatabaserna utgörs av *distribuerade databaser* där innehållet är hämtat från andra databaser och datakällor, så som exempelvis en sensor.[40] En distribuerad databas är en databas, där delar av informationen finns på olika datorer i ett nätverk, men där databasen för användaren ändå uppträder som en enda databas.

Programvaran i medlarna, som verkar mellan användare och en uppsättning databaser, har förmågan att intelligent transformera frågor och sammanställa resultat. Medlardatabaserna kan presentera information utan en ökad fördröjning. Därmed är funktionen viktig i AHN, mot bakgrund av att medlardatabasen står för en förmedlad och förädlad information. I och med att tillgängligheten på informationen ökar genom de distribuerade databaserna minskas risken för fördröjning orsakad av databashantering.

En *databasagent* är ett autonomt program med uppgiften att underlätta arbetet för en användare som jobbar i ett distribuerat medlar databassystem. Agenterna är självständiga och ”intelligenta”[41] med kommunikations- och inlärningsförmåga. En farhåga som finns avseende databasagenten är att den kan ”leva sitt eget liv” och näst intill karaktäriseras av att vara ett virus. Dock är det fallet enbart beroende på hur nätverket upprättas och konfigureras samt hur rättigheter i nätverket tilldelas. Fördelar måste alltid vägas mot risker. Detta är inte ett problem om nätverksledningen helt och hållet är egenstyrd inom nätet. De distribuerade databaserna i kombination med en databasagent ger informationen i databaserna en högre tillgänglighet.

[39] Bilaga 2, s 11
[40] Ibid
[41] Begreppet intelligens i detta sammanhang grundar sig på datavetenskapens vilja att åstadkomma artificiell intelligens, d.v.s. ett beteende som kan uppfattas som intelligent av människor. Man har ännu inte nått till den punkt där något datorprogram kan kallas intelligent i en vidare mening. Men däremot har man i försöken med att uppnå detta uppfunnit en mängd nya programmeringstekniker. Agenten kan sägas vara intelligent om någon av dessa nya tekniker används, m.a.o. om den har ett självständigt och flexibelt beteende, med en stomme i ett datorprogram som kan förändras över tiden i takt med att erfarenheten växer.; Jungert E, Walter J, *Marksensornät och intelligenta agenter*, Användarrapport, Totalförsvarets Forskningsinstitut, 2001, s. 8

De olika databasteknikerna kan erbjuda gott stöd för nätstrukturerna i ett AHN, det gäller i synnerhet de distribuerade medlardatabaserna i kombination med funktionen agent.

TCP i AHN
Ett grundläggande problem med TCP är som sagt att protokollet inte kan skilja mellan olika fel på länken, utan alltid antar att felen beror på överbelastningar med påföljd att datatakten automatiskt sänks. Därför önskar man hitta en form av TCP som kan separera felen, och sålunda inte minska överföringshastigheten i onödan. Det skulle resultera i en ökad kapacitet hos AHN.

FOI har inom ramen för en studie tittat på problematiken.[42] Studien fokuserar på hur tappade paket och länkfel gör att överföringskapaciteten ändras. Studien granskar också om man genom att modifiera TCP kan se om det är möjligt att öka kapaciteten på förbindelsen. Studien visade att i trådlösa nät erhålls en hög bitfelshalt, vilket innebär att TCP sänker takten. I AHN förvärras situationen ytterligare eftersom information skickas mellan mobila noder. En modifiering av TCP är nödvändig.

FOI:s studie, som bygger på simuleringar, visade att om andelen tappade paket inte överskrider 10 % påverkas kapaciteten inte allvarligt. Den nivån kan man komma ned till medelst felrättande kodning i länklagret. I simuleringsmodellen visade det sig att inte heller avbrott ger särskilt stora problem. Det berodde bland annat på buffrandet i AHN. Kapaciteten ökade då paketen buffrades. Används *buffring* får korta avbrott endast en fördröjande effekt. Buffring innebär att informationen lagras tillfälligt för att sedan återges. Buffringen utförs främst för att tappade paket skall kunna sändas om och återgivningen skall bli sammanhängande.

Vid simuleringarna gjordes också en modifiering av TCP genom att låta datatakten öka hastigt efter avbrott vilket också visade att en ökning av kapaciteten var möjlig. Slutsatsen var att man kan göra effektiva modifieringar av TCP. Men vill man uppnå full effekt måste man förändra TCP för att kunna sända med information om ev. överbelastning.

Notera att förändringarna i TCP gav en kapacitetsökning, men att den byggde på buffring. Buffring medför alltid en viss fördröjning. Buffring har alltså inte bara positiva effekter. Det är viktigt att veta under vilka omständigheter buffring är till för- resp. nackdel i det här fallet.

FOI:s studie visar sålunda att utvecklingen av TCP kan medföra en ökning av kapaciteten genom buffring. Korta avbrott får bara en fördröjande effekt. Det viktiga i detta sammanhang är att kunna garantera en maximal tidsförlust i samband med länkfel och bitfel. Detta bedöms på sikt kunna klaras genom QoS-protokollen som berörs i nästa avsnitt.

[42] Persson, *TCP/IP i taktiska ad hoc-nät*, kap 6

3.2.4 QoS

Quality of Service – QoS – berör frågan om hur kapacitet skall reserveras på en länk. Det går relativt bra i ett fast nät där påverkan mellan länkar saknas. Köhanteringen kan då sköta det hela genom att skicka prioriterade paket först. Detta är dock ett större problem i radionät där andra sändande noder ger interferenser. Det är svårt för en nod att veta när prioriterade paket finns i grannoderna. QoS-problemen uppstår i radionät, därför kommer detta avsnitt att ta upp de olika QoS-teknikerna i förhållande till radionät.

Vissa applikationer och tjänster bygger på att fördröjningarna i förbindelserna inte är för stora. Förutsättningarna för dessa radioförbindelser varierar fortlöpande. Därför är det viktigt att granska de protokoll som hanterar kvalitetsgarantier inom TCP/IP. Här följer en beskrivning av de mest utvecklade varianterna för QoS som är aktuella i radionät som exempelvis AHN:

- Integrated Services (IntServ) karaktäriseras av resursreservering, vilket innebär att resurser reserveras längs den väg tidskritisk data skall sändas.
- I Differentiated Services (DiffServ) skapas olika prioritetsklasser som hanteras på olika sätt.
- MultiProtocol Label Switching (MPLS) använder sig också utav prioritering av paketen, vilka märks med olika etiketter. Etiketterna kan också användas för att snabbt hitta vägar och tunnla paketen.

IntServ ger absoluta garantier för trafiken men är inte skalbar i stora nät eftersom varje router måste hålla reda på informationen om varje datatrafikflöde. Därför utvecklades DiffServ som inte har detta problem. DiffServ har dock svårare att ge absoluta garantier. MPLS används på ett liknande sätt som Diffserv för att ge QoS-garantier. Att beakta är att dessa protokoll i första hand har utvecklats för fasta nät. På senare tid har intresset för QoS i AHN ökat och på sikt finns nog möjligheter att något av protokollen utvidgas för att även kunna fungera i sådana nät.[43]

Den stora nackdelen med IntServ är skalbarheten, men sett ur AHN-synpunkt är detta ett mindre problem eftersom AHN inte kommer att vara allt för stora, med stora menas i detta samanhang flera hundra stationer. Den begränsande faktorn är snarare kapaciteten på kanalen, än hur mycket data varje router kan hantera.

Någon form av reservation av kanalen är också nödvändig – man behöver ett QoS-garanterande MAC-protokoll på länknivån. Den allmänt mest förekommande standarden är den som jobbar med CSMA/CA (Carrier Sense Multiple Access /Collision Avoidance), som är ett exempel på dynamisk tilldelning av kanalen. Den standarden ger dock idag inga möjligheter till reservation. QoS på länknivån i radionätverk är ett område som kräver framtida forskningsinsatser.

Vissa ledningssystemstjänster kan bli svåra att realisera om det inte går att hantera garantier för fördröjningen i kommunikationsnätet. Detta gäller i synnerhet AHN, där förutsättningarna för radioförbindelser ständigt varierar. *Möjligheterna att*

[43] Persson K, Grönkvist J, Hansson A, *Garanterad tjänstekvalitet i taktiska IP-nät,* Användarrapport, Totalförsvarets Forskningsinstitut, 2002, s 14

med IP erhålla QoS i försvarets framtida kommunikationsnät är därmed en avgörande faktor för att kunna realisera mobilitet inom NBF.

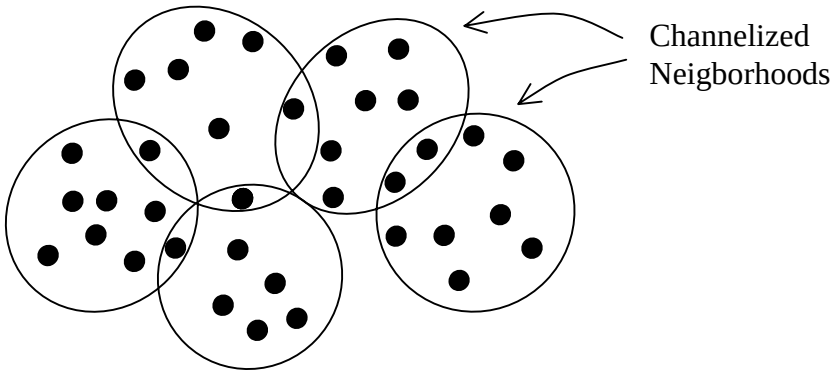
3.2.5 Standarder för ad hoc-nät

AHN är inte färdigdefinierat eller standardiserat.[44] Dock finns det de facto-standarder som bär framåt, exempelvis WirelessLAN (WLAN). Det är den hittills mest förekommande standarden i AHN-lösningar, men den har ingen utvecklad QoS.

Orthogonal Domain Multiple Access (ODMA), har potential att bli den tekniken som kan utvecklas inom AHN. Det är ett s.k. *multi-hopp* reläprotokoll som utnyttjas i cellulära lösningar. Principiellt bygger det på att man utnyttjar andra mobila stationer för att nå in i en stations täckningsområde.[45] ODMA är en attraktiv lösning för framtida mobila taktiska kommunikationssystem, beroende på fördelarna med reducerad signalstyrka och ökad täckning samt bättre QoS. I synnerhet när flera noder kombineras med varandra.

Detta protokoll utgör grunden i den systemlösning för AHN som Rockwell Collins utvecklat. Kommunikationsdelarna bygger på mjukvaruradio. I systemet finns en funktionsmodell för bredbandigt trådlöst nätverk, *Wireless-wideband Networking Engine* (WNE). WNE:n bygger på ODMA-teknik och medger att multipla noder kan sända simultant på kanaler utan interferens. Det resulterar i att hela nätverket får en ökad systemkapacitet med stor flexibilitet i nätbildningen.

En nyutvecklad funktion inom WNE:n är de s.k. *Channelized Neigborhoods* (CN), CN bygger på att ett antal noder inom ett räckviddsområde delas upp till subområden, för att få ökad prestanda när man utnyttjar smalbandiga kanaler. Det konceptet som finns i provbänkarna bygger på upp till 6 st. RF-kanaler på ca 1 MHz med kanalseparationer på 25 kHz. Just nu bedöms frekvensområdet 225-380 MHz som intressant.[46]



Figur 3.1 Konceptet Channelized Neigborhoods
(källa:Rockwell Collins)

[44] inom IEEE (Institute of Electrial and Electronics Enginers) som är en organisation som bl.a. arbetar med att standardisera kommunikationsprotokoll.
[45] Bilaga 2, s 10
[46] Rockwell Collins, Studiepresentation ad hoc-nätverk, 2002-11-12

Som felrättande kodning används en turbokodning som är förbunden med demodulationsteknik. Det hela resulterar i nivåer som ligger inom 3 dB från Shannons teoretiska gränser. CN-protokollet arbetar på MAC-lagret, direkt på länken. *Hela syftet med CN är att gruppera stora mängder noder till sammanslagna mindre och närliggande "kanaliserade områden"*, se figur 3.1. Dessa CN är inte cellulära i tidigare nämnd mening. De har sålunda inte någon nod med basstationskarraktär.[47]

AHN som bygger på den utvecklade ODMA-tekniken kan hantera många fler multiplar av noder utan att utnyttja någon som basstation. Detta innebär att noder kan sända simultant på kanaler utan interferens. Det medför att hela nätverket får en ökad systemkapacitet med stor mobilitet. Denna lösning innebär att utvecklingen mot en fungerande självkonfigurerande nätverksbildning har kommit så långt att AHN-tekniken kan prövas i fältförsök.

3.2.6 Ad hoc-nätverk i praktiken

FMV har inom ramen för den kunskapsuppbyggande verksamheten Försvarets Framtida Taktiska Kommunikation (FFTK) en uppgift att för Försvarsmakten under 2003 demonstrera dynamiska adaptiva nät. För detta har FMV engagerat Rockwell Collins.[48] Förstudien har omfattat en simulerad modell bestående av ett stort antal noder närmare bestämt 157 st, som skall kunna avveckla trafik med gruppsamtal i form av tal eller data inom kompani, IP-trafik och s.k. *trafik för situationsuppfattning.* Trafiken för situationsuppfattningen är till för att AHN:s noder skall ha en medvetenhet om den aktuella nätbildningen. Denna trafiken tar ca. 5-10 % av den totala trafikavvecklingen. Modellstudierna för 157 noder visar att det endast behövs 60 st. 25 kHz kanaler och 3 st. sändtagare per nod. [49]

Mjukvaruradio

En väsentlig del i ett AHN är de mjukvarustyrda radiostationerna. Det inte bara frågan om att använda mjukvara för att implementera radiofunktioner. Mjukvaruradio består av standarder med en öppen arkitektur. Tidigare brukades specifika radiosystem från enskilda tillverkare. I framtiden skall radiohårdvaran och mjukvaran komma från flera olika tillverkare. Den öppna arkitekturen bygger på publicerade standarder. Hårdvaran är modulär med standardgränssnitt. Mjukvaruradions affärsidé torde därför bli lik den kommersiella PC-industrin, på gott och ont. Mjukvaran bygger sedan på att man nyttjar de standardvågformer som är specifika för den situation man befinner sig i.[50]

Det intressanta med mjukvarustyrd radio sett ut ifrån AHN är att nya digitala nätverksvågformer utvecklas. De ska omfatta förmåga till interoperabilitet mellan försvarsgrenar, sömlös distribution av video, tal och data, automatiska eller manuella sändnings- och "routing"-möjligheter och slutligen *ad hoc-formering av nätverken med skalbarhet*. En intensiv utveckling av mjukvaruradio pågår. Inget av det som har med ad hoc-nätverk att göra finns i fullskala ännu. Endast försök i

[47] Rockwell Collins, Studiepresentation ad hoc-nätverk, 2002-11-12
[48] Bilaga 2, s 12
[49] Rockwell Collins, Studiepresentation ad hoc-nätverk, 2002-11-12
[50] Ibid

labb och provbänkar har genomförts hittills. Ett mindre försök[51] med 5 noder engagerade i ett AHN har demonstrerats under 2002. Sent 2003 skall FMV genom Rockwell Collins demonstrera AHN med 3-5 st. noder i Sverige.

3.2.7 Trender kring begreppet AHN[52]

Det är svårt att se någon trend kring applikationer med krav på liten fördröjning. En stadigt ökande forskning bedrivs i USA inom området, vilket innebär att provbänkslösningar och demonstratorer börjar visas. (Bl.a. genom ovan beskrivna projekt)

En annan aspekt är att frågor som rör säkerhet och adressering också måste lyftas fram för att ytterligare höja QoS i AHN. En uppfattning är att AHN-utvecklingen ännu inte har ett kommersiellt drivet intresse. Det beror på att man inte sett några väsentliga civila lösningar eller applikationer för AHN ännu.

Man måste vara på sin vakt vid användandet av begreppet ad hoc-nät. Det används med olika betydelse, eller åtminstone olika förväntningar på funktionsdugligheten, i olika användningsområden. T.ex. används det för den automatiska etableringen av ett nät av fast utplacerade marksensorer, likväl som för den här beskrivna dynamiska självupprättande och självkonfigurerande funktionen hos ett nät av noder som rör sig i terrängen. Lösningarna på dessa båda problem ser olika ut, främst beroende på tidskonstanterna i det rörliga nätet.

3.3 AHN och tidskraven

Den kretskopplade överföringen har en bestämd tidsförlust och den varierar inte över tiden. Det medför att vissa prestanda kan garanteras. I en paketförmedlad förbindelse kan sådana garantier inte ges.

Det är svårt att göra en generell uppskattning av skillnaderna i fördröjning mellan paket- och kretskopplade förbindelser. Med den kretskopplade förbindelsen har man tillgång till resurserna hela tiden och kan därmed ha en nästan konstant fördröjning, som beror på uppkopplingen i form av avstånd, kapacitet etc.[53]

Tal på IP är en kommersiell tjänst som driver på de kvalitetsmässiga krav man kan ställa på dataöverföringar. Än är inte den teknologin så långt driven att den erbjuder en kvalitetsmässig vinst. Men när IP-tal nått till nivån att man inte uppfattar någon eftersläpning i talet via hörseln, ca 0.25 s, innebär det att garantier för konstant tidsfördröjning i nätverk kan ges för olika typer av applikationer.[54]

I den paketförmedlade förbindelserna har man normalt inte tillgång till resurserna hela tiden. Paketen kan skickas olika vägar mellan sändare och mottagare och är beroende av annan trafik i nätet och därmed kan fördröjningen variera mycket. Om man t.ex. ska spela musik eller se på video eller dyl. via paketförmedlad förbindelse kan man buffra paketen hos mottagaren och sända dem med en konstant

[51] Inom ramen för projektet MOSIAC (Multifunctional On-the-move Secure Adaptive Integrated Communications) som CECOM (U.S. Army Communications-Electronics Command) driver.
[52] Bilaga 2, s 11
[53] Ibid, s 11
[54] Ibid, s 7

tidsförskjutning. Fördröjningen kan då bli hög men applikationen blir inte "hackig". QoS-protokollen används här för att kunna ge garantier även på denna trafik. *Man kan t.ex. reservera resurser eller låta paket få så hög prioritet att applikationer med krav på liten tidsförlust kan användas*. Om man kan uppnå något nära realtidskrav beror på applikationen och förbindelsens kapacitet. Man kan tyvärr inte dra någon generell slutsats.[55]

Routing- och accessprotokollen påverkar AHN kraftigt. De påverkar kapaciteten på så sätt att det kan ta olika lång tid att hitta nya och effektiva vägar. Dagens routingprotokoll är *inte* anpassade för QoS-trafik i AHN. På TCP/IP-nivån genom QoS-protokollen IntServ, DiffServ och MPLS förutsätts att routingen är löst av andra protokoll. Om QoS skall kunna erhållas i ett AHN med radionät krävs att man även utvecklar QoS-funktionerna på andra lager än IP. Ett sätt är att ge olika användare tillgång till kanalen vilket ger QoS på MAC-lagret. Lösningen på protokollproblemet kan ligga på länklagret med utvecklade QoS-funktioner inom *MAC-protokollet*.

QoS-problemen måste lösas om AHN skall kunna realiseras. Problem finns på alla nivåer i TCP/IP-protokollstacken. Målet är en effektiv QoS-arkitektur med systemkrav för dynamiska trådlösa nätverk. Olika protokoll har olika grad av förträfflighet. Det är bara att konstatera att man måste beakta vilka kvalitetskrav man vill sätta på de dataströmmar som går genom nätverket och välja protokoll efter detta. I AHN är det viktigt att ha en uppfattning om vad som bör krävas för att nå en acceptabel QoS-nivå. I AHN bör följande punkter utvecklas för att ge en acceptabel kravnivå:

- varje enskild nod kan klassificera paket som skall sändas.
- den som är behörig att kunna ge sin trafik en viss prioritet skall kontrolleras.
- ett protokoll som kan begära och reservera resurser används i det mobila nätet.
- ett protokoll som garanterar kapacitet för ett nytt flöde som skall etableras. Syftet med det är att noderna inte skall överbelastas.

Generellt kan man säga för att QoS ska fungera väl måste man se till att inte för mycket trafik går genom nätet, framför allt inte för mycket högprioriterad trafik. Annars har inte QoS-protokollet någon chans att garantera fördröjningsnivån för den prioriterade trafiken. I en situation med sensorer och robot mot ett flygplan under ett anfalls slutskede (som beskrivet i kap 1.2) är det inte troligt att en paketförmedlad förbindelse kan erbjuda tillräckligt liten tidsförlust. I den snabba situationen är det troligtvis endast den kretskopplade förbindelsen som kan lösa uppgiften. I ett AHN bör därför en möjlighet finnas att kunna koppla upp kretskopplade förbindelser för de tidskrävande situationerna. När detta utförs måste även vetskapen finnas att nätets utnyttjbara kapacitet minskar.

[55] Bilaga 2, s 11

4 Sensorintegration i ad hoc-nät

4.1 Bakgrund

Behovet av datautbyte mellan olika delar i ett nätverk ökar, inte minst beroende på att mängden sensorer blir fler. Detta påverkar i sin tur ett sensornäts uppkopplingar, med deras krav på liten tidsförlust. I ett framtida AHN med många ingående sensorer måste en minskning av datainnehållet göras, s.k. *kompression*, för att generellt kunna spara bandbredd i nätverken.

Innebörden av begreppet *gemensam lägesbild* (se kap 1.1) kan sammanfattas med att alla enheter har en likartad uppfattning om verkligheten. Det viktiga i sammanhanget är att alla aktörer i nätverket inte behöver ha samma mållägesbild. Aktörerna skall enbart erhålla den lägesbild som är relevant för deras uppgift. Rätt information ska fördelas till rätt befattningshavare. I processen har jämförelsen ett viktigt syfte att fylla, nämligen att rekonstruera ett enda läge utav de värden som står i samband med varandra och kommer från olika sensorer m.a.o. ställs mållägena i relation till varandra.

4.2 Källan till måldata: sensorer

Forskning och tekniska utveckling inom gamla och nya sensorteknikområden har resulterat i en utvecklingen av taktiska förmågor. Ett exempel på detta är nyttan av marksensorer, såsom ett markradarsystem, som både detekterar och noggrant fastställer fordons läge och riktning samt i vissa fall även klassificerar mål.[56] En större flexibilitet än dagens systemlösningar kan erhållas om *flera sensorer från flera olika delar av spektrumet kan kombineras*.

4.2.1 Sensorstyrning

I moderna radarlösningar är identitets- och positionsfunktioner (ID/Pos) intressanta beroende på att de erbjuder utökade möjligheter i ett AHN. Mjukvarumässigt kan sensorn erbjuda en mängd funktioner, t.ex. stridsvärdessammanställning, gemensam fusionerad mållägesbild och sensorledning.[57]

4.2.2 Bearbetning av sensordata

Var skall integrationsprocessen utföras – vid sensorn eller högre upp i nätverkshierarkin, eller rent av vid vapnet? Vilka för- och nackdelar finns? Flera sensorer i olika våglängdsområden har varit integrerade i en och samma plattform fram till och med dagens sensorsystemlösningar. Men i framtiden behöver det inte bara vara aktiva sensorer, det kan lika gärna vara passiva sensorer som är integrerade i systemen. Det nya är dock att de kan samordnas och samutnyttjas i nätverk.

Förbättrad datorkapacitet kommer att möjliggöra allt mera sofistikerad bearbetning och fusionering av data från flera sensorer. Det kan på sikt komma att innebära att data från bildalstrande sensorer kan fusioneras, liksom att automatisk analys av bildinnehållet blir möjligt. Arkitekturen för en sådan fusionsprocess

[56] Bilaga 2, s 3
[57] Ibid, s 5

kommer att vara varierande. Det beror på att det måste vara möjligt att fusionera data med varierande grad av förbehandling.

Kompression
Det har konstaterats att i ett framtida ledningssystem kommer det att ingå många fler sensorer än i dagsläget. Frågan är var *kompressionen* skall utföras? Kompression innebär att datainnehållet minskas, exempelvis genom att råradarbilden omsätts till målplottar. Kompressionen syftar till att kunna hålla nere dataflödet. Är det vid sensorn eller längre bak i systemet det ska ske? Två principer finns:

- Låt kompressionen ske så nära sensorn som möjligt.
- Komprimera inte vid sensorn utan skicka vidare all information,

I allmänhet måste den första gälla p.g.a. den generella bandbreddsbegränsning som i synnerhet finns i mobila radionät. För sensordata som har fusionerats innebär det som regel att den ursprungliga sensorinformation inte finns kvar längre, om den inte av något skäl sparats i databas.[58]

4.2.3 Informationsfusionering

Den totala mängden sensordata kommer att öka p.g.a. att antalet sensorer helt enkelt blir många fler i framtiden. Detta leder fram till att olika former för selektering av information i ledningssystemen måste finnas.[59] Selekteringen syftar till att beslutsfattarna i den nätverkscentriska striden inte skall drabbas av ett informationsöverflöde. För att motverka detta utvecklas former för automatisk informationsfusionering i nätverket. En sådan första åtgärd är att automatiskt skapa en gemensam lägesbild som alla enheter som medverkar i nätverket har del i. *Hur den gemensamma lägesbilden åstadkommes är en av nyckelfrågorna kring hur det nätverksbaserade försvaret skall anordnas.*

Det ökade informationsflödet förskjuter successivt den militära chefens huvudproblem som tidigare baserats på vag och ofullständig information till att stora mängder komplex information står till förfogande. Den stora mängden information kan göras hanterbar genom informationsfusion. Ett verktyg som används för att skapa en bild av datafusion är den s.k. JDL-modellen[60] med sina 4 förädlingsnivåer.[61]

4.3 Sensorintegration

4.3.1 Datafusion

Fusion som företeelse får en allt större plats i vitt skilda sammanhang. Inom nätverken rör det sig framförallt om hur data kan integreras i olika databaser. Fusionering som begrepp används även inom sensorsammanhanget genom att se på möjligheterna att ta måldata från sensorer i olika våglängdsområden och av det

[58] Tummala M, NPS, föreläsning kursen Advances in High Speed Networking, 2001-05
[59] Jönsson L m fl, *Informationsfusion i den taktiska underrättelseprocessen*, s.17-22
[60] JDL-modellen: är en abstrakt modell för datafusionsbegreppet, så som det uppfattas av en studiegrupp från de amerikanska försvarsforskningslaboratorierna, Joint Directors of Laboratories. Modellen beskriver datafusionsbegreppet som om det i informationssystemet finns olika förädlingsnivåer. Svensson P, FOI, föreläsning Robusta Informationssystem, 2000-11
[61] Svensson P, FOI, föreläsning Robusta Informationssystem, 2000-11

skapa kombinerad målinformation. FOI beskriver datafusion som: informationsbehandlingsprocesser där information från olika källor slås samman för att ge en mer komplett och mindre osäker tolkning av ett skeende. Informationen kan från början vara osäker, ofullständig och motstridande. Datafusion spänner över ett stort område, det går genom följande steg i JDL-modelens förädlingsnivåer: från *multisensordatafusion* (lägsta nivån i JDL-modellen), via situationsanalys, hotanalys till beslutsstöd.[62] *Multisensordatafusion innebär* att en större robusthet, precision och överblick av sensorsystem uppnås genom att i nära realtid fusionera information från flera sensorer, ofta baserade på olika slags sensorteknik.[63]

4.3.2 Trender inom ”sensor-networking”

Den digitala antenntekniken medger att ett antal enskilda sändare och mottagare kan styras och att man därmed kan sända ut en varierad lob och ta emot signalen med flera smala lober i intressanta riktningar Tekniken kallas *digitala gruppantenner* (DGA). En DGA-radar är därmed även svårare att störa än andra typer av radarstationer. De digitala gruppantennerna medger att radarsystem som bistatisk radar och multistatiska-radarnätverk är tekniker som kan vinna terräng i framtiden.[64]

Varför är detta intressant ur AHN-synvinkel? Sensorkoncepten bygger på nätverk i och med att sensorerna skall samverka på olika sätt. Det innebär att varje enskild flerfunktionsradar mäter, och att samverkan sker när mätdata fusioneras. Mätresurserna för radarsensorerna styrs och fördelas också genom nätverk. Plattformarna för många radarstationer är mobila och därmed kan sensorerna komma att ingå i AHN. Det är därmed avgörande att AHN kan garantera att fördröjningen inte blir för stor.

4.3.3 Multisensordatafusion

En fråga som kan ställas innan multisensordatafusion beskrivs är: När räcker det med en sensor för att upptäcka ett mål? Svaret på den frågan är: Alltid, p.g.a. att om det finns många sensorer, måste alltid en vara först med att upptäcka målet och följaktligen ge måldata för bekämpning.

När kan fler än en sensor behövas? Svaret på den frågan blir: För det mesta, fler sensorer ger en bättre möjlighet till att klassificera ett mål. Dock har den tekniska utvecklingen på sensorsidan medfört att den bästa sensorn kanske ofta ger ett resultat som tävlar med resultatet från en genomförd multisensordatafusion.

Varför inte alltid ta bästa sensorns värden är en relevant följdfråga i sammanhanget? Ta liknelsen med ögonpar: ”Två par ögon ser mer än ett par”. Genom en fusionering av information från sensorer med olika sensorteknik i olika våglängdsområden kan också en mängd fördelar uppnås. Väljs enbart bästa sensorns resultat istället för sensorfusionens resultat, uppnås inte heller möjligheten att gå vidare i fusionsprocessen.[65]

---

[62] Jönsson L, föreläsning i Robusta Informationssystem, 2000-11-22
[63] Jönsson L m fl, *Informationsfusion i den taktiska underrättelseprocessen*, s 118
[64] Bilaga 2, s 5
[65] Jönsson L m fl, *Informationsfusion i den taktiska underrättelseprocessen*, s 46-47.

Sensorintegrationen är en förutsättning för att kunna gå vidare med de s.k. bi- och multistatiska radarteknikerna för att på olika sätt att uppnå multisensordatafusion. Antingen kan sensordata levereras direkt till nätet eller gå via en fusionsnod. En kombination ger bra robusthet. En viktig del i fusioneringen är sensorstyrning och sensorledning.[66] För att åstadkomma det skall de paket med sensordata som skall till en annan nod inkapslas innan vidarebefordring. Det medför att paketen kan erhålla rätt prioritering i nätet och att deras tidsfördröjning har en konstant nivå.

Svårigheter och möjligheter
Faran med fusion på målspårsnivå, d.v.s. då man fusionerar t.ex. spår från två olika sensorplattformar som var för sig följt målet, är att informationen kan tidsfördröjas. En svårighet kan också vara att olika nivåer strukturerar om informationen vilket medför osäkerhet i beslutsunderlaget på en högre nivå. Frågan som uppstår är om det är samma iakttagelse? Vad är korrekt, vad är förvanskat? Detta problem kan uppstå när flera källor levererar information via olika kanaler.[67] Genom att använda information från fler sensorer ökar möjligheterna till en säkrare associationer.[68] Det innebär att ju fler sensorer som är sammankopplade i nätverket desto större möjligheter finns att åstadkomma en bättre kvalité på sensorfusionen.

Integration av arvet i AHN
Nuvarande och tidigare generationers sensorer bör vara en del i NBF. Det gäller såväl de kvalificerade sensorer som behövs i den fasta strukturen, som de sensorer som kan agera inom ett AHN:s område. Det kan exempelvis röra sig om markmålssensorer, artillerilokaliseringsradar och luftvärnsradar.[69] De moderna befintliga sensorerna har ofta en sådan utvecklingsnivå att de kan medverka i ett AHN.

”Sensor to Shooter”
Termen ”sensor to shooter” används i vida sammanhang. Den är dock inte helt adekvat för att beskriva situationen när även en beslutsfattare i ett nätverk är inblandad. Beslutsfattaren vet var målet finns via sin mållägesbild, men vapenplattformen vet det inte. Det avgörande behovet är att lyckas förmedla sensorinformation till beslutsfattaren och mållläge till vapenplattformen. Tillgången på bandbredd är nyckeln till framgång tillsammans med förståelse för hur mycket information betjäningspersonal kan ta emot och förstå.[70] Det kommer att krävas en högre grad av automatisering om den tidskritiska överföringen av information skall kunna hanteras effektivt. Detta är speciellt viktigt i och med att både insatsavstånden för vapenplattformarna och beroendet av målinformation från en annan plattform med sensor ökar. Denna samverkan mellan sensor och vapenplattform är beroende av att uppkopplingar med garanterad snabbhet finns att tillgå. Det är vad ett AHN i framtiden skall kunna stödja om QoS-protokollen utvecklas med tidsgarantier.

---

[66] Bilaga 2, s 6
[67] Jönsson L m fl, *Informationsfusion i den taktiska underrättelseprocessen*, s 72.
[68] Lauberts A, föreläsning Multisensorfusion, 2000-11
[69] Bilaga 2, s 4
[70] Hoyle C, Sensor to shooter capabilities: Sensors working overtime, Jane's Defence Weekly, 16 juli, 2002

4.4 AHN – ett led i sensorintegrationen

Multisensordatafusion innebär säkrare lokalisering, målföljning, identifiering, och bättre positionsangivelse, bättre klassificering och därmed färre tvetydigheter än autonoma system. Det ger ett robustare system, än om man är beroende av endast en sensor. System blir också svårare att lura med störning. Resultatet av en sensordatafusionsprocess tolkas som en mer komplett och mindre osäker bild av ett skeende, än om endast data från enskilda sensorer använts. Förmågor till detta är något som eftersöks på stridsfältet i NBF.

För att genomföra multisensordatafusion krävs en hel del parametrar: modeller av möjliga beteenden, adekvata och kvalitetsmärkta indata såsom sensordata, förbandsdata, geografisk information och väder, allt mer eller mindre tillgängligt men ändå komplext att sammanföra. Denna information finns lagrad i databaser i nätverket. *Det innebär att sensordatabaser måste ges en hög tillgänglighet i AHN.* I syfte att förenkla dataflödet bör man i NBF definiera ett antal enhetliga protokoll för exempelvis spaningssensorer, måldatameddelande etc.

Multisensordatafusion på taktisk nivå inom NBF hänger på att AHN kan ombesörja förmedlingen av den information som krävs för att skapa dessa tjänster. Granskningen har visat att det är möjligt för AHN att på sikt utföra *förmedling* av datatrafik för multisensordatafusion, förutsatt att prioriteringar kan utföras.

5 Sammanfattning

Kapitel 1-4 har avsett att belysa och om möjligt besvara de tre frågorna på s.6. Här följer en sammanfattning av det som framkommit i dessa kapitel.

- **Vilka krav på nätverk måste ställas för att ge erforderliga förbindelser mellan rörliga enheter?**

Ett syfte med NBF är att man ska erhålla s*nabbare reaktionstider* i ledningssystemen. Nätverken måste därför tillse att databasernas *information är tillgänglig* för de aktörer som har behov av den. Ett krav är därmed att nätverksuppkopplingarna ska kunna *garantera överföring* av tidskritisk information.

Mobila nätverk kommer att utgöra en stomme i den nätverksbaserade striden, inte minst med tanke på att stridens karaktär i framtiden kommer att förändras. Denna kommer att präglas av ett högt anfallstempo, över stora ytor. *Snabbhet* och rörlighet är ledord för framtidens nätverksbaserade strid.

Tillgänglig information
Medlardatabaserna är en teknik som utgörs av distribuerade databaser, där innehållet är hämtat från andra databaser och datakällor. Styrkan med medlardatabaserna är att de kan presentera information utan en nämnvärd ökad fördröjning, vilket är viktig i mobila nätverk.

De mobila nätverken ska vara kompatibla med NBF:s övriga nätstruktur, vilket innebär att TCP/IP används (se kap. 2.7).

Garantier för överföring
Har det mobila nätverket en väl utvecklad och fördefinierad virtuell LAN-struktur, kan olika typer av datatrafik hanteras smidigt och även förenkla prioriteringar.

Variationerna av datatyper är stor i ett mobilt nätverk, allt från tal och målinformation till lägesbilder och video. En utvecklad multicast-funktion (se kap 2.3) inom VLAN-strukturen är nödvändigt, annars kan en mottagare som tar emot stora mängder data kraftigt försämra prestanda för andra i det mobila radionätverket.

Snabbhet
Kravet på snabbhet för en nätverksförbindelse varierar beroende på den typ av applikation som skall nyttja informationen som överförs. I de mest extrema situationerna, som exempelvis de när måldata skall överföras från sensor till vapen, får den totala fördröjningen i systemet inklusive nätverksförbindelsen inte överstiga ca 1-2 s (se kap 1.2).

- **De fasta nätverkens protokoll skapar okontrollerbara fördröjningar när de utnyttjas i mobila radionätverk. Kan ad hoc-nät erbjuda en lösning på problemet?**

Problemet med TCP är att protokollet inte skiljer mellan olika fel på länken, utan alltid antar att felen beror på överbelastningar i nätet. Detta medför att datatakten sänks. Ad hoc-nät (AHN) påverkas negativt av detta beroende på att det vanligaste felet på radioförbindelser är avbrott. Kapaciteten måste därför kunna varieras, vilket medför att *trafiken måste kunna regleras*. AHN:s kapacitet påverkas kraftigt av routing- och accessprotokollen. De är optimerade för fasta nät, vilket medför att det kan ta olika lång tid att hitta nya vägar.

Den största utmaningen i ett AHN bygger på att ingen nod agerar som centralnod, som vidaredistribuerar routingprotokoll och har kännedom om nätstrukturen – detta skall alla noder hantera självständigt.

Fördröjning
FOI:s studier visar att utvecklingen av TCP medför att kapaciteten kan ökas genom buffring (se kap 3.2.3). Korta avbrott får bara en fördröjande effekt. Det viktiga i detta sammanhang är att kunna garantera en största fördröjning i samband med avbrott. Detta är något som QoS-protokollen på sikt bedöms kunna klara. Notera att buffringen i sig också åstadkommer en tidsförlust som dock är känd. Detta är inte en lösning för de mest tidskrävande dataöverföringarna som används vid mycket snabba stridsförlopp. Fördröjning i AHN beror på flera saker: förmedlingsprincip, applikation, avstånd och förbindelsens kapacitet. Därmed kan man inte dra någon generell slutsats om en konstant tidsfördröjning.

Trafikreglering
Det väsentliga i utvecklingen av AHN-teknologin är att finna en modell av TCP, som kan separera felen och ändå inte minska överföringshastigheten i onödan. Det skulle resultera i en ökad kapacitet hos AHN, med ökad snabbhet som resultat.

Kretskopplade förbindelser är överlägsna vad gäller att kunna garantera en konstant fördröjningsnivå på dataöverföringen. Det medför att delar av nätet blir upptagna med en totalt försämrad kapacitet på nätverket. Den paketförmedlade förbindelsen kan ännu inte garantera en nivå på fördröjning. Funktioner som hanterar detta är Quality of Service. För att ha kvar *flexibiliteten* som den paketförmedlade förbindelsen har måste QoS-protokoll utvecklas för att kunna ge garantier för routing i nätverket och garantier för tidsförluster.

Routingprotokoll är inte anpassade för QoS-trafik. För att QoS skall fungera väl måste man tillse att inte för mycket högprioriterad trafik går genom nätet – ge nätet en chans. I AHN måste följande QoS-relaterade funktioner utvecklas:

- enskild nod skall kunna klassificera paket som sänds.
- protokoll som kan begära och reservera resurser.
- protokoll som garanterar kapacitet för ett nytt flöde som skall etableras, för att kunna reservera plats.

Dessa åtgärder kan medföra att QoS hamnar på en acceptabel nivå vad avser fördröjning.

Mjukvaruradion med sina nya digitala vågformer kan åstadkomma och garantera ad hoc-formering av radionätverken.

AHN-tekniken som bygger på ODMA, ett multi-hopp reläprotokoll, har utvecklats för att hantera flera noder utan att utnyttja någon som basstation. Det innebär att multipla noder kan sända simultant på kanaler utan interferens. Det resulterar i att hela nätverket får en ökad systemkapacitet med stor mobilitet. En ny funktion är ”Channelized Neigborhood”-tekniken (se kap 3.2), vilket innebär att noderna delas upp i olika områden för att få ökad mobil prestanda med totalt många fler ingående noder. *Denna teknik har en potential att kunna utvecklas mot en konkret AHN-systemlösning.*

- **Kan ad hoc-nätverken erbjuda vägar för sensorintegration med tillräcklig kapacitet och snabbhet?**

Utvecklingen inom sensorområdet går mot kombinationer av flera sensorer. Multisensordatafusion ger ökade möjligheter till att åstadkomma mer relevant sensorinformation. Därför måste man skapa en hög *tillgänglighet* av sensor-information i AHN.

Multisenordatafusion kräver en mängd information, den finns bl.a. tillgänglig i nätverkens databaser. Det är dock komplext att sammanföra informationen. Fusionsprocessen är därmed beroende av ett fungerande nätverk med möjligheter att prioritera och ha kända parametrar för tidsförluster.

Tillgänglighet
Utvecklingen av AHN bidrar till att sensorinformationen kan utnyttjas bättre. Tiderna från upptäckt till bekämpning kommer därmed att kunna minskas.

Fusionsprocessen
Det mesta av den aktuella information som krävs för multisensorfusionen kan lagras i databaser och inom ramen för nätverket erhålla en hög tillgänglighet. Det innebär att det ställs krav på att AHN:s sensordatabaser har en hög tillgänglighet. Tillgängligheten på databaserna kan skapas genom en kombination av principer där medlardatabaserna med sina distribuerade databaser utgör stommen. Multi-sensordatafusionen går också ut på att märka upp och reservera kapacitet i nätverket. Det kan åstadkommas genom att använda QoS-protokoll som begär och reserverar resurser. AHN kan därmed på sikt ge de tids- och kapacitetsgarantier som behövs för att en multisensordatafusion skall kunna ske med tillräcklig snabbhet.

Snabbheten för sensorintegration kan därmed uppnås i de framtida AHN om QoS-protokollen utvecklas.

Avslutning

Kraven på dataöverföring i nätverket är olika i olika skeden av ett stridsförlopp. Det krav på snabbhet i överföringen, som vi fick fram i slutet av kap. 1, hänförde sig till slutfasen av en bekämpning av flygplan med robot. Vi fann med en enkel modell att en fördröjning av informationen i slutskedet, från sensorer till robotens styrorgan, inte fick vara större än 1-2 sekunder, däri inbegripet tiden i själva sensorn, ev. uppkoppling i nätet (om det skett avbrott), processer för multisensor-datafusion, paketförmedling i nätet, mekanismer för störningsskydd o.s.v. Skulle ett ad hoc-nät kunna fylla kraven i en så extrem situation, så skulle AHN förstås fungera utmärkt i mindre krävande situationer.

Frågan om ad hoc-näten i tidsperspektivet fram till 2007-2010 skulle kunna klara kravet i det extrema exemplet gav mina intervjuer inte något klart svar på. Det framgick att prestanda kan väntas bli avsevärt förbättrade jämfört med nuläget, men några säkra kvantitativa uppgifter kunde jag naturligt nog inte få.

Vissa försiktiga bedömningar kan dock göras. Man räknar med att det ska bli möjligt att använda paketförmedling för vanligt mänskligt tal i realtid. I en samtalssituation kan en fördröjning av signalen från den talande till den lyssnande på mer än ca 0.25 sekunder inte accepteras. Blir fördröjningen större än så, försvåras samtalet märkbart. Förväntas det kravet kunna uppfyllas, är det inte orimligt att fördröjningen av sensordata ska kunna bli mindre än 1-2 sekunder.

Men alldeles uppenbart är det inte. Att överföra ett talat meddelande rätt och slätt, är något mycket enklare än att förmedla data från ett antal sensorer till lämpliga databaser, fusionera dem, och förmedla informationen vidare till vapnet i en miljö med stor störningsrisk. Vi måste därför planera för en framtid, då AHN inte kan uppfylla de krav som ställs i slutskedet av en bekämpning. Nätverket kan fungera utmärkt i mer normala situationer. *Men i slutfasen av en bekämpning med robot måste roboten vara autonom*. Den måste vara försedd med en egen sensor, och kan inte förlita sig på data från nätverket.

Referenser

Tryckta källor

Alberts S, Garstka J, Stein F, *Network Centric Warfare*, Library of Congress Cataloging-in-Publication Data, 1999

FM idé och målbild, rapport 5, Försvarsmakten

Hellman A, *Att förstå Telekommunikation*, Ericsson Telecom, Telia studentlitteratur, 1996

Hoyle C, Sensor-to-shooter capabilities: Sensors working overtime, Jane's Defence Weekly, 16 juli, 2002

Jungert E, Walter J, *Marksensornät och intelligenta agenter*, Användarrapport, Totalförsvarets Forskningsinstitut, 2001

Jönsson L m fl, Informationsfusion i den taktiska underrättelseprocessen, Försvarets Forskningsanstalt, Linköping, 1998

Persson K, Grönkvist J, Hansson A, *Garanterad tjänstekvalitet i taktiska IP-nät*, Användarrapport, Totalförsvarets Forskningsinstitut, 2002

Persson K, *TCP/IP i taktiska ad hoc-nät*, Teknisk rapport, Totalförsvarets Forskningsinstitut, 2002

Söderqvist I, *Kommunikationsnät*, kompendium, Totalförsvarets Forskningsinstitut, 2001

Tekniska utvecklingstrender, Försvarets Materielverk, 2001

Övriga källor

Andersson J, Stensby O, föredrag och samtal angående sensorutveckling och nätverk, Ericsson Microwave Systems, 2002-10-03

Cisco systems, Produkter och lösningar, http://www.cisco.com/warp/public/3/se/lan/teknologi_lan.html, 2002-10

Ericsson T, samtal angående synen på ad hoc-nät, Kompetenscentrum Sensor och Telekom, Försvarets Materielverk, 2002-11-12

Grönkvist J, Persson K, intervju angående utveckling av ad hoc-nät, avdelningen för sensorteknik, Totalförsvarets Forskningsinstitut, 2002-10-30

Hansson A, Totalförsvarets Forskningsinstitut, föreläsning Kommunikationsnät, kursen Robusta Sambandssytem, 2001-04

Hyllander A, intervju angående sensorer och bekämpningssystem, Artilleridemonstrator-projektet, 2002-09-20

Neider G, föreläsning Databasteknik, kursen Robusta Informationssystem, Totalförsvarets Forskningsinstitut, 2000-11-24

Persson R, FMV, föreläsning Försvarsmaktens telekommunikationer i framtiden, 2001-02-23

Rockwell Collins, studiepresentation ad hoc-nätverk mm, 2002-11-12

Svensson P, Totalförsvarets Forskningsinstitut, föreläsning Robusta Informationssystem, 2000-11

Tummala M och McEachen J, Naval Postgraduate School, föreläsningar inom kursen Advances in High Speed Networking, , 2001-05-02

Zettersten B, KTH, föreläsning Datakommunikation, kursen Robusta informationssystem, 2000-11-15

Figurförteckning

Figur 1 Uppsatsens struktur
Figur 2.1 Paketförmedlad förbindelse
Figur 2.2 Kretskopplad förbindelse
Figur 2.3 TCP/IP-stacken
Figur 2.4 ATM i förhållande till TCP/IP-stacken
Figur 3.1 Konceptet Channelized Neigborhoods (källa:Rockwell Collins)

Förkortningsförteckning

Förkortning	*Betydelse*	*Sida*
AHN	Ad hoc-nätverk	4
ATM	Asyncron Transfer Mode	17
CN	Channelized Neigborhood	25
CSMA/CA	Carrier Sense Multiple Access/Collision Avoidance	15
DGA	Digitala Grupp Antenner	31
DiffServ	Differentiated Services	24
FFTK	Försvarets Framtida Taktiska Kommunikation	26
IEEE	Institute of Electrical and Electronics Enginers	24
IntServ	Integrated Services	24
JDL	Joint Directors of Labratories	30
LAN	Local Area Network	11
MAC	Medium Access Control	18
MPLS	Multi Protocol Lable Switching	24
NBF	Nätverksbaserat Försvar	4
NCW	Network Centric Warfare	4
ODMA	Orthogonal Domain Multiple Access	25
QoS	Quality of Service	23
TCP/IP	Transmission Control Protocol / Internet Protocol	16
VLAN	Virtuella Local Area Network	11
WLAN	Wireless LAN	24
WNE	Wireless-wideband Networking Engine	25

Genomförda intervjuer och samtal

Först redovisas de frågor som framtagits inför intervjuerna. Valda delar av frågorna har legat tillgrund för de olika intervjuerna, beroende på att intervjupersonerna har olika kunskapsinriktning. Därefter redovisas intervjuerna i kronologisk ordning. Under intervjuerna har diskussionerna tagit sådana vändningar att nya eller omformulerade frågor utkristalliserats. Dessa frågor är redovisade under respektive intervjusvar. Texten som redovisas baseras på anteckningar från de olika samtals- och intervjutillfällena.

Intervjuunderlag

1.1.1 Vad uppsatsen handlar om i stort

- De IP-baserade nätverkslösningarnas begränsningar i mobila radionätverk.
- Ad hoc-nätverkens möjligheter inom NBF. Frågan är om de svarar mot de krav som ställs på uppkopplingar i exempelvis mobila sensornätverk.
- De tidskritiska informationsöverföringar som skall kunna ske i ett nätverkskoncept.
- Frågan om man kan genomföra multisensordatafusion i ad hoc-nätverk.

Problemet handlar i grunden om huruvida det finns möjligheter att med framtida ad hoc- nätverkskopplingar skapa tillräckligt snabba och säkra sensor-vapen kopplingar i nätverksstriden.

1.1.2 Intervjufrågor

- Kan man i det utvecklingsstadium som ad hoc-nätverk befinner sig i, uttrycka några krav på säkerhet och snabbhet i uppkopplingarna och då med tonvikt på fördröjningar i uppkopplingarna?

- En stor del av dagens dator-dator nättrafik åtgår åt databasreplikering. Vilken trend kan man skönja vad avser att minska en sådan effektkrävande nättrafik, och hur påverkar det ett tänkt sensornätverk med krav på liten fördröjning?

- Det finns många nya databastekniker. Är det en trend att de används i sensordatafusion? Kan teknikerna även minska databasreplikeringen? Vilken påverkan får de på ad hoc-nät (distribuerade databaserna, databasagenter och datareplikeringsagenter)

- Finns det möjligheter att i IP överföra tidskritisk och realtidsnära information med krav på liten fördröjning?

- Bearbetning av sensordata - skall bearbetningsprocesserna utföras vid sensorn eller högre upp i nätverkshierarkin, eller rent av vid vapnet? För- och nackdelar.

- I ett framtida ledningssystem kommer det att ingå många sensorer. Var skall kompressionen ske för att kunna spara bandbredd i de mobila nätverken?

- Kan sensordata representeras i realtid eller nära realtid genom multisensordatafusion ?

- Kan trådlösa ad hoc-nätverk erbjuda mindre fördröjningar än ett fast nätverk som kopplas upp via ett backbone?

- Det gäller dels den trådlösa kommunikationen och men även uppkoppling mot fasta nätstrukturer, särskilt sådana som normalt används i andra nätverk (Internet etc.)

- Vad innebär ”Sömlös Kommunikation" för Er?

- Är det möjligt att i ett integrerat nätverk ha med moderna sensorer och sådana ur ”arvet”?

- Vilken verksamhet bedriver Ni inom Ad hoc-nätområdet?

- Genomförs någon framtidsinriktad kunskapsuppbyggning knutet till ad hoc-nätverk?

Intervju angående nätverk, sensorer och bekämpningssystem

Anders Hyllander
Amfibiekårens Stridsskola och deltagare i Artilleridemonstrator-projektet
Datum: 2002-09-20

Finns det en ny allmän syn på principer som rör bekämpningsystem inom mobila nätverk med sensorer, i och med att både armén och fd. kustartilleriet (nuv. amfibiekåren) ingår i artdemo-projektet?

Armén har i alla tider enbart utnyttjat bäring och avstånd för lägesangivning för att sedan omsätta det till en fix punkt i ett koordinatsystem vid bekämpning av markmål.Kustartilleriet har även utnyttjat bäring - avstånd men framför allt använt värdena för beräkning av mållägets Vx - Vy. D.v.s. de rörliga sjömålens vinkelhastighet har varit huvudnumret. Denna förmåga har sedan även omsatts till markmålsfallet.Inom ramen för artdemo-projektet har nu även armén fått upp ögonen för rörligt mål och då på land, i form av ex.vis. fordonskolonner och enskilda stridsvagnar eller andra fordon som inte har extrema farter (> 70-80 km/h) eller är för små (målyta < 10 m^2). Detta har medfört att helt nya typer av sensorer och krav på dessa har kommit fram inom bekämpningsgenren.

På vilket sätt har detta utmynnat i en ny syn på sensorer och deras utnyttjande?

Sensortaktik börjar därmed även bli intressant i armén, framförallt för att kunna följa rörliga mål. Det handlar då inte bara om att en sensor skall kunna beräkna vinkelhastigheten utan ett helt nytt tänk med sensorer som kan utnyttjas taktiskt på olika sätt inom ramen för en nätverkslösning. Detta medför även att sensortaktiken måste utvecklas. En större flexibilitet än dagens systemlösningar kan erhållas om flera sensorer från flera olika delar av spektrumet kan kombineras.

Bearbetning av sensordata – skall bearbetningsprocessen utföras vid sensorn eller högre upp i nätverkshierarkin, eller rent av vid vapnet? För och nackdelar.

Flera sensorer i olika våglängdsområden har varit integrerade i en och samma plattform fram till dagens sensorsystemlösningar. Men i framtiden behöver det inte bara vara aktiva sensorer. Det kan lika gärna vara passiva optroniska sensorer. Det viktiga är dock att de kan samordnas i gemensamma nätverk.

Enligt Anders Hyllander är inte ordet "sensor" det mest lämpliga för att beskriva en sådan konstellation. För de mer initierade i sensorbegreppet är frågan kanske inte given men för de flesta handlar det dock om att tänka sig att till och med en kikare är en sensor. Ett typiskt exempel är arméns nya eldobservationsinstrument (EOI) som bygger på principen med en vanlig kikare integrerad med en enkel avståndsmätare. Många har svårt att ta begreppet sensor i sin mun för att beskriva denna produkt. Med begreppet sensor ser de istället framför sig ett stort komplext radarsystem. Dock är det

inte lätt att finna något annat begrepp som skulle kunna ge en liknande heltäckande beskrivning av företeelsen som ordet sensor gör.

Var skall mållägesberäkningen ske?

Enligt ett synsätt skall målberäkningen *inte* ske i varje sensor eller vapen plattform. Orsaken till det är att felen kan öka om beräkningarna genomförs på flera platser. Fusioneringen får m.a.o. en bättre kvalitet om den baseras på opåverkad data. Man erhåller en allt större felberäkningsfaktor om beräkningarna utförs på flera ställen. En mer centraliserad beräkningsfunktion är att föredra om felberäkningsfaktorn skall hållas nere för att nå en bättre kvalité i måldatafusioneringen.

Ett annat synsätt är att det är viktigt att generera en fusionerad mållägesinformation som inte innehåller för stora datamängder vid sensorn. Främst för att hålla ner den mängd datainformation som skall överföras.

Ser man någon utvecklingstrend inom radarsensorområdet?

Det kan handla om 2D-radar versus 3D-radar. 3D-radarn kan ge en något längre beräkningstid p.g.a. sin digitala gruppantenn med adaptiva antennelement. För att öka noggrannheten hos en 2D-radar kan den istället kompletteras med en Doppler-funktion.

Vilka nya tendenser och trender finns inom bekämpningsfunktionen?

”Net fire” – på svenska ”eld pall”, det handlar om autonoma utplacerade eldgivnings-enheter, som är anslutna i nätverket och skjuter på i nätet erhållna positioner. Systemet behöver inte någon specifik personal för betjäning utan endast bevakningsbemanning om hotbilden kräver det.

Är det möjligt att i ett integrerat nätverk ha med moderna sensorer och sådana ur ”arvet”?

Så länge arvets system är kompatibelt och möjligt att integrera i de nya nätverken finns inga konflikter. Tvärtom kan en ökning av antalet sensorer i ett inledande skede bara vara bra för fusioneringsprocessen. Dock är framtidens sensorer rationellt bättre mot bakgrund av att de får mer smygegenskaper eller rent av är passiva, de kräver mindre personal och är mer kompatibla i nätverksstriden vilket skulle tala för att det är bättre att i första hand satsa på det nya både vad gäller sensorer och vapen än att fastna i kostsamma omkonfigureringar för att nå kompatibilitet.

Samtal angående sensorutveckling, nätverk mm

Johan Andersson och Ola Stensby
Ericsson Microwave Systems
Datum: 2002-10-03

Hur skall sensorer styras?

Det handlar inte enbart om att ha en förmåga att maskinellt styra enskilda sensorer utan också om att säkerställa täckning.
Det kan åstadkommas dynamiskt inom ett nätverk med autonoma sensorer som ändå kan styras in mot vissa riktningar eller ett visst område. Allt beroende på den funktionalitet som de olika sensorerna har. Här kommer ex.vis. de digitala gruppantennerna (DGA) tillpass i radarlösningar, med sin flexibilitet i att kunna styra loberna.

Andra funktioner som kommer att bli generella i moderna radarlösningar är identitets- och positionsfunktioner (ID/Pos). Mjukvarumässigt kan sedan nätverket erbjuda en mängd nya funktioner som baseras på sensordata, ex.vis. stridsvärdessammanställning, gemensam fusionerad mållägesbild och sensorledning.

Trender inom sensorområdet?

DGA, bistatisk radar och multistatiska-radarnätverk är tekniker som kan vinna gehör i framtiden.

DGA – den digitala tekniken medger att ett antal enskilda sändare och mottagare kan styras och att man därmed kan sända ut en bred lob och ta emot signalen med flera smala lober i intressanta riktningar. Denna radar är därmed även svårare att störa än andra.
Bistatisk – radar där sändaren och mottagaren står på olika ställen.
Multistatisk – radar med en eller flera sändare och flera mottagare.

Teknikerna är inte nya men det framtiden innebär för bistatisk och multistatisk radar är att de kombineras med de aktiva digitala gruppantennerna tillsammans med digitalsignalbehandling. Det ger en flerfunktionsradar som har optimal prestanda i olika önskade riktningar. Även räckvidd och noggrannhet samt möjligheter för bättre signalskydd och styrning förbättras.

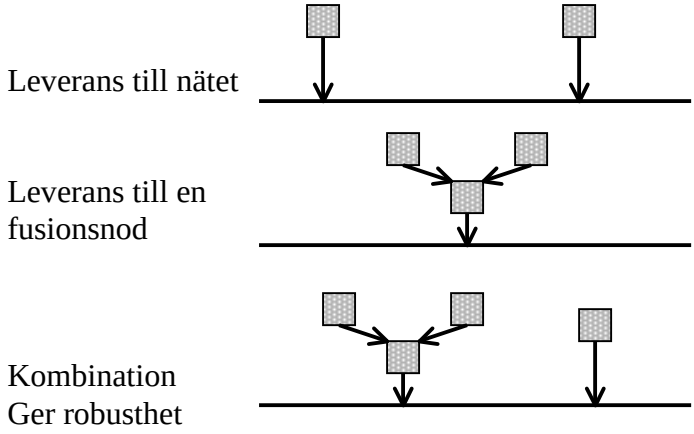
Koncepten bygger på nätverk i och med att sensorerna skall samverka på olika sätt. Det innebär att varje enskild flerfunktionsradar mäter och att samverkan sker när mätdata fusioneras samt genom att mätresurserna för radarsensorerna styrs och fördelas.

Samverkan mellan många sensorer används som multistatisk radar med sändare och mottagare på olika platser. Avståndet mellan sensorerna kan i stort vara det samma som mellan målen. Sändare och mottagare kan befinna sig på marken, på ett fordon eller på ett fartyg. En klar fördel är att hot från signalsökande robotar och störsändning minskar med en sändare i skyddad gruppering och mottagare framgrupperade. Det ger också ökad flexibilitet när det gäller geometrin för radarns sändare och mot-

tagare mot smyganpassade mål. Det finns därmed möjligheter att följa smyganpassade mål beroende på att radarvågen inte måste reflekteras tillbaka till en samlokaliserad sänd/mottagare.

Hur ser EMW på multisensordatafusion?

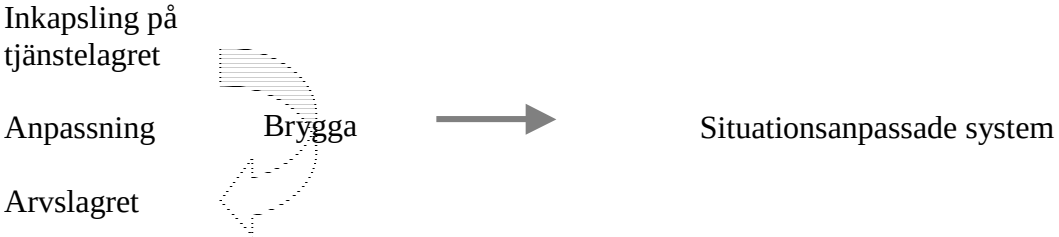
Det är i vissa stycken en förutsättning för att kunna gå vidare med de ovan nämnda teknikerna med bi- och multistatisk radar och erhålla en sensorfusion inom ramen för ett sensornät. Sensorintegration leder därmed fram till en sensorfusion inom sensornätet.
Ett antal olika principiella sätt att uppnå sensorfusion kan utkristalliseras.
Det handlar om olika ”samverkansätt” i nätverk.



Figur Multisensordatafusion

Fusioneringen baseras även på den sensorstyrning/sensorledning som utverkas i nätverken.

En förutsättning för sensorfusionen är att informationen som skall förmedlas ”paketeras” på ett relevant sätt. Det krävs inkapsling på tjänstelagret som svara mot behoven att få fram informationen tillräckligt snabbt.



Figur Brygga

Bryggan används för att koppla ihop två segment av ett LAN. Bryggan filtrerar paket och vidarebefordrar endast de paket som skall till en nod ”på andra sidan”. Detta resulterar i en funktion som är väsentlig i ad hoc-nätverksstrukturen, nämligen att minska den totala trafiken på nätet. Bryggan arbetar på andra lagret i OSI-modellen.

EMW:s syn på NBF?

Realtidskrav i TCP/IP-nät ökar kontinuerligt. Tal på IP är en kommersiell tjänst som driver på de kvalitetsmässiga krav man kan ställa på dataöverföringar. Än är inte den teknologin så långt driven att den erbjuder en kvalitetsmässig vinst. Nivån ligger vid ca. 0.25 s för att människan inte skall uppfatta fördröjningen.
Den gemensamma nätverksarkitekturen är dock en förutsättning för att nå någon vart med ett nätverkscentrerat försvar.

Ad hoc-nätverk, är det ett koncept som ligger i EMW:s intresse att driva?

Ad hoc-nätverk är definitivt ett teknikområde som i princip är en förutsättning för att de sensorer som är installerade i autonoma plattformar skall kunna uppträda taktiskt men ändå ständigt kan vara en del i nätverket. Det krävs en kontinuerligt uppkopplad datalänk för att kunna bidra med sensordata i de bi- och multistatiska radarsystemen och skapa de tidigare nämnda tjänsterna. Ad hoc-nätverken kräver en mjukvarustyrd taktisk radio så som exempelvis USA:s JTRS radiokoncept. Radiokonceptet jobbar inte EMW med, men dock har man dotterbolag som arbetar med både hård- och mjukvaruprodukter till ad hoc-nät samt framförallt integrationen av sensorerna i nätverket.

Intervju angående ad hoc-nätverk

Katarina Persson och Jimmi Grönkvist
Avdelningen för sensorteknik, FOI, Linköping
Datum: 2002-10-30

Vad representerar begreppet ad hoc i nätverkssammanhanget?

Ad hoc, latin och betyder ”för detta ändamål” – i detta sammanhang anger det att något är improviserat. Det skall tolkas som att ett ad hoc-nät är ett nät som förändras kontinuerligt och anpassas till terrängen och situationen.

Som en grund för resonemanget kring ad hoc-nät är det nödvändigt att titta närmare på det protokollsystem som nästan alla maskinvaru- och programvaruplattformar använder idag och som också utgör stommen i Internet.

Informationen som sänds över ett nät måste behandlas och tolkas. Idag används ett antal protokoll som tar hand om data för att få fram den information man är ute efter. Man kan jämföra protokollen med en samling regler för hur data ska tas om hand. Protokollen har olika ansvarsområden och egenskaper, t.ex. adressering och kodning. De delas upp i olika lager. Två av de vanligaste protokollen är TCP och IP, de verkar i två skilda lager – i den sk. protokollstacken. Överföringsprotokollet ATM kan sägas befinna sig på länknivån med dragning mot routing på nätlagret.

TCP/IP-stacken började utvecklas under 60-talet och har idag nått långt över förväntningarna. En stadig utveckling och förnyelse av protokollen har skett under åren. Viktigt är att förstå hur protokollstackens funktioner och egenskaper passar in i nya nätarkitekturerna som ad hoc-nät. Protokollstacken har fyra lager eller nivåer som kommunicerar uppåt och neråt samt med motsvarande lager i andra plattformar.

Hur utvecklad är ad hoc-nätverksteknologin?

Ad hoc-nätverk är inte färdigdefinierat inom IEEE (står för Institute of Electrial and Electronics Enginers och är en organisation som bl.a. arbetar med att standardisera kommunikationsprotokoll). Det finns dock finns de facto-standarder som bär framåt på vägen mot en mer renodlad standard.

En sådan standard är den som omfattar WLAN, IEEE 802.11. Den är den hittills mest förekommande i ad hoc-nätverkslösningar, men har dock ingen utvecklad QoS. D.v.s. hur skall kapacitet reserveras på en länk. Det går relativt bra i ett fast nät där påverkan mellan länkar saknas. Köhanteringen kan då sköta det hela genom att skicka prioriterade paket först. Detta är dock ett större problem i radionät där andra sändande noder ger interferenser. Det är svårt för en nod att veta när prioriterade paket finns i grannoderna. Någon form av reservation av kanalen blir nödvändig, d.v.s. man behöver ett QoS-garanterande MAC-protokoll.

Det finns MAC-protokoll som skulle kunna ge den möjligheten till exempel TDMA-baserade MAC-protokoll, men det allmänt mest förekommande är standarden som jobbar med CSMA/CA. Det är ett exempel på dynamisk tilldelning av kanalen. Den standarden ger idag dock inga QoS möjligheter. Det finns inte heller idag några enkla tillägg för att hantera QoS. RTS/CTS (request-/clear to send) är i så fall en antydan till QoS.

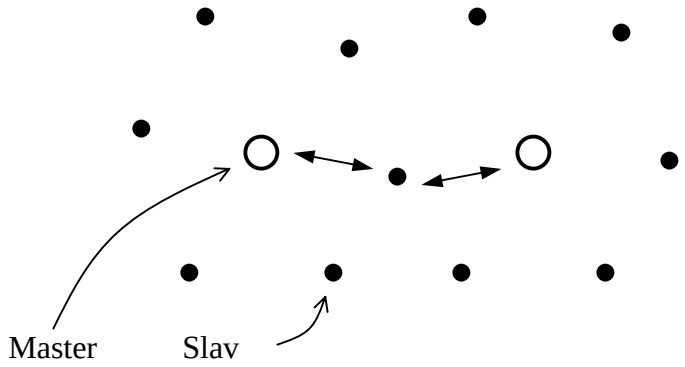
Vilken kvalitet och säkerhet finns i ad hoc-nätverk?

QoS i Internet utvecklas allteftersom. Internet Engineering Task Force (IEFT) ansvarar för standardisering och utveckling av de protokoll som används över Internet. I och med att de taktiska näten använder Internet Protocol (IP) är det intressant att studera de protokoll som rör QoS. Det är främst IntServ och DiffServ samt MPLS. IntServ karaktäriseras av resursreservering, vilket innebär att resurser reserveras längs den väg realtidsdarta skall sändas. I DiffServ skapas olika prioritets klasser som hanteras olika. MPLS använder sig också av prioritering utav paketen som märks med olika etiketter. Etiketterna kan också användas för att snabbt hitta vägar och tunnla paketen.

Har bluetooth en status som ad hoc-nät?

Bluetooth är ej något ad hoc-nät i och med att det bygger på en master-enhet och upp till sju stycken slav-enheter, med andra ord är det ett cellulärt nät. Systemet använder sig av bandspridning genom frekvenshopp. Bluetooth använder ISM-bandet (Industrial, Scientific and Medical) 2,4000 – 2,4835 GHz, som är licensfritt och används av diverse hemelektronik. Ur ISM-bandet nyttjas 80 MHz, som är uppdelat i 1 MHz kanaler. Principen bygger på att sändning sker på frekvensen under 625 µs och hoppar sen till nästa frekvens. Överföringshastigheten blir 1 Mbit/s.

Det finns dock ett mellanting, sk. scater nets där två olika piconät kopplas samman. En master-slav-master uppkoppling är då upprättad. Dock har denna lösning inte ad hoc-nätets flexibilitet.



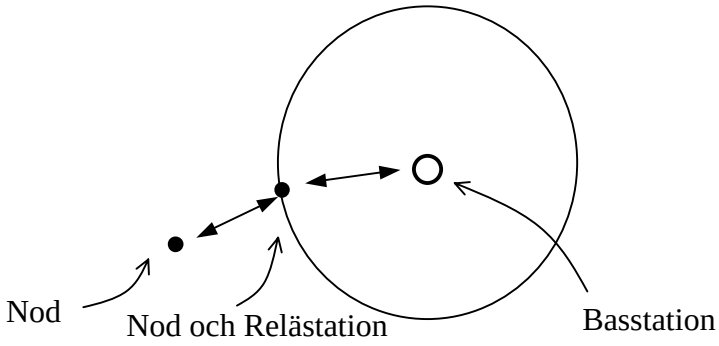
Figur Scatter net

Vilka andra principer finns för ad hoc-nätverkslösningar?

Istället för WLAN standarden IEEE 802.11 kan TDMA scheduling användas. Det innebär att man delar in tiden i periodiskt återkommande intervall då en sändare får

utnyttja hela det disponibla frekvensutrymmet. Rockwell Collins utvecklar en enklare aplikation som utnyttjar TDMA, en sk. soldier phone. Inte en renodlad ad hoc-nätverkslösning men dock en ansats.

ODMA – oportunity driven multiple access, är ett multi-hopp reläprotokoll som utnyttjas i cellulära lösningar. Principiellt bygger det på att man utnyttjar andra mobila stationer/slavar för att nå in i basstationens täckningsområde. ODMA övervägdes som en standard för 3G men bedöms bli för komplex beroende framförallt på hur debitering skulle ske samt omognaden vad gäller att ”låna ut” sin mobiltelefon för andras trafik. I vilket fall som helst är ODMA en attraktiv lösning för framtida mobila kommunikationssystem beroende på fördelarna med reducerad signalstyrka och ökad täckning samt bättre QoS.



Figur ODMA, reläprotokoll

Vilka utmaningar står ad hoc-nätverken inför för att kunna realiseras i framtiden?

Att lösa QoS-problemen är ett måste. Problem eller trånga sektorer måste lösas på alla nivåer i protokollstacken. Och det finns problem inte bara på transportlagret med TCP men även på nätlagret med IP och routing samt på länklagret med MAC.

Vilka routingprinciper är mest adekvata för ad hoc-nätverk?

Det finns två övergripande principer för ”routing”:

- *Proaktiva routingprotokoll* – kontinuerlig uppdatering av rutter, när en rutt behövs finns den tillgänglig omedelbart. Det kräver en stor apparat för hantering av alla rutterna. Denna lösning slösar med kanalresurserna eftersom den kräver en stor overhead.

- *Reaktiva routingprotokoll* – rutter skapas endast då de behövs. Detta spar minnesutrymme och beräkningskapacitet. Tiden för upprättande av rutt blir längre än för den proaktiva routingmetoden, eftersom den innebär att nätet avsöks globalt för att hitta en rutt, vilket ger långsamma rutter.

Routingalgoritmerna Ad hoc On Demand Vector (AODV) och Dynamic Source Routing (DSR) är ej gjorda för nära realtidslösningar. Algoritmerna utgör basen i två proaktiva protokoll med samma namn?

Finns det några ytterligare trender som rör realtidsapplikationer?

– mycket svårt att säga något ytterligare om trenden men en stadigt ökande forskning bedrivs i USA och främst med understöd från DARPA, vilket innebär att provbänkslösningar eller demonstratorer börjar visas. En annan aspekt är att frågor kring säkerhet och adressering också måste lyftas fram för att ytterligare höja QoS i ad hoc-nätverk.

En följd är att Ad hoc inte är kommersiellt drivet vilket beror på att man inte sett några tänkbara civila lösningar eller applikationer för ad hoc-nätverk ännu.

En fråga om tidsfaktorer.
Det handlar om man kan göra någon generell tidsjämförelse mellan paketförmedlade förbindelser och kretskopplade förbindelser. Eller är det så att det är där QoS funktionerna kommer in och ger olika kvalitetsnivåer på den paketförmedlade förbindelsen?

När det gäller den kretskopplade överföringen att har man access till den och därmed är fördröjningen känd och den varierar inte övertiden, vilket medför att prestanda kan garanteras. Detta är inget man kan göra i en paketförmedlad förbindelse i och med att alla användare har tillgång till nätet och fördröjningen varierar.
Därmed också bättre att tala om mer eller mindre fördröjning än att tala i termer om mer eller mindre nära realtid i syfte att vara mer precis kring vilken tidsfördröjning det rör sig om. Men visst kan man ha en fast eller dynamisk tilldelning med låg eller hög fördröjning även på ad hoc-nät.

Det är i och för sig svårt att göra en generell uppskattning av skillnaderna i fördröjning mellan paket- och kretskopplade förbindelser!

Med den kretskopplade förbindelsen har man tillgång till resurserna hela tiden och kan därmed ha en nästan konstant fördröjning. Hur stor den är beror på uppkopplingen – avstånd, kapacitet etc.

I den paketförmedlade förbindelserna har man normalt inte tillgång till resurserna hela tiden. Paketen kan skickas olika vägar mellan sändare och mottagare och är beroende av annan trafik i nätet och därmed kan fördröjningen variera mycket. Om man t.ex. ska spela musik eller se på video eller dyl. via paketförmedlad förbindelse kan man buffra paketen hos mottagaren och sända dem med en konstant fördröjning. Fördröjningen kan då bli hög men applikationen blir inte "hackig". QoS-protokollen används här för att kunna ge garantier även på denna trafik. Vi kan t.ex. reservera resurser eller låta våra paket få så hög prioritet att realtidsapplikationer kan användas.

Om man kan uppnå något realtidskrav beror på applikation och förbindelsens kapacitet och man kan tyvärr inte dra någon generell slutsats. Man kan ha lång/kort fördröjning i båda fallen. I ad hoc-nät kan man ha fast eller dynamisk tilldelning av resurser, t.ex. CSMA/TDMA. CSMA (dynamiskt) kan t.ex. fungera bra i ett nät med lite trafik men är det för hög trafik kan det bli för mycket "krockar" och ineffektivt. TDMA (fast) däremot är bra om man har mycket trafik i ett nät men är det låg trafik finns risken att inte resurserna utnyttjas och man får onödigt hög fördröjning.

Samtal angående FMV:s syn på ad hoc-nätverk

Torbjörn Ericsson, Ralph Persson
Kompetenscentrum Sensor & Telekom, FMV

Datum: 2002-11-12

Vilken verksamhet har FMV inom Ad hoc-nätområdet?

Området är aktuellt och verksamhet bedrivs på många håll både inom den kommersiella världen och i olika försvarsmakter.

Man måste vara på sin vakt vid användandet av begreppet ad hoc. Det används med olika betydelser, eller åtminstone olika förväntningar på funktionaliteten, i olika användningsområden. T ex används det för den automatiska etableringen av ett nät av fast utplacerade marksensorer likväl som för den dynamiska självupprättande och självläkande funktionen hos ett nät av noder som rör sig i terrängen. Det senare är den innebörd på begreppet som bör gälla. Lösningarna på dessa båda problem ser olika ut, främst beroende på tidskonstanterna i det rörliga nätet, vilket förmodligen är nära besläktat med din kärnfråga.

Genomför FMV någon framtidsinriktad kunskapsuppbyggnad knutet till ad hoc-nätverk?

FMV genomför en kunskapsuppbyggande framtidsinriktad verksamhet benämnd FFTK, Försvarets Framtida Taktiska Kommunikation. En av de uppgifter vi har inom denna är att före utgången av 2003 för FM demonstrera dynamiska adaptiva nät. För ändamålet har vi engagerat Rockwell Collins i en studie, Tactical Battlefield Networking and Software Radio, som kommer att avslutas med en demo nästa höst. Jag tror att du där kan finna svar på många av dina frågor. Rockwell genomför parallellt med vår studie en vida mer omfattande verksamhet, MOSAIC, på uppdrag av US Army CECOM, som vi har indirekt stor nytta av.

Har FMV något specifikt arbete på gång inom området "Sömlös Kommunikation"?

LedsystT har ansvar för "Sömlös Kommunikation".
Begreppet sömlöshet används i samband med mobila trådlösa nätverk. Det man syftar på är en sömlös yttäckning som består av ett stort antal trådlösa överlappande nät, sammanbundna av kommersiella och försvarsunika kärnnät. Sömlösheten består därmed inte av ad hoc-nät i sig. Utan det handlar mer om helheten, det nätverksbaserade försvaret med sin kombination av fast infrastruktur och trådlösa mobila nätverk.