

Prediktering av fiendeintention, baserat på bayesiansk hypotesprövning

Fredrik Johansson

Prediktering av fiendeintention, baserat på bayesiansk hypotesprövning

Examensrapport inlämnad av Fredrik Johansson till Högskolan i Skövde, för Magisterexamen (M.Sc.) vid Institutionen för kommunikation och information.

2005-06-06

Härmed intygas att allt material i denna rapport, vilket inte är mitt eget, har blivit tydligt identifierat och att inget material är inkluderat som tidigare använts för erhållande av annan examen.

Signerat: _____

Handledare för examensarbetet: Mikael Johannesson

Prediktering av fiendeintention, baserat på bayesiansk hypotesprövning

Fredrik Johansson

Sammanfattning

I detta arbete beskrivs hur den bayesianska metodiken kan användas för att stödja en militär beslutsfattare, då denne ska fatta beslut under osäkerhet. Genom att analysera vilka parametrar som kan användas för att prediktera fiendens intentioner, tas ett bayesianskt nätverk fram, vilket implementeras och integreras i simuleringsramverket GTSIM. För att möjliggöra denna prediktering har extra funktionalitet lagts till i GTSIM, såsom att skapa olika typer av mål. Dessa mål kan sättas ut på valfria platser och senare läsas in då en fusionerad lägesbild skapas av de olika sensorer som placerats ut. Målen representerar då de olika handlingsalternativ som en simulerad fiendestyrka har, och allteftersom fiendestyrkan rör sig uppdateras sannolikheten för att de olika målen ska anfallas av den framtagna modellen. En utvärdering av den framtagna modellen och det utvecklade verktyget har gjorts, samt så har förslag på hur modellen kan utvecklas i framtiden tagits fram.

Nyckelord: Bayesiansk hypotesprövning, bayesianska nätverk, beslutsstöd, hotanalys, informationsfusion, situationsanalys

Innehållsförteckning

1	Introduktion	1
2	Bakgrund	3
2.1	Beslutsfattande.....	3
2.1.1	Beslutsteorier.....	4
2.1.2	Sannolikhetslära.....	4
2.1.3	Beslut under osäkerhet.....	5
2.1.4	Metoder för beslut under osäkerhet.....	5
2.2	Bayesiansk metodik.....	6
2.2.1	Matematiska regler inom den bayesianska metodiken.....	6
2.2.2	Bayesiansk beslutsteori.....	7
2.2.3	Bayesiansk hypotesprövning.....	9
2.3	Informationsfusion.....	10
2.3.1	Situationsanalys.....	10
2.3.2	Hotanalys.....	11
2.3.3	Adaption.....	12
3	Problem	13
3.1	Problembeskrivning.....	13
3.2	Problemprecisering.....	14
3.3	Avgränsningar.....	14
4	Metod	16
4.1	Identifiera parametrar.....	16
4.2	Implementation av modellen och det grafiska gränssnittet.....	17
4.3	Utvärdering av modellen och det framtagna verktyget för datainsamling.....	18
5	Genomförande och resultat	19
5.1	Bayesianska nätverk.....	19
5.1.1	Konstruktion av bayesianska nätverk.....	20
5.2	Framtagande av parametrar/noder.....	23
5.2.1	Intervju med officer från Markstridsskolan.....	25
5.2.2	Samtal med representant från Ericsson Microwave Systems.....	25
5.2.3	Parametrar som valts ut att tas med i modellen.....	25
5.3	Implementation av modellen i GTSIM.....	27
5.3.1	ScenarioGenerator.....	27

5.3.2	VehiclePackage	28
5.3.3	SensorPackage.....	28
5.3.4	PresentationPackage.....	28
5.3.5	BayInferencePackage.....	30
5.4	Utvärdering av modellen	35
5.4.1	Utvärdering av den framtagna modellen.....	36
5.4.2	Utvärdering av det framtagna verktyget.....	37
5.5	Finjustering av modellen	37
5.5.1	Identifiering av lämpliga ändringar.....	38
6	Relaterat arbete	39
6.1	Enhanced Situation Awareness using Random Particles.....	39
6.2	Representation and Recognition of Uncertain Enemy Policies Using Statistical Models	39
7	Slutsatser	41
7.1	Modellen	41
7.2	Det grafiska verktyget.....	42
7.3	Förslag på framtida arbete	43
	Tack.....	44
	Referenslista	45

1 Introduktion

Högteknologiska väpnade styrkor runt om i hela världen är på väg in i ett stort förändringsskede, kallat för *Revolution in Military Affairs* (Arnborg, Artman, Brynielsson och Wallenius, 2000). I Sverige har en förändrad hotbild tillsammans med den snabba teknologiska utvecklingen lett till att det framtida försvaret ser ut på ett helt annat sätt än det gamla invasionsförsvaret (Hållmats, 2002). Detta framtida försvar brukar inom den svenska militären kallas för det nätverksbaserade försvaret och kan ses som en övergång mot ”informationsåldern” inom försvaret. Förändringarna för med sig att mängden insamlad data hela tiden ökar, vilket innebär en ökad komplexitet och arbetsbörda för de militära beslutsfattarna, vilket i sin tur för med sig ett ökat behov av effektiva beslutsstödsystem (Westberg, 2001). I och med detta har informationsfusion, vilket handlar om att beskriva ett specifikt tillstånd i världen genom att använda tillgänglig information på bästa möjliga sätt (Suzić, 2003a), kommit att spela en allt viktigare roll.

Inom informationsfusion har forskningen tidigare fokuserat på problem med en låg abstraktionsnivå, såsom att slå samman sensordata eller att identifiera olika fordon (Brynielsson och Arnborg, 2005). Nästa steg i informationsfusionsprocessen ligger dock på en högre abstraktionsnivå, då det gäller att förutsäga fiendens handlingar och utifrån detta föreslå olika handlingsalternativ (Brynielsson och Arnborg, 2005). För att lyckas med detta krävs att det finns möjlighet att resonera och fatta beslut under osäkra förhållanden. Ett sätt som kan användas för att fatta beslut under osäkerhet är den bayesianska metodiken, eftersom den ger möjlighet att beräkna sannolikheten för olika hypoteser givet viss data och förhandsinformation genom användandet av Bayes teorem. Bayesiansk metodik bygger dock på användandet av subjektiva prior-sannolikheter, vilket ifrågasätts av vissa forskare (se vidare Davies Withers 2002). Den bayesianska metodiken kommer i detta arbete att användas för att undersöka möjligheten att bygga en modell som kan beräkna sannolikheterna för fiendens olika handlingsalternativ inom området markstrid. Utöver detta kommer även denna modell förses med ett grafiskt gränssnitt för att användaren ska kunna se situationsutvecklingen och på så sätt få större förtroende för modellens utdata. Detta grafiska gränssnitt är även tänkt som ett verktyg för att samla in data om hur mänskliga experter skulle skatta sannolikheterna i olika scenarion. Denna insamlade data kan exempelvis användas för att finjustera den framtagna modellen.

I kapitel 2 (bakgrund) görs en genomgång av grundläggande sannolikhetslära, hur beslutsfattandeprocessen fungerar, samt så diskuteras ett antal olika metoder för beslut under osäkerhet. Därpå beskrivs den bayesianska metodiken i mer detalj, med fokus på bayesiansk hypotesprövning. Sist i kapitlet diskuteras informationsfusion och hur den bayesianska metodiken kan användas för att genomföra situations- och hotanalys, vilka är viktiga steg inom informationsfusionsprocessen.

Kapitel 3 (problem) snävar av det problemområde som presenterats i föregående kapitel och preciserar det valda problemet samt de avgränsningar som gjorts. Dessutom presenteras ett antal delmål, vilka ska uppnås för att det övergripande målet med arbetet ska gå att nå. Utifrån dessa delmål tas i kapitel 4 (metod) ett antal olika alternativa metodförslag fram, vilka representerar olika sätt att nå de olika delmålen på. De olika metodernas för- och nackdelar ställs emot varandra för att på så sätt få fram vilka metoder som är de lämpligaste för de olika delmålen.

Nästföljande kapitel (genomförande och resultat) beskriver vad bayesianska nätverk är, hur de konstrueras, samt hur inferenser dras i nätverken. Därpå tas de noder fram

Introduktion

som ska ingå i det bayesianska nätverk som beräknar sannolikheten för fiendens olika handlingsalternativ. Efter detta presenteras GTSIM, vilket är ett simuleringsramverk utvecklat av Ericsson Microwave Systems, samt hur den framtagna modellen har integreras i GTSIM. Sist i kapitlet beskrivs också hur implementationen av den framtagna modellen utvärderas, dels när det gäller hur bra dess prediktering fungerar, och dels hur väl verktyget kan användas för att samla in data som kan förbättra modellen.

Kapitel 6 (relaterat arbete) positionerar detta arbete i förhållande till de närbesläktade arbeten som redan finns inom det aktuella problemområdet. Här tas likheter och skillnader upp mellan detta arbetes och de övriga arbetenas problemställningar och tillvägagångssätt, samt så identifieras de delar i de andra arbetena som i framtiden kan tillföra något till utvecklingen av detta arbete. Dessa utvecklingsförslag tas tillsammans med övriga förslag på framtida arbete upp i kapitel 7 (slutsatser). Utöver olika förslag på framtida arbete görs i detta sista kapitel även en sammanfattning av de resultat och erfarenheter som erhållits i samband med detta arbete.

2 Bakgrund

I detta kapitel beskrivs beslutsfattande i stort, för att sedan leda in på en mer detaljerad beskrivning av beslutsfattande under osäkerhet. En noggrann redogörelse görs över den bayesianska metodiken, varpå slutligen en introduktion till ämnet informationsfusion görs, vilket är tänkt att minska graden av osäkerhet vid beslutsfattande.

2.1 Beslutsfattande

Beslutsfattande kan ses som processen att av en mängd möjliga alternativ välja det alternativ som med störst sannolikhet leder till önskat resultat (Balasubramanian, Nochur, Henderson och Millie Kwan, 1999). Beslutsfattandeprocessen består generellt av fyra olika steg: problemdefinition, identifiering av möjliga lösningar, val av alternativ samt en beslutsimplementationsplan (Borges, Pino och Valle, 2005). Generellt sett drivs allt beslutsfattande av ett mål (Balasubramanian et al., 1999). När ett beslut ska fattas är det ofta till hjälp att bryta ner beslutsproblemet i mindre delar, i syfte att visualisera beslutssituationens komplexitet (Westberg, 2001). Enligt Raiffa (1968) är de viktigaste delarna av beslutsfattande följande:

- Kunskap om omgivningen: För att kunna välja vilken handling som ska utföras är det till stor fördel om omgivningen är känd. Exempelvis kan en militär beslutsfattare genom kunskap om terrängen utnyttja dess möjligheter till naturligt skydd, till exempel genom att välja att gå i försvar i kuperad terräng istället för i öppen terräng, för att därigenom försvåra för anfallaren.
- Möjliga handlingsalternativ: Givet vad som är känt om omgivningen existerar olika handlingsalternativ som kan väljas för att uppnå det önskade målet. Om den militäre beslutsfattaren får information om att fienden befinner sig alldeles i närheten kan två möjliga handlingsalternativ till exempel vara att gå till anfall eller att retirera.
- Konsekvenser för olika handlingsalternativ: Olika handlingsalternativ för med sig olika konsekvenser, även om det ofta är omöjligt att förutsäga alla olika konsekvenser av en handling i förväg. En möjlig konsekvens av att ett överraskningsanfall skulle kunna vara att fienden överrumplas och kan nedkämpas med minimala egna förluster.
- Sannolikheter för olika konsekvenser: Olika konsekvenser kan vara mer eller mindre sannolika. Exempelvis kan sannolikheten för ett lyckat överraskningsanfall uppskattas till 0.7 om det finns relativt stora möjligheter att lyckas.
- Nyttan för olika konsekvenser: Detta avser hur mycket det är värt att en viss konsekvens inträffar. Nyttan av att nedkämpa ett fiendeförband skulle kunna vara att en viktig anläggning skyddas, medan ett misslyckat anfall skulle kunna leda till den negativa nyttan av att förlora anläggningen samt att förlora ett stort antal soldater.
- Kostnad för att få bättre information: Ofta kan bättre information fås om omgivningen, de olika handlingsalternativen, sannolikheterna, och så vidare. I det militära exemplet kanske beslutsfattaren beslutar att riskera att röja sina egna styrkors position för att via radarsändning få reda på fiendens exakta position.

2.1.1 Beslutsteorier

Det finns många olika teorier om hur beslutsfattande ska gå till, men gemensamt för dem alla är att de kan klassificeras som antingen normativa eller deskriptiva. De normativa teorierna anger hur en beslutsfattare *bör* fatta beslut på ett rationellt sätt medan de deskriptiva teorierna beskriver hur beslutsfattare *faktiskt* fattar beslut (Wallenius, 2004b).

Ett av de äldsta exemplen i litteraturen på normativt beslutsfattande är då Aristoteles ger kloka råd till en grekisk yngling som söker vägledning om hur han ska leva sitt liv. Aristoteles råd blir med modernt språkbruk att ynglingen själv ska ta reda på vad denne betraktar som ett gott liv, undersöka de troliga konsekvenserna av de olika sätten att leva detta liv på, samt att välja det alternativ som med störst sannolikhet leder till ett gott liv. Även om rådet sett ur ett modernt vetenskapligt perspektiv är väldigt enkelt är kärnan i det ändå överensstämmande med modern beslutsteori (Wallenius, 2004b). Modern normativ beslutsteori handlar generellt sett om att av en mängd handlingar välja det alternativ som maximerar den förväntade nyttan (Jaynes, 2003).

Inom deskriptiv beslutsteori studeras istället de sociala eller psykologiska processerna av beslutsfattande (Wallenius, 2004b). Teorin om att maximera den förväntade nyttan är ofta inte tillräcklig för att förklara människors beteende, exempelvis tenderar små sannolikheter att överskattas medan stora sannolikheter ofta underskattas. Överhuvudtaget fattar människor väldigt ofta beslut som inte alls är särskilt rationella. Tversky och Kahneman visar i sin forskning att människor fattar beslut genom att använda sig av ett begränsat antal heuristiska principer, vilka ofta inte är rationellt grundade (Tversky och Kahneman, 1974). Kahneman och Tversky är två forskare som dessutom utarbetade den så kallade prospektteorin för att förklara hur människor fattar beslut under osäkerhet. Enligt Wallenius (2004b) bygger denna teori på att det finns ett starkt beroende mellan hur ett beslutsproblem presenteras och vilket beslut som väljs, det vill säga att sättet en beslutssituation presenteras på för en beslutsfattare i hög grad kan inverka på dennes beslut.

2.1.2 Sannolikhetslära

Inom sannolikhetslära finns det två alternativa sätt att se på sannolikheter, det klassisk-frekventistiska och det bayesianska (även kallat det subjektivistiska). Gemensamt för alla sannolikheteorier är det primära elementet *händelsen*. Med en händelse menas ett tillstånd i någon del av världen inom ett tidsintervall i det förgångna, nutiden eller framtiden (Heckerman, 1999). Inom klassisk-frekventistisk sannolikheteori ska sannolikheten för en händelse e tolkas som den relativa frekvensen som e inträffar med, när ett slumpexperiment med utfallen e och \bar{e} (inte e) upprepas ett stort antal gånger (Heckerman, 1999). En fördel med detta synsätt är att det i princip kan beskrivas som intersubjektivt, det vill säga att alla som observerar experimentet kan enas om en och samma sannolikhet. Nackdelen med det klassisk-frekventistiska synsättet är att i situationer där det inte går att upprepa experiment flera gånger så kan helt enkelt inga sannolikheter definieras. Anhängare av det bayesianska tankesättet hävdar dock att det i dessa situationer är rimligt att använda subjektiva sannolikheter (Heckerman, 1999). Inom den bayesianska sannolikheteorin tolkas sannolikheten för händelsen e på ett annat sätt än inom den klassisk-frekventistiska sannolikheteorin, närmare bestämt som att sannolikheten för e representerar ett mått på en persons övertygelse (*degree of belief*) om att händelsen

ska inträffa i ett enstaka experiment (Heckerman, 1999). En noggrannare beskrivning av den bayesianska metodiken kan hittas i kapitel 2.2.

2.1.3 Beslut under osäkerhet

Människors beteende i situationer där de relevanta sannolikheterna inte är kända eller där de är otillförlitliga, det vill säga beslut under osäkerhet, är av speciell karaktär. I allmänhet tenderar beslutsfattare vara mer benägna att ta risker i situationer där sannolikheten för olika utfall är känd, än där beslutsfaktorerna inte till fullo är kända (Tversky och Kahneman, 1974). Osäkerhet är ett problem som finns vid nästan alla typer av verkliga beslutssituationer. Enligt Raiffa (1968) kräver analys av ett beslutsproblem under osäkerhet följande steg:

1. Lista de genomförbara alternativen som är tillgängliga för informationsinsamlande och handlande.
2. Lista de händelser som har möjlighet att inträffa.
3. Ställ upp informationen som kan fås och valen som kan göras.
4. Bestäm hur tilltalande konsekvensen av de olika handlingsalternativen är.
5. Bedöm sannolikheten för att de olika osäkra händelserna kommer inträffa.

När dessa steg genomgåts kan en strategi utarbetas för att nå en lösning på problemet (Raiffa, 1968).

Som tidigare nämnts finns det många situationer som inbegriper beslutsfattande under osäkerhet, det finns dock vissa områden där osäkerheten är av kritisk betydelse. Ett exempel på detta är de situationer som militära beslutsfattare ställs inför. Förmåga att hantera osäkerhet är ofta väldigt avgörande för militära beslutsfattares framgång eller misslyckande (Jönsson, Neider, Schubert och Svensson, 1998; Das, 1999).

2.1.4 Metoder för beslut under osäkerhet

Sannolikhetsbaserade modeller har under en lång tid föredragits vid beslut under osäkerhet inom vetenskapsområden såsom fysik och ekonomi (Russel och Norvig, 2003). Detta är dock långtifrån den enda typen av metoder som existerar. Speciellt inom AI-området har flera olika alternativ till sannolikhetsteorin utvecklats (Russel och Norvig, 2003). Den sammanställning av metoder som presenteras här är på intet sätt heltäckande, men är tänkt att ge en överblick över några av de existerande metoderna:

- Bayesiansk sannolikhetsteori: Användandet av sannolikheter ger möjlighet att väga olika alternativ emot varandra baserat på hur troliga olika händelser är (Das, 1999). Den bayesianska sannolikheten för händelse x är ett mått på en persons övertygelse om att händelsen ska inträffa (Heckerman, 1999). En betydligt noggrannare redogörelse av den bayesianska metodiken återfinns i kapitel 2.2.
- Säkerhetsfaktorer: En enkel modell för osäkra resonemang baserade på regler är säkerhetsfaktorer, denna modell utvecklades för att användas tillsammans med expertsystemet MYCIN (Cruz och Beliakov, 1996). Cruz och Beliakov (1996) menar att säkerhetsfaktorer har många styrkor, medan bland andra Russel och Norvig (2003) hävdar att metoden inte kan rekommenderas då säkerhetsfaktorer kan ge väldigt felaktiga resultat vid en överskattning av tilltron till en hypotes.

- Dempster-Shafer: Dempster-Shaferteori är enligt Shafer (1990) en generalisering av den bayesianska sannolikhetsteorin. Istället för att beräkna sannolikheten för olika hypoteser beräknas inom Dempster-Shaferteori sannolikheten för att den tillgängliga informationen stödjer hypotesen. För en mer utförlig beskrivning av Dempster-Shaferteori hänvisas den intresserade läsaren till Shafer (1990).

Valet av metod är inte på något vis självklart, men som Das (1999) påpekar gör faktumet att den bayesianska metodiken bygger på en rigorös teori och är väl beprövad att den har en väsentlig fördel. Även Arnborg et al. (2000) hävdar att det faktum att den bayesianska metodiken visat sig framgångsfull i en rad olika applikationer är en anledning till att välja den framför andra. Exempel på ett antal lyckade applikationer ges bland annat av Chan och Darwiche (2002). Den metod som kommer att användas för beslut under osäkerhet i detta arbete är av ovanstående anledningar den bayesianska metodiken. I följande kapitel kommer därför en mer detaljerad beskrivning av den bayesianska metodiken att presenteras.

2.2 Bayesiansk metodik

Som tidigare nämnts bygger den bayesianska metodiken på användandet av subjektiva sannolikheter. Om en person tilldelar sannolikheten 1 till händelsen e innebär detta att personen tror att e med säkerhet kommer inträffa och sannolikheten 0 att e absolut inte kommer inträffa. En sannolikhet däremellan innebär att personen till en viss grad är osäker på huruvida e kommer inträffa eller ej. Givet den bayesianska tolkningen är sannolikheten alltså alltid beroende av kunskapsstillståndet hos den person som sätter sannolikheten. Därför skrivs sannolikheten för e som $p(e|\xi)$ vilket utläses som sannolikheten för e givet ξ (Heckerman, 1999). Symbolen ξ representerar då kunskapsstillståndet hos personen som sätter sannolikheten. Personen kan också sätta sannolikheten baserat på information som denne antar är sann. Sannolikheten för händelsen e_2 givet att händelsen e_1 är sann och personens bakgrundskunskap ξ skrivs $p(e_2|e_1, \xi)$ (Heckerman, 1999).

2.2.1 Matematiska regler inom den bayesianska metodiken

Det finns många olika regler inom bayesiansk sannolikhetsteori. Två enkla regler, vilka kan användas för att härleda andra regler är produktregeln och summeringsregeln (Heckerman, 1999).

Summeringsregeln säger att: $p(e|\xi) + p(\bar{e}|\xi) = 1$ (2.1)

Produktregeln säger att: $p(e_1, e_2|\xi) = p(e_2|e_1, \xi)p(e_1|\xi)$, för alla e_1 och e_2 (2.2)

Summeringsregeln säger uttryckt med ord att summan av alla sannolikheter alltid uppgår till 1, något som till exempel kan utnyttjas för att beräkna sannolikheten för en viss händelse då sannolikheten för alla andra händelser redan är känd. Produktregeln säger att sannolikheten för att båda händelserna e_1 och e_2 inträffar kan beräknas genom att multiplicera sannolikheten för att e_2 inträffar, givet att e_1 inträffat, med sannolikheten för att e_1 inträffar.

Andra regler som ofta används uttrycks i termer av variabler snarare än händelser. En variabel kan anta värden från en samling av ömsesidigt uteslutande och kollektivt uttömmande tillstånd, där varje tillstånd tillhör någon händelse (Heckerman, 1999). För att beteckna att variabel x är i tillståndet k skrivs $x=k$. Om tillståndet för alla variabler i mängden X observeras kallas denna mängd av observationer för ett tillstånd

hos X , vilket skrivs $X=k$. Sannolikhetsdistributionen över en mängd variabler X , skrivs $p(X|\xi)$ och betecknar mängden av alla sannolikheter $p(X=k|\xi)$ för alla tillstånd på X (Heckerman, 1999).

Ett mycket viktigt begrepp inom den bayesianska metodiken är Bayes teorem (vilket också ofta kallas för Bayes sats). Teoremet framstår idag jämfört med matematiskt invecklade teorem som mycket enkelt, men är trots detta den i särklass viktigaste grundläggande principen inom vetenskaplig inferens (Jaynes, 1985).

Bayes teorem säger att:

$$p(X|Y, \xi) = \frac{p(Y|X, \xi)}{p(Y|\xi)} \cdot p(X|\xi), \text{ för alla } p(Y|\xi) > 0 \quad (2.3)$$

$p(X|\xi)$ är sannolikhetsdistributionen hos X innan vi har någon kunskap om Y och kallas därför ofta för *prior probability* (på svenska prior-sannolikhet), medan $p(X|Y, \xi)$ är sannolikhetsdistributionen hos X efter det att vi fått kunskap om Y och kallas följaktligen för *posterior probability* (på svenska posteriori-sannolikhet) (Heckerman, 1999).

För att illustrera hur Bayes teorem fungerar kan läsaren föreställa sig följande scenario: Anta att herr Andersson känner till att sannolikheten för att få inbrott är 0,3 % och sannolikheten för att larmet går igång (på grund av inbrott eller alternativa orsaker) är 3 %. Anta vidare att herr Andersson uppskattar sannolikheten för att larmet går igång givet att villan utsätts för inbrott till 80 %. Om herr Andersson en natt vaknar av att hans larm gått, hur stor är då sannolikheten för att villan utsatts för inbrott? Svaret kan beräknas genom användandet av Bayes teorem:

$$p(\text{Inbrott} | \text{Larm}, \xi) = \frac{p(\text{Larm} | \text{Inbrott}, \xi)}{p(\text{Larm} | \xi)} p(\text{Inbrott} | \xi) = \frac{0.8}{0.03} 0.003 = 0.08$$

Det vill säga att sannolikheten för att ett inbrott begåtts, givet herr Anderssons bakgrundsinformation, är 8 %. Vad händer då om prior-sannolikheten ändras? Anta att herr Andersson uppskattar sannolikheten för inbrott till 3 % istället för 0,3 % och att övriga sannolikheter ser ut som i exemplet tidigare. Sannolikheten för att villan utsatts för ett inbrott blir då istället:

$$p(\text{Inbrott} | \text{Larm}, \xi) = \frac{p(\text{Larm} | \text{Inbrott}, \xi)}{p(\text{Larm} | \xi)} p(\text{Inbrott} | \xi) = \frac{0.8}{0.03} 0.03 = 0.8$$

Alltså har sannolikheten för inbrott skjutit i höjden till 80 %. Med andra ord kan valet av prior-sannolikheter starkt påverka utfallet, det vill säga posteriori-sannolikheten. Ofta består dock en beslutssituation av en mängd olika parametrar, varför det inte är säkert att en förändring av prior-sannolikheten för en enskild parameter påverkar posteriori-sannolikheten så mycket i en stor modell bestående av en mängd parametrar. Vid användandet av bayesianska nätverk (vilket bygger på Bayes teorem och beskrivs utförligare i kapitel 5.1) tyder en del forskning på att små förändringar av prior-sannolikheterna för en eller ett par parametrar inte spelar någon större roll för utfallet av posteriori-sannolikheterna, medan en del annan forskning tyder på att det i vissa typer av bayesianska nätverk kan påverka utfallet väldigt mycket (Chan och Darwiche, 2002).

2.2.2 Bayesiansk beslutsteori

Generellt sett kan ett beslut enligt Heckerman (1999) sägas bestå av tre komponenter: vad en beslutsfattare kan göra (dennes *alternativ*), vad beslutsfattaren vet (dennes

tilltro) samt vad denne vill (dennes *preferenser*). Inom bayesiansk beslutsteori används en *beslutsvariabel* för att representera en mängd ömsesidigt uteslutande och uttömmande alternativ, bayesianska sannolikheter för att representera beslutsfattarens tilltro, samt *nyttor* för att representera beslutsfattarens preferenser (Heckerman, 1999). Som tidigare nämnts finns det en huvudregel inom modern beslutsteori: att maximera den förväntade nyttan (Jaynes, 2003). Denna regel tillämpas inom bayesiansk beslutsteori genom att en beslutsfattare, givet en beslutsvariabel, ska tilldela en nytta till varje möjligt utfall för varje möjligt alternativ, tilldela subjektiva sannolikheter till varje möjligt utfall för varje möjligt alternativ, samt välja det alternativ som maximerar den förväntade nyttan (Heckerman, 1999). I de fall det inte rör sig om att generera nytta utan snarare välja mellan olika förlustsituationer ska beslutsfattaren istället sträva efter att minimera den förväntade förlusten (Jaynes, 2003).

Den traditionella nyttomaximeringsprocessen enligt Brynielsson (2002) kommer nu att beskrivas. Beakta varje möjlig värld, w_j , och låt varje sådan värld inträffa med sannolikheten p_j . Beslutsfattaren har då ett antal möjliga strategier/handlingar, s_i , att välja mellan. Låt u_{ij} vara nyttan av att utföra strategin s_i i världen w_j . Givet dessa beteckningar kan en nyttomatrix skapas (se figur 2.1).

	ω_1	ω_2	...	ω_j	...	ω_n
s_1	$u_{1,1}$	$u_{1,2}$...			
s_2	$u_{2,1}$	$u_{2,2}$...			
\vdots	\vdots	\vdots	\ddots			
s_i				$u_{i,j}$		
\vdots					\ddots	
s_m						$u_{m,n}$

Figur 2.1 Nyttomatrix enligt Brynielsson (2002)

Om strategi s_i väljs blir enligt Brynielsson (2002) den förväntade nyttan för denna

$$\text{strategi: } E(u_i) = \sum_{j=1}^n p_j u_{i,j} \tag{2.4}$$

Eftersom att den strategi, s_i , som maximerar den förväntade nyttan ska väljas, kommer valet av strategi falla på den strategi som maximerar summan i formel 2.4 ovan.

För att illustrera hur nyttomaximeringsprocessen fungerar kan läsaren föreställa sig följande exempel, hämtat ur Brynielsson (2002): En militärbas får in ett radareko som kan tänkas vara en möjlig missil. I detta läge existerar två möjliga världar, w_1 och w_2 , där w_1 innebär att det existerar ett reellt hot och w_2 att det inte existerar något reellt hot. Befälhavaren på radarstationen har då två alternativa handlingar, s_1 och s_2 , att välja emellan, där s_1 innebär att inte göra någonting alls och s_2 innebär att öppna eld. Detta ger en 2*2-matrix med fyra olika nyttovärden, där $u_{1,1}$ definierar nyttan av att inte öppna eld trots att en missil är på väg mot basen, $u_{1,2}$ motsvarar nyttan av att inte öppna eld när det inte finns något reellt hot, $u_{2,1}$ definierar nyttan av att öppna eld när det existerar ett reellt hot samt $u_{2,2}$ definierar nyttan av att öppna eld när det inte existerar något riktigt hot. Nyttan av att öppna eld om det observerade ekot verkligen kommer från en riktig missil är givetvis stor. Om det är en riktig attack kommer radarplotten förhoppningsvis förespråka w_1 med allt större sannolikhet, vilket gör att

den förväntade nyttan för s_2 blir störst, varpå beslutsstödsystemet råder befälhavaren att öppna eld.

2.2.3 Bayesiansk hypotesprövning

Inom vissa områden bygger beslut ofta på vad en motpart förväntas göra, till exempel handlar beslutsfattandet i exemplet i stycke 2.2.2 till stor grad om att bestämma vilken av de olika världarna som är den troligaste, det vill säga om fienden har attackerat eller ej. Denna typ av förutsägelser, som inom det militära används vid situationsanalys och hotanalys (se kapitel 2.3), är exempel på hypotesprövning. Hypotesprövning kan därför sägas ligga till grund för beslutsfattande där den maximala nyttan ska tas fram.

Tanken med bayesiansk hypotesprövning är enligt Lindberg (2002) att istället för att bedöma hur trolig en viss hypotes är, givet vissa underrättelser, vända på frågeställningen. Det som istället bedöms är sannolikheten för att få in olika underrättelser, givet att den riktiga hypotesen är känd (Lindberg, 2002). För att svara på den ursprungliga frågan kan sedan Bayes teorem användas. Bayes teorem kan formuleras med lite andra beteckningar än i stycke 2.2.1 för att mer passa in i kontexten av hypotesprövning. Teoremet kan då skrivas:

$$p(H | D, I) = p(H | I) \frac{p(D | H, I)}{p(D | I)} \quad (2.5)$$

där I = priori-information, D = erhållen data och H = hypotesen som ska prövas (Lindberg, 2002).

Genom att använda produktregeln (formel 2.2) kan Bayes teorem utvecklas till att gälla för fall där det finns tillgång till en mängd olika data (Lindberg, 2002):

$$p(H | D_1, D_2, D_3, I) = p(H | I) \frac{p(D_1 | H, I)p(D_2 | D_1, H, I)p(D_3 | D_2, D_1, H, I)}{p(D_1 | I)p(D_2 | I)p(D_3 | I)} \quad (2.6)$$

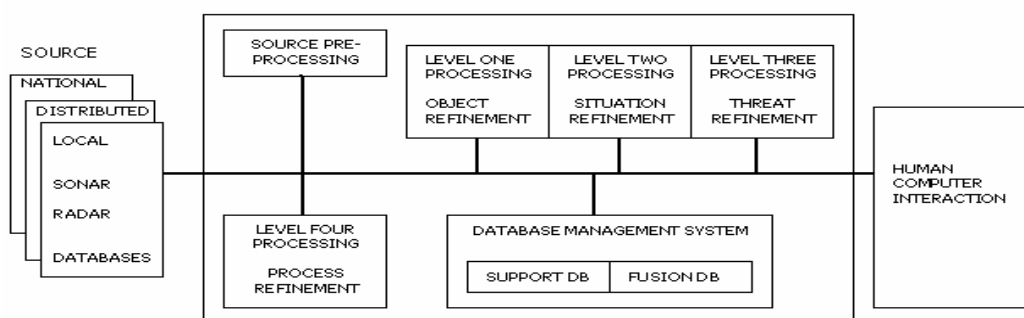
Genom att använda lagen om oberoende händelser kan formel 2.6, givet att de olika underrättelserna är oberoende, förenklas till:

$$p(H | D_1, D_2, D_3, I) = p(H | I) \frac{p(D_1 | H, I)p(D_2 | H, I)p(D_3 | H, I)}{p(D_1 | I)p(D_2 | I)p(D_3 | I)} \quad (2.7)$$

Den bayesianska metodiken är långtifrån obestridd. Vissa kritiker menar att sannolikheter kräver uppräknig av alla möjligheter, vilket de hävdar kräver väldigt mycket lagringsutrymme och så mycket beräkningar att metoder som bygger på sannolikhet beräkningsmässigt blir ogenomförbara (Das, 1999). En lösning på detta som föreslagits i litteraturen är användandet av så kallade bayesianska nätverk (Jensen, 1996; Runqvist, 2004). Detta område beskrivs närmare i kapitel 5.1. Ett problem som fortfarande kräver en lösning om angreppssättet med bayesianska nätverk väljs är att omvandla ett kunskapstillstånd till en sannolikhetstilldelning. Das (1999) konstaterar att problemet är långt ifrån löst och att detta är ett fält där det krävs fortsatt forskning. Davies Withers (2002) konstaterar att bayesiansk inferens kan vara känsligt för valet av prior-sannolikheter, något som också visades i stycke 2.2.1. Hon hävdar att detta gör att vissa forskare anser att den bayesianska metodiken är alltför subjektiv för att kunna användas. Trots allt har den bayesianska metodiken dock visat sig framgångsfull i väldigt många områden varför den är ett utmärkt val under förutsättning att valet av prior-sannolikheter görs grundat på kunskap om tillämpningsområdet (Davies Withers, 2002).

2.3 Informationsfusion

Informationsfusion är en del av det vidare begreppet datafusion, vilket enligt Wallenius (2004a) syftar på processen med att kombinera data eller information för att estimeras eller förutsäga tillstånd i världen. Informationsfusion nämns ofta som ett krav för att kunna erbjuda ett effektivt beslutsstöd (Westberg, 2001). Datafusion betecknar en mängd informationsbehandlingsprocesser där osäker och ofullständig information från olika källor slås samman (fusioneras), för att ge en mer komplett och mindre osäker bild av det aktuella problemområdet (Jönsson et al., 1998). Termen datafusion används ofta på ett opreciserat sätt varför den bör undvikas, istället bör termen fusion användas som ett samlingsnamn på sensordatafusion (nivå 1) och informationsfusion (nivå 2-4) (Lindberg, 2002). Dessa fyra nivåer beskrivs i JDL-modellen (se figur 2.2).



Figur 2.2 JDL-modellen (efter Jönsson et al., 1998)

JDL-modellen är en abstrakt modell av datafusionsbegreppet, framtagen av en grupp som tillsatts av chefskommittén för de amerikanska försvarsforskningslaboratorierna (Jönsson et al., 1998). Det är tydligt att modellen har sitt ursprung i det militära tillämpningsområdet, men enligt Jönsson et al. (1998) kommer denna typ av fusion med en modifierad terminologi även bli väldigt viktigt inom civila tillämpningsområden i framtiden.

De fyra nivåerna i JDL-modellen är sensordatafusion, situationsanalys, hotanalys samt adaption, där informationsfusion alltså inbegriper de tre senast nämnda nivåerna. Målet med informationsfusion är enligt Suzić (2003a) att beskriva ett specifikt tillstånd i världen genom att använda all tillgänglig information på bästa möjliga sätt.

2.3.1 Situationsanalys

Vid situationsanalysen, vilket motsvarar nivå 2 i JDL-modellen, identifieras den situation som är orsaken till observerade händelser och data. Vidare genereras också en mängd olika alternativa hypoteser om den aktuella situationen, vilka sedan utvärderas utifrån tillgängliga underrettelser, varpå de alternativa hypoteserna kan tilldelas sannolikheter baserat på hur troliga de är (Jönsson et al., 1998). Ett primärt område för situationsanalysen är att ta reda på var motståndaren har möjlighet att rycka fram genom olika korridorer. Situationsanalysen är enligt Jönsson et al. (1998) en kronologiskt ordnad process, såtillvida att data anländer över tiden och att detta leder till en successivt förfinad analys mot en alltmer säker trolig hypotes. För att skapa den lägesbild som används vid situationsanalys matas resultat från multisensordatafusion samt information från bland annat kartdatabaser in i systemet (Svensson och Schubert, 2003).

Das (1999) identifierar behovet av mer forskning om problemet med hur en mängd hypoteser som fångar möjliga fiendeintentioner, givet ett verkligt scenario, ska kunna tas fram.

2.3.2 Hotanalys

Processen hotanalys, vilken motsvarar nivå 3 i JDL-modellen, kan ses ur flera olika perspektiv. Inom hotanalysen analyseras vilka risker och möjligheter som finns för de egna styrkorna att möta fienden på ett effektivt sätt (Jönsson et al., 1998). Vid hotanalysen kombineras resultatet från den tidigare genomförda situationsanalysen med erhållna indikationer om motståndarens avsikter och information lagrad i taktiska och doktrinära databaser. De alternativa framryckningsvägar som togs fram vid situationsanalysen analyseras vidare, varpå några av dessa utifrån kunskap om taktik och doktrin identifieras som mer troliga än andra. Därigenom går det att beräkna när fiendens framryckning tidigast kan ske och vid vilken tidpunkt vissa kritiska punkter i terrängen troligen kommer att passeras (Jönsson et al., 1998). I tidningen *Framsyn* ges följande förklaring av vad hotanalys innebär:

”[Inom hotanalysen] ska man i princip kunna lista ut vad motståndaren ska göra innan han kommit på det själv. För att nå denna nivå krävs mycket information från många olika håll. En stor del av denna information är dock basfakta som motståndarens kända taktik, doktrin, väder, broars bärighet, terränghinder, egna svagheter, egna resurser som kan vara värdiga mål osv.” (Askelin, 2001, s. 25).

Det är inom gränslandet mellan situationsanalys och hotanalys som bayesiansk hypotesprövning kan komma väl till pass, för att utifrån ett antal olika handlingsalternativ för fienden komma fram till vilket som är de troligaste. Den grundläggande idén med hypotesprövning inom det militära är enligt Westberg (2001) att skapa ett antal hypoteser av vad fiendens plan är. Dessa hypoteser jämförs sedan kontinuerligt med omgivningen. Lindbergs tolkning av detta är att anta att fienden har n stycken handlingsalternativ, vilka betecknas H_i , där i tillhör mängden $[1, \dots, n]$. Enligt Lindberg (2002) är syftet med hypotesprövning att avgöra vilket av dessa n stycken handlingsalternativ som är fiendens verkliga avsikt.

Lindberg (2002) beskriver i sin magisteruppsats hur han använt bayesiansk hypotesprövning för att försöka utvärdera fiendens handlingsalternativ på förbandsnivå inom sjöstrid. Lindberg slutsats blev att det inom sjöstrid inte är lämpligt att använda bayesiansk hypotesprövning för att försöka förutsäga fiendens avsikt. De skäl han ger till detta är bland annat att:

- Fartygens stora vapenräckvidd gör att fartygens position inte avslöjar speciellt mycket om var en vapeninsats kan komma att genomföras.
- Havet erbjuder en väldigt stor rörelsefrihet vilket gör att det utifrån fartygens position, kurs och fart inte är möjligt att dra några direkta slutsatser om var de kan tänkas vara på väg.
- Moderna örlogsflottor består av få enheter, vilket leder till få indikatorer sett utifrån den taktiska nivån.

Det är dock viktigt att notera att även om bayesiansk hypotesprövning inte är tillämpligt i de fall som Lindberg (2002) studerat, betyder inte detta att bayesiansk hypotesprövning inte alls går att använda för att förutsäga fiendens avsikter. Som ett exempel kan nämnas att även om havet erbjuder en stor rörelsefrihet så ser förutsättningarna ut på ett helt annat sätt inom den svenska skärgården. Där gör alla

kobbar och skär att rörelsefriheten blir betydligt mer begränsad än ute till havs. Även Lindberg (2002) ser andra områden som han anser vara värda att undersöka då det gäller möjligheten att kunna tillämpa bayesiansk hypotesprövning. Bland annat identifierar han markstrid som ett potentiellt område för hypotesprövning av vad fienden har för intentioner. Lindberg konstaterar att antalet dugliga indikatorer bör vara tillräckligt många, då terrängen begränsar rörelsefriheten och stora mängder soldater och fordon måste föras relativt nära fienden.

Utöver det arbete som Lindberg (2002) utfört finns det också andra exempel på tidigare forskning inom området. Runqvist (2004) använder till exempel hotanalys för ett militärt försvarssystem som ordnar inkommande mål efter graden av hot de utgör. Ett annat exempel är Suzić (2003b) som använder existerande kunskap om olika fiendedoktriner för att på så sätt reducera storleken på hypotesrymden av fiendens handlingsalternativ. Enligt Askelin (2001) hade forskningsfronten vid denna tidpunkt kommit en liten bit in på situationsanalysen medan hotanalysen än så länge var näst intill outforskat territorium. Totalt sett är den forskning som lagts ner på dessa bitar av informationsprocessen väldigt liten jämfört med den forskning som lagts ner på sensordatafusion.

2.3.3 Adaption

Enligt Jönsson et al. (1998) betecknar adaption en kategori av olika processer, vilka syftar till att förbättra resultatet av en datafusionsprocess. Detta ska göras genom att utifrån identifierade brister i det producerade resultatet ge återkoppling på vad som behöver förbättras. Ett exempel på detta kan till exempel vara att i en adaptionsprocess identifiera att otillräckliga sensorresurser gjort att positionsbestämning av ett mål blivit helt felaktigt. Detta kan nästa gång förbättras genom att öka tilldelningen av sensorresurser (Jönsson et al., 1998). Eftersom adaption kräver att en ordentlig situations- och hotanalys har genomförts ligger forskningsområdet adaption dock en bit in i framtiden.

3 Problem

I detta kapitel beskrivs problemområdet och de frågor som detta arbete syftar till att besvara, dessutom redovisas också de avgränsningar som har gjorts i arbetet.

3.1 Problembeskrivning

I och med att en övergång håller på att ske till ”informationsåldern” inom militären, i samband med dess omställning till ett nätverksbaserat försvar, innebär detta att mängden insamlad data hela tiden ökar. Detta för med sig en ökad komplexitet och arbetsbörda för de militära beslutsfattarna (Westberg, 2001). För att kunna dra nytta av den ökande mängden data och för att undvika katastrofalt felaktiga beslut, såsom USS Vincennes nedskjutning av det iranska passagerarflygplanet av typen Airbus år 1988, har behovet av beslutsstödsystem blivit allt större inom militären (Westberg, 2001). För att kunna erbjuda effektiva beslutsstödsystem spelar som tidigare nämnts informationsfusion en central roll.

Enklare former av multisensoranalys gjordes för redan 60 år sedan då britterna i samband med slaget om Storbritannien fusionerade data från radar, akustiska sensorer, med mera. Sedan dess har forskarna blivit duktiga på multisensoranalys men högre nivåer inom informationsprocessen kräver fortfarande mycket forskning (Askelin, 2001).

Lindberg (2002), som konstaterar att bayesiansk hypotesprövning inte är tillämpligt inom sjöstrid för ytstridsfartyg, identifierar bland annat markstrid som ett område där bayesiansk hypotesprövning/inferens kan tänkas vara användbart. Inom markstrid är antalet indikatorer i form av antal enheter större än inom sjöstrid, dessutom minskar vapenräckvidden jämfört med fartygs vapenräckvidd, vilket leder till att enheterna måste föras närmare fienden. Också detta bör leda till bättre indikatorer som kan ge ledtrådar om fiendens avsikt. Det vore därför av intresse att försöka bygga en modell som bygger på bayesiansk hypotesprövning för att försöka prediktera fiendens intention. Detta arbete lägger inte så stor vikt på att undersöka de teoretiska möjligheterna att använda den bayesianska metodiken till förutsägelser om fiendens intentioner utan har ett mer empiriskt tillvägagångssätt. Istället för att lägga mycket tid på att väga teoretiska för- och nackdelar med olika tillvägagångssätt emot varandra har den bayesianska metodiken valts, då det finns en hel del stöd i tidigare gjord forskning för att den skulle kunna vara en lämplig metod. Det finns dock ingenting som säger att till exempel Dempster-Shaferteori inte skulle kunna fungera lika bra som den bayesianska metodiken, utan ska ses som att den bayesianska metodiken är en möjlig väg att gå och har valts i detta arbete.

Användandet av den bayesianska metodiken är som tidigare konstaterats inte helt problemfri. För att beräkna sannolikheten hävdar vissa kritiker att en uppräknings av alla olika möjligheter krävs, något som kräver väldigt mycket lagringsutrymme och beräkningskapacitet. En lösning som föreslagits i litteraturen på detta problem är användandet av bayesianska nätverk (Jensen, 1996; Runqvist, 2004). Användandet av den bayesianska metodiken för dock även med sig vissa andra problem: hur ett kunskapsstillstånd kan omvandlas till en sannolikhetsfördelning på ett tillförlitligt sätt (Das, 1999; Starr och Shi, 2004) samt att bayesiansk inferens är känsligt för valet av prior-sannolikheter (Davies Withers, 2002). Den bayesianska metodiken har dock visat sig framgångsfull på många områden (Chan och Darwiche, 2002) varför den är ett utmärkt val under förutsättning att valet av prior-sannolikheter görs grundat på kunskap om tillämpningsområdet (Davies Withers, 2002).

För att kunna undersöka hur bra modellen fungerar krävs det att den kan jämföras med hur en militär expert skulle ha satt sannolikheterna för fiendens olika handlingsalternativ i samma situation. Då det faller sig orimligt att vänta på en verklig invasion för att undersöka hur väl modellen fungerar blir alternativet att presentera motsvarande scenario grafiskt för en militär expert, för att denne ska kunna skatta sannolikheter i olika situationer som kan jämföras med den framtagna modellen. Detta innebär att modellen bör förses med ett grafiskt användargränssnitt, eftersom att det är i det närmaste nödvändigt för att kunna göra en utvärdering av hur bra modellen fungerar. Genom att på detta sätt samla in information om hur en expert skulle bedöma sannolikheterna för fiendens olika handlingsalternativ erbjuds också möjligheten att justera modellen så att den bättre stämmer överens med verkligheten. Om en modell på detta sätt förses med ett grafiskt användargränssnitt öppnas alltså stora möjligheter med att både validera och finjustera den underliggande modellen. Det grafiska gränssnittet bör också öka användarens förtroende för de sannolikhetsberäkningar som modellen utför. Detta hör samman med det faktum att sättet en beslutssituation presenteras på för en beslutsfattare i hög grad kan påverka dennes beslut (Wallenius, 2004b).

Den modell som skapas bör i framtiden kunna byggas ut, varför det också är viktigt att försöka identifiera eventuella tecken som tyder på att det kan bli svårt att utöka modellen i ett senare skede.

3.2 Problemprecisering

Målet med detta arbete är att försöka bygga en modell baserad på bayesiansk inferens/hypotesprövning i syfte att kvantifiera sannolikheten för fiendens olika handlingsalternativ inom markstrid, för att på detta sätt försöka prediktera vad fienden har för intentioner. För att öka användbarheten och förtroendet för de beräknade sannolikheterna ligger ett stort fokus på att modellen också förses med ett grafiskt gränssnitt, vilket ska ge möjlighet att validera modellens riktighet samt att samla in data från experter för att möjliggöra finjusteringar av densamma. Eventuella tecken som under arbetets gång framkommer på att det kan bli svårt att bygga ut modellen ska identifieras, eftersom en framtida utbyggnad antagligen krävs för att modellen ska fungera helt tillfredsställande.

Från den ovanstående problempreciseringen kan tre stycken olika delmål identifieras. Dessa delmål kan sammanfattas i följande punkter:

- Identifiera de parametrar som är viktigast då det gäller att försöka förutsäga vad fienden kommer att göra i framtiden.
- Implementation av modellen (genom användandet av ovanstående parametrar), samt integrering av denna med det grafiska användargränssnittet.
- Utvärdering av modellen och det framtagna verktyget för datainsamling.

3.3 Avgränsningar

Den modell som ska tas fram gör inte några anspråk på att vara fullständig eller perfekt, utan arbetet ska ses som ett empiriskt försök av huruvida det är möjligt att skapa en modell för prediktering av fiendens intention. Detta innebär att modellen endast kommer att bygga på de parametrar som identifieras som de viktigaste, men att övriga parametrar som under arbetets gång framkommer som viktiga ska dokumenteras, för att på så sätt möjliggöra en komplex framtida modell med en mycket bra kvalitet på skattningen av de olika sannolikheterna.

Problem

För att minska antalet alternativa hypoteser om fiendens handlingsalternativ kommer antagandet att fiendens enheter endast utnyttjar vägnätet för förflyttning göras. Om inte detta antagande görs kommer hypotesrymden bli oerhört stor, precis som inom sjöstriden. Hänsyn kommer inte heller att tas till fiendens doktrin eller taktik då detta ökar komplexiteten avsevärt, faktorer som dessa kommer istället att föras fram som förslag på framtida arbete.

4 Metod

I detta kapitel beskrivs de metoder och det tillvägagångssätt som valts för att uppnå de delmål som identifierades i föregående kapitel. I vart och ett av de olika delkapitlen beskrivs ett av de tre delmålen, olika metoder som är möjliga för att uppnå delmålet, samt motiven till varför just den valda metoden valts för att uppnå det identifierade delmålet. Genom att uppnå dessa delmål kommer också svaret på problempreciseringen att erhållas.

4.1 Identifiera parametrar

För att kunna bygga en modell av hur fienden troligtvis kommer att agera i framtiden måste först de parametrar som kan säga något om fiendens framtida agerande identifieras. Sådana parametrar kan till exempel tänkas vara fiendens trupprörelser, typen av fiendeförband, och så vidare. För att kunna identifiera dessa parametrar finns det några olika möjliga metoder som kan användas. Ett alternativ är att utföra en litteraturstudie för att undersöka om andra forskare har studerat detta tidigare och vad de i så fall har kommit fram till. Ett annat alternativ är att utföra intervjuer med experter på området och ta reda på vilka parametrar dessa anser är de viktigaste. Ytterligare ett alternativ är att använda sig av en enkätundersökning vilken skickas ut till en mängd respondenter, för att därpå använda statistiska tekniker för att analysera svaren.

Fördelen med litteraturstudier skulle kunna vara att någon forskare valt att studera problemet med att identifiera dessa parametrar som ett huvudproblem och därmed gjort noggranna och djupgående undersökningar om vilka parametrar som är de viktigaste. En potentiell risk och därmed en nackdel med litteraturstudier är att det kan visa sig att ingen forskare tidigare ägnat sig åt detta problem. Detta skulle kunna föra med sig att mycket tid lades ner på en litteraturstudie utan att det gick att få ut något resultat alls. Fördelen med att intervjua militära experter skulle vara att det är de som sitter inne med den verkliga kunskapen om vilken information som kan användas för att göra realistiska prognoser om vad fienden kommer att göra inom en snar framtid. Under förutsättning att det är möjligt att göra denna typ av förutsägelser är chanserna dessutom stora att identifiera lämpliga parametrar med hjälp av intervjuer. En potentiell nackdel med denna teknik är att det kan vara svårt att få tag på denna typ av experter då de antagligen är mycket upptagna med andra uppgifter på grund av den expertkunskap de besitter. Det finns också en risk att dessa experter skulle vara motvilliga till att hjälpa till, då det kan finnas en rädsla för att denna typ av system skulle kunna ersätta experterna, trots att det egentligen handlar om att systemen ska minska den kognitiva belastningen och vara ett stöd för beslutsfattarna. Enkätundersökningar har fördelen av att de ger ett mer utförligt material, det vill säga att det troligtvis ger tillgång till en stor kvantitet svar, vilka går att analysera med hjälp av statistiska metoder, men nackdelen är att det är svårt att få tag i experter i den omfattningen samt att detta mer eller mindre kräver att troliga parametrar identifierats på förhand, varpå enkätundersökningen syftar till att ta reda på vilka parametrar som är de absolut viktigaste.

Valet av metod har fallit på en öppen intervju, då fördelen med att få relativt säkra resultat har övervägt. Genom att kontakter tagits med både Markstridsskolan och Ericsson Microwave Systems har även risken med att det kan bli svårt med att få tag i experter som är insatta på området eliminerats.

4.2 Implementation av modellen och det grafiska gränssnittet

Att lösningen på detta delmål åstadkoms genom en implementation är ganska självklart, med tanke på delmålet's namn. Det finns dock flera sätt att göra en implementation av en modell som bygger på bayesiansk inferens och hypotesprövning. Ett sätt som tidigare diskuterats i arbetet är att implementera modellen som ett bayesianskt nätverk. Fördelen med detta sätt är bland annat att det är en lösning på problemet med beräknings- och lagringskapacitet som identifierades i kapitel 3.1. Starr och Shi (2004) ser flera andra fördelar med att använda just bayesianska nätverk vid beslut under osäkerhet inom markstrid, bland annat att de är mycket snabba när de väl konstruerats och för att nätverket ibland kan dra inferenser som är för komplicerade att göra för den mänskliga hjärnan. Som ett exempelområde för bayesianska nätverk nämner Starr och Shi (2004) just förutsägelse av vad fienden kommer att göra i framtiden baserat på bland annat information om doktrin, miljö, logistik, eldunderstöd och truppstyrkor. I detta arbete kommer inte extra information som kan lagras i databaser, såsom fiendens doktrin, taktik med mera, att beaktas men däremot spelar faktorer såsom miljö (i form av vilka vägar som vägnätet erbjuder) samt fiendens position och typ av förband stor roll för de olika alternativens utfall. Lindberg (2002) beskriver ett annat tillvägagångssätt för hur den bayesianska inferensmodellen kan implementeras, vilket beskrivs utförligare av Jaynes (2003). Tillvägagångssättet bygger på att istället för att beräkna sannolikheten för att en enskild hypotes ska inträffa så beräknas sannolikheten för att hypotesen ska inträffa jämfört med sannolikheten för att alla övriga hypoteser ska inträffa. Det värde som då fås fram kallas för oddset för hypotesen. Lindberg (2002) nämner två fördelar med att använda sig av odds: att den svårsatta sannolikheten $p(D)$ kan förkortas bort, samt att risken med att vilseledas av den så kallade lotteriprincipen reduceras, det vill säga att betydelsen för värderingen av en enskild hypotes riskerar att urvattnas om hypotesen ska jämföras med en stor mängd alternativa hypoteser (Lindberg, 2002).

Valet har fallit på att implementera modellen som ett bayesianskt nätverk då denna typ av lösningar har visat sig fungera tidigare inom det militära området (se till exempel Ivansson, 2002; Runqvist, 2004) och är relativt lätta att förstå (Heckerman, 1999). En annan stor fördel med bayesianska nätverk är att mängden beräkningar som krävs reduceras kraftigt, jämfört med många andra sorter av sannolikhetsberäkningar.

När det gäller att förse modellen med ett grafiskt användargränssnitt har valet fallit på att implementera modellen som en integrerad komponent i GTSIM (Ground Target Simulator) En utförlig beskrivning av vad GTSIM är ges i kapitel 5.3, men kortfattat kan det beskrivas som ett verktyg som fusionerar samman data från olika sensorer och utifrån detta skapar en gemensam lägesbild över var olika förband befinner sig. Genom att lägga till funktionalitet till GTSIM i form av skapandet och inläsning av mål (vilka representerar fiendens olika handlingsalternativ) samt integrering och implementation av modellen byggd i form av ett bayesianskt nätverk kan verktyget användas för att skapa olika typer av scenarion där fiendens handlingsalternativ finns representerade, och utifrån detta beräkna sannolikheten för de olika handlingsalternativen.

Det framtagna verktyget ska utöver att användas för att prediktera fiendeintentionen med hjälp av den bayesianska inferensmotorn även kunna användas för att förbättra modellen/inferensmotorn. Genom att lägga till stöd för insamling av data över hur en expert skulle bedöma sannolikheten för de olika handlingsalternativen kan dessa data användas för att finjustera modellen. En utförligare beskrivning av detta ges i kapitel 4.3.

4.3 Utvärdering av modellen och det framtagna verktyget för datainsamling

För att kunna göra en utvärdering av hur ”rätt” modellen är krävs det att en jämförelse görs mellan modellens utdata och hur en expert på området skulle bedöma sannolikheten för fiendens olika handlingsalternativ i samma situation. Att det inte går att vänta på att ett valt scenario inträffar i verkligheten för att sedan utvärdera skillnaden mellan den mänskliga beslutsfattarens skattning av sannolikheten för fiendens olika handlingsalternativ med den framtagna modellen är ganska uppenbart, därför återstår det två realistiska alternativ. Det ena alternativet är att använda sig av ett scenario som redan inträffat på riktigt och där det finns tillgänglig information om hur troliga fiendens olika handlingsalternativ ansetts vara av den militära beslutsfattaren. Det andra alternativet är att använda sig av ett konstruerat scenario där först den byggda inferensmodellen får dra slutsatser om sannolikheten för olika handlingsalternativ allteftersom scenariot utspelas. Därpå kan samma scenario presenteras för en militär expert vilken i olika tidslägen får ange hur denne skattar sannolikheten för att de olika målen ska anfallas. Genom att jämföra resultaten från modellens skattningar med den militära expertens kan därigenom en utvärdering göras av hur rätt modellen är vilket framöver kan användas för finjustering av modellen.

Fördelen med historiska scenarion är att de bygger på riktiga data, det vill säga att all data är hämtad ur verkligheten och att det finns ett facit över vad fienden valde att göra. Deras nackdel är att det handlar om gammal data, dagens krigsföring ser ut på ett annat sätt än vad krigsföringen gjorde under andra världskriget som ett exempel. Inferensmotorn som ska implementeras är avsedd att användas inom informationsfusionsområdet och ska därför förutsäga fiendens handlingsalternativ inom modern markstrid. Detta är styrkan hos konstruerade scenarion, det vill säga att de på ett annat sätt än historiska scenarion kan anpassas till dagens (och om önskat även framtidens) krigsföring. En annan potentiell nackdel med historiska scenarion är att det finns en risk att inte all data som behövs finns tillgänglig. Av den anledningen har det bedömts som lämpligt att presentera några enkla konstruerade scenarion för en expert, vilken får bedöma sannolikheten för fiendens olika handlingsalternativ i olika situationer. Dessa skattade sannolikheter kan sedan jämföras med hur den implementerade inferensmotorn skattar sannolikheterna i samma situation.

Genom att förse modellen med ett grafiskt användargränssnitt, vilket redan har diskuterats, fås ett mycket bra verktyg för att kunna utvärdera hur rätt modellen är. Experten kan då direkt på skärmen se hur scenariot utvecklar sig vilket gör det mycket lättare att skatta sannolikheterna för fiendens olika handlingsalternativ. En annan fördel med det grafiska användargränssnittet är att det kan användas som ett verktyg för att kalibrera in en framtida förfinad modell. Genom att notera de fall där expertens sannolikhetsbedömningar skiljer sig mycket från de sannolikheter som ges som utdata av inferensmotorn, kan en analys göras av vilka parametrar som bör justeras och på vilket sätt modellen bör förändras för att bättre återspegla de sannolikheter som en mänsklig expert har skattat. För att kunna göra detta bör verktyget förse med en funktion för pausning, där användaren får en chans att mata in dennes skattningar av de olika sannolikheterna, i syfte att senare finjustera modellen utifrån dessa data.

5 Genomförande och resultat

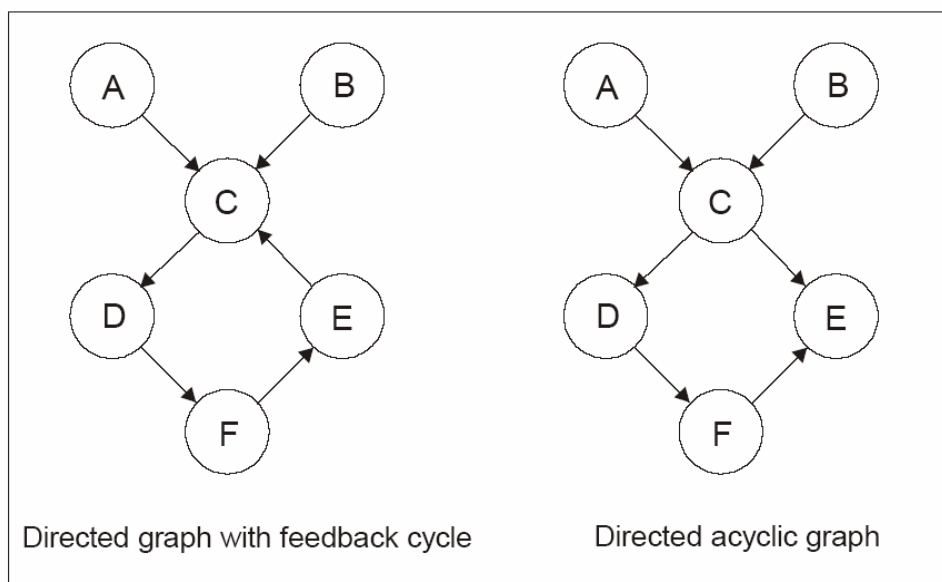
I detta kapitel görs en genomgång av vad bayesianska nätverk är och hur de fungerar. Därefter beskrivs vilka parametrar som har valts ut för att utgöra den modell som ska användas för att försöka prediktera fiendens intentioner. Därpå beskrivs hur modellen har implementerats och vilka tillägg som har gjorts till GTSIM, samt så presenteras en utvärdering av den implementerade modellen och det grafiska verktyget. Slutligen redogörs det också för hur en finjustering av den framtagna modellen kan göras, utifrån data som samlats in med det framtagna verktyget.

5.1 Bayesianska nätverk

Bayesianska nätverk kan sägas vara en grafisk representation av osäker kunskap som de flesta människor tycker är relativt lätta att tolka, där representationen dessutom gör att nätverket passar bra till statistiska modeller (Heckerman, 1999).

Ett bayesianskt nätverk består av en mängd sammankopplade noder och beskriver en specifik domän i världen. Det bayesianska nätverket representeras som en riktad graf där varje nod har tillhörande information om sin kvantitativa sannolikhet. Enligt Russel och Norvig (2003) är den fullständiga specifikationen för ett bayesianskt nätverk följande:

- En mängd stokastiska variabler utgör noderna i nätverket, där de stokastiska variablerna kan vara antingen diskreta eller kontinuerliga.
- En mängd riktade kanter kopplar samman par av noder. Om det finns en kant som går från nod X till nod Y sägs X vara förälder till Y .
- Varje nod X_i har en tabell över den tillhörande betingade sannolikhetsfördelningen $p(X_i | \text{Föräldrar}(X_i))$ som kvantifierar den effekt som eventuella föräldrar har på barnnoden.
- Grafen får inte ha några cykler (se figur 5.1) och är därför av typen riktad, acyklisk graf (DAG).



Figur 5.1 Exempel på otillåtna och tillåtna bayesianska nätverk (efter Ivansson, 2002).

Alla de noder som inte har någon sammankopplad väg mellan sig (till exempel A och B i figur 5.1) är oberoende. För dessa gäller därför lagen om oberoende:

$$p(A, B) = p(A)p(B) \quad (5.1)$$

För de noder som har en sammankopplad väg mellan sig (till exempel A och C i figur 5.1) måste sannolikheten beräknas genom att använda de tabeller med betingande sannolikheter som definierats för de sammankopplade noderna. I högra delen av figur 5.1 skulle tabellen för nod A bestå av $p(A)$, tabellen för nod B av $p(B)$, tabellen för nod C av $p(C|A,B)$, och så vidare.

5.1.1 Konstruktion av bayesianska nätverk

Processen med att konstruera och bygga modellen av det bayesianska nätverket är ofta en flaskhals då det gäller att tillämpa användandet av bayesianska nätverk på verkliga applikationer (Wang, Rish och Ma, 2002). Av den anledningen ska här en genomgång ske av hur bayesianska nätverk konstrueras.

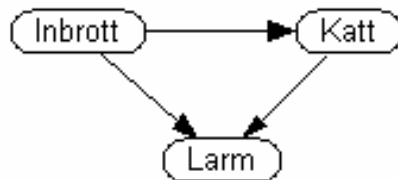
Det finns en del befintlig programvara för att konstruera bayesianska nätverk, både kommersiell och icke-kommersiell. Exempel på programvara som ofta nämns inom informationsfusionsforskning är HUGIN (Ivansson, 2002; Lindberg, 2002; Starr och Shi, 2004) och Netica (Das, 1999; Starr och Shi, 2004). I detta arbete används det kommersiella Java-API:et till Netica, vilket är mycket smidigt att använda. Det finns även en gratisversion vilken har all funktionalitet som den kommersiella versionen har, förutom att gratisversionen har en begränsning på hur många noder som kan användas. På grund av att den framtagna modellen krävt mer än de femton noder som gratisversionen erbjuder har dock alltså den kommersiella versionen använts. Neticas Java-API finns tillgängligt att ladda ner från tillverkaren Norsys hemsida¹.

Det som behövs för att kunna konstruera nätverket är kunskap om vilka noder som ska ingå, vilka olika tillstånd dessa noder kan anta, vilka kopplingar som finns mellan de olika noderna samt tabeller över betingade sannolikhetsfördelningar (Jensen, 1996). För att de läsare som inte har någon erfarenhet av bayesianska nätverk ska förstå hur dessa fungerar kommer nu konstruktionen av ett enkelt exempelnätverk beskrivas i detalj.

Ponera att ett bayesianskt nätverk ska tas fram för att avgöra om ett inbrott håller på att begås eller inte (jämför med exemplet i stycke 2.2.1). Anta att det endast finns två tänkbara orsaker till att ett larm löser ut: att det pågår ett inbrott eller att grannens katt av någon outgrundlig anledning lyckats ta sig in i huset. I detta fall finns det tre stycken noder: inbrott, larm och katt (ett ganska rimligt antagande är att variabler såsom öppna eller stängda fönster påverkar sannolikheten för att både katter och inbrottstjuvar kommer in i huset men för att göra exemplet så trivialt som möjligt bortser vi från detta). Kopplingarna mellan dessa noder blir att ett inbrott påverkar sannolikheten för att larmet ska lösa ut, närvaron av en katt i huset påverkar sannolikheten för att larmet ska lösa ut samt att ett inbrott påverkar sannolikheten att det finns en katt i huset (genom att katten till exempel kan smita in genom ett krossat fönster). Samtliga dessa noder har diskreta tillstånd: larm har tillstånden tjuver/tyst, inbrott tillstånden ja/nej, samt så har katt tillstånden inne/inte inne. Dessa förhållanden åskådliggörs i figur 5.2

¹ <http://www.norsys.com/netica.html>

Genomförande och resultat



Figur 5.2 Exempel på ett enkelt bayesianskt nätverk

Med detta gjort återstår det att skapa tabellerna med betingade sannolikheter. För inbrott består denna tabell endast av de betingade sannolikheterna (och tillika prior-sannolikheterna) för tillstånden ja och nej. Anta att sannolikheten för att drabbas av inbrott är 0.3 %. Följaktligen blir då sannolikheten för att inte drabbas av inbrott 99,7 % eftersom summan av hela utfallsrummet måste bli 1 i enlighet med det som sagts i formel 2.1 i stycke 2.2.1. Att definiera de betingade sannolikhetstabellerna i ett sådant här litet exempelnätverk är inga problem, men i större nätverk kan det bli enorma antal betingade sannolikheter att sätta, vilket är bland de största problemen med användandet av bayesianska nätverk (Wang et al., 2002).

Ja	Nej
0,3	99,7

Tabell 5.1 Sannolikhetstabellen för inbrott uttryckt i procent

När det gäller den betingade sannolikhetstabellen för katt är denna lite mer komplicerad eftersom moderna inbrott och katt har ett kausalt samband. Anta att sannolikheten för att grannens katt kommer in i huset är 1 % om inget inbrott pågår och 10 % om ett inbrott pågår. Resultatet kan ses i tabell 5.2.

Inbrott	Inne	Inte inne
Ja	10,0	90,0
Nej	1,0	99,0

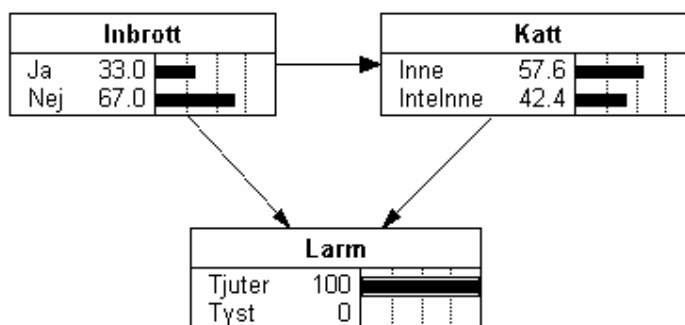
Tabell 5.2 Sannolikhetstabellen för katt uttryckt i procent

Slutligen ska också den betingade sannolikhetstabellen för larm tas fram. Sannolikheten att larmet tjuver givet att ett inbrott pågår men att ingen katt finns i huset sätts till 80 % och sannolikheten för att larmet tjuver givet ett inbrott och en katt sätts till 95 %. Motsvarande sannolikhet för att larmet tjuver givet en katt men inget inbrott sätts till 40 %. Slutligen sätts sannolikheten för att larmet tjuver trots att varken någon katt eller inbrottstjuv finns i huset till 0,1 %. Detta kan ses i tabell 5.3. I detta lilla exempelnätverk har de betingade sannolikheterna satts lite på en höft, vilket inte är några problem eftersom nätverket inte kommer att ha någon seriös användning, men eftersom det är de betingade sannolikhetstabellerna som tillsammans med nätverkets topologi ligger till grund för de posteriori-sannolikheter som erhålls då nätverket körs är dessa betingade sannolikhetstabeller ofta mycket viktiga, varför det vanligtvis är experter inom domänen som får sätta dessa betingade sannolikheter (Wang et al., 2002).

Inbrott	Katt	Tjuter	Tyst
Ja	Inne	95,0	5,0
Ja	Inte inne	80,0	20,0
Nej	Inne	40,0	60,0
Nej	Inte inne	0,1	99,9

Tabell 5.3 Sannolikhetstabellen för larm uttryckt i procent

Med de betingade sannolikheterna satta är nu det bayesianska nätverket färdigt och är redo att dra inferenser. Om information exempelvis fås om att larmet tjuter kan detta matas in i det bayesianska nätverket varpå nätet drar inferenser om sannolikheten för de olika tillstånden. Figur 5.3 visar sannolikheten för de olika tillstånden då kunskap om att larmet tjuter matats in.



Figur 5.3 Sannolikheten för olika tillstånd då fakta om att larmet tjuter matats in

Hur fungerar det då när det bayesianska nätverket drar inferenser? För att kunna göra beräkningar för alla olika sannolikheter i ett bayesianskt nätverk används vid kompilering av nätverket en teknik som på engelska kallas för *propagation* (Ivansson, 2002), vilket ungefärligen kan översättas till spridning eller utbredning på svenska. Beräkningar av en så kallad *joint probability* (sammanslagen sannolikhet) görs för alla möjliga tillstånd som kan förekomma i modellen, varpå tabeller över dessa skapas för varje nod (Ivansson, 2002). För noden inbrott ser denna ut precis som dess betingade sannolikhetstabell eftersom denna inte har några föräldranoder. För noden katt däremot ser den sammanslagna sannolikhetstabellen annorlunda ut. Denna fås fram genom att beräkna $p(\text{katt}=\text{inne})$ på följande vis:

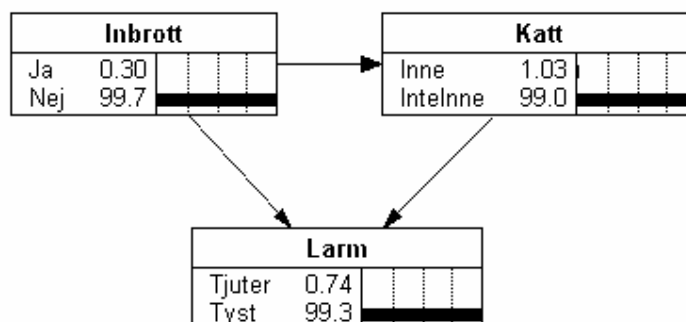
$$p(\text{katt} = \text{inne}) = p(\text{katt} = \text{inne} | \text{inbrott} = \text{ja}) * p(\text{inbrott} = \text{ja}) + p(\text{katt} = \text{inne} | \text{inbrott} = \text{nej}) * p(\text{inbrott} = \text{nej}) = 0,1 * 0,003 + 0,01 * 0,997 \approx 0,010$$

Eftersom att summan av sannolikheterna för att katten befinner sig inne och att katten inte befinner sig inne ska summeras till ett blir följaktligen sannolikheten för att katten inte befinner sig inne 0,990 innan några fakta har matats in. För noden larm som har två föräldranoder blir motsvarande beräkning:

$$p(\text{larm} = \text{tjuter}) = p(\text{larm} = \text{tjuter} | \text{inbrott} = \text{ja}, \text{katt} = \text{inne}) * p(\text{katt} = \text{inne} | \text{inbrott} = \text{ja}) * p(\text{inbrott} = \text{ja}) + \dots = 0,95 * 0,1 * 0,003 + 0,8 * 0,9 * 0,003 + 0,4 * 0,01 * 0,997 + 0,001 * 0,99 * 0,997 \approx 0,0074$$

... innebär att på motsvarande sätt beräkna sannolikheterna då det pågår inbrott men katten inte befinner sig inne, när det inte pågår inbrott men att katten befinner sig

inne, samt då det inte pågår inbrott och katten inte befinner sig inne. De sammanslagna sannolikhetstabellerna för de olika noderna i nätverket kan ses i figur 5.4. Detta motsvarar alltså att det bayesianska nätverket har kompilerats men att inga fakta har matats in i det.



Figur 5.4 Nätverket då det är kompilerat visar joint probabilities

När väl nätverket har kompilerats och sannolikheten för de olika nodernas tillstånd beräknats, givet att det inte finns någon fakta inmatad om de olika noderna, är nätverket alltså redo att ta emot fakta om olika tillstånd i världen. När dessa fakta matas in propageras kunskapen vidare i nätverket varpå sannolikheterna för de olika nodernas tillstånd uppdateras. Om kunskap matas in om en nod som saknar föräldrar är det relativt lätt att förstå vad som händer för de noder som enbart har denna nod som föräldranod. Anta att kunskap om att ett inbrott håller på att begås matas in i nätverket. Då går det i den betingade sannolikhetstabellen för katt att se, att om ett inbrott begås är sannolikheten för att det finns en katt inne i huset 10 %.

Om det istället är känt att det finns en katt inne i huset men att det är okänt om larmet har löst ut och huruvida det pågår ett inbrott eller inte är det inte lika enkelt att beräkna sannolikheten för att ett inbrott håller på att begås. Lösningen är då att använda sig av Bayes teorem eftersom det med hjälp av detta går att få fram sannolikheten för att ett inbrott begås givet att det finns en katt i huset. Dessa beräkningar redovisas inte här eftersom det ändå är det färdigutvecklade Netica-API:et som används till att utföra alla uträkningar av sannolikheter i detta arbete. Ifall det finns någon som i detalj vill studera hur beräkningarna sker i ett bayesianskt nätverk hänvisas den intresserade läsaren till Jensen (1996).

Det som har diskuterats här är endast ett litet exempelnätverk men visar ändå de grundläggande idéerna med bayesianska nätverk.

5.2 Framtagande av parametrar/noder

För att kunna implementera det bayesianska nätverket som ska användas för att beräkna sannolikheterna för fiendens olika handlingsalternativ krävs det att de olika noderna i nätverket tas fram. Dessa motsvarar de parametrar som diskuterades i kapitel 4.1. Som tidigare nämnts har ett försök att ta fram dessa parametrar gjorts genom att genomföra en öppen intervju med en militär expert från Markstridsskolan i Skövde. För att ha ett underlag och öppningsfrågor till intervjun plockades i förväg ett antal parametrar fram, vilka hade som syfte att få igång diskussionerna. De parametrar som i förväg valdes ut är:

- Fiendens avstånd till potentiella mål
- Fiendestyrcans sammansättning

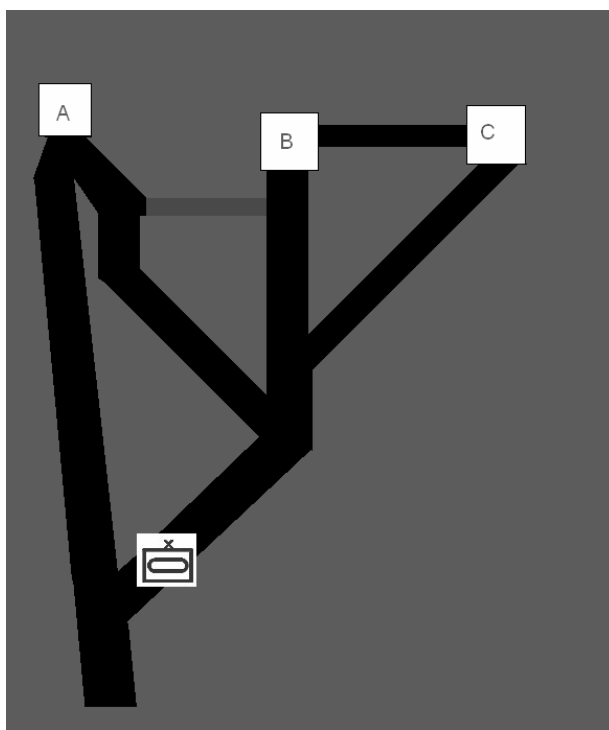
Genomförande och resultat

- Potentiella måls attraktionskraft
- Övriga tecken vid potentiella mål (såsom sabotageverksamhet)

Avstånd bygger på fiendens position i förhållande till positionen för potentiella mål och bedöms som en viktig parameter. Den nuvarande positionen spelar en stor roll vid ett annat arbete inom området som handlar om positionsprediktering, där prediktering görs av fiendens framtida position (Brynielsson, Engblom, Franzén, Nordh och Voigt, 2005). Detta arbete går det att läsa mer om i kapitel 6.1.

Fiendestyrkans sammansättning och målens attraktionskraft bygger på att fiendens framtida agerande bör bero på nyttan med olika handlingsalternativ. Om fienden kan uppnå mycket stor nytta med att slå ut ett mål torde detta höja sannolikheten att fienden väljer att försöka slå ut målet. Likaså torde sammansättningen hos fiendestyrgan påverka vilka sorts mål som fiendestyrgan väljer att anfälla, då ett infanteriförband och ett stridsvagnsförband passar olika bra för olika uppgifter. Övriga tecken är en generalisering av indikatorer såsom skottfältsröjning, broarbeten och spaningsenheter vilka är indikatorer som Lindberg (2002) hävdar kan ge information om fiendens avsikter inom markstriden.

Utöver parametrarna konstruerades även ett enkelt scenario för att ha en utgångspunkt ifall tiden skulle räcka till att även diskutera vad som skulle kunna vara ett lämpligt scenario att testa modellen på. Scenariot som konstruerades består av tre stycken potentiella mål (städerna A, B och C), en fiendlig pansarbrigad samt ett vägnät. Stad A har ett starkt försvar samt några användbara flygfält, B har stora bränsleförråd och ett starkt försvar medan C har ett svagare försvar och tillverkar en del krigsmateriel. Dessa olika städer är sammankopplade via ett enkelt vägnät (se figur 5.5). Scenariot beskriver fiendebrigadens position i olika ögonblicksbilder, samt en del händelser såsom sabotage av delar av elförsörjningen i stad C.



Figur 5.5 Exempel på ögonblicksbild ur enkelt scenario

5.2.1 Intervju med officer från Markstridsskolan

Under intervjun med en militär expert² från Markstridsskolan framkom att modern krigsföring i mångt och mycket grundas på *manövertänkande*. Manövertänkande kan sägas utgöra principer för hur fysiska faktorer såsom stridskrafter och moraliska faktorer som till exempel ledarskap ska kunna användas på bästa sätt för att uppnå ett bestämt mål, ett så kallat *avgörande* (Försvarsmakten, 2002). Enligt experten är ett syfte med manövertänkande att uppnå avgöranden genom att åstadkomma en så kallad *systemchock*. En militär konflikt kan ofta ses som en interaktion mellan två (eller flera) komplexa system, där systemchock kan uppstå då samordningen upphör i något av systemen genom att vitala funktioner i systemet upphör att fungera (Försvarsmakten, 2002). Den militäre experten förklarade att denna form av doktrin alltså bygger på att försöka besegra fienden utan att behöva nedkämpa dennes huvudstridskrafter. Istället ska fienden besegras genom att lamslå motståndarens vilja att fortsätta slåss. Han menade vidare att detta görs genom att identifiera fiendens *kritiska sårbarheter*, vilket är punkter där motståndaren har sina svagheter eller där motståndaren inte förväntar sig ett angrepp. Exempel som denne expert gav på sådana kritiska sårbarheter är spränggattentat vid polisstationerna i Irak och NATO:s attacker mot infrastruktur i det forna Jugoslavien, under kriget på Balkan. Dessa kritiska sårbarheter varierar enligt experten mycket från situation till situation, och av den anledningen bedömde han därför att det är svårt att identifiera några enskilda parametrar för att förutse fiendens handlingsalternativ som fungerar i alla situationer. Istället bör utgångspunkten enligt den militäre experten vara en given situation eller ett scenario där kritiska sårbarheter kan identifieras, för att utifrån detta se vilka parametrar som kan vara viktiga för att förutsäga fiendens framtida handlingsalternativ. Han höll dock med om att de parametrar som tagits fram i förväg var parametrar som i många typer av situationer kunde säga något om vad fienden kunde tänkas göra i framtiden, även om de borde kompletteras med situationsspecifik information om kritiska sårbarheter.

5.2.2 Samtal med representant från Ericsson Microwave Systems

Eftersom mötet med den militäre experten från Markstridsskolan inte resulterade i några klart definierade parametrar togs frågan upp med en anställd på Ericsson Microwave Systems, som arbetar med bland annat informationsfusion och det nätverksbaserade försvaret. De parametrar som tidigare diskuterats ansågs då vara väl valda, dock med tillägget att inte bara fiendestyrelsens sammansättning påverkar målets attraktionskraft, utan att attraktionskraften även påverkas av målets så kallade skyddsvärde, det vill säga hur värdefullt målet bedöms vara. Ett annat samtalsämne var att det utöver den spatiala dimensionen (det vill säga den rumsliga) även är viktigt att ta hänsyn till den temporala dimensionen. Av den anledningen bedömdes även parametern riktning som viktig att implementera då den bygger på rörelse över tid, vilket gör att även den temporal dimensionen fås med.

5.2.3 Parametrar som valts ut att tas med i modellen

Situationsspecifika parametrar som bygger på kritiska sårbarheter skulle vara mycket intressanta att implementera i framtiden, liksom information om fiendens doktrin, väderlek, med mera. I detta arbete har dock sådana parametrar setts som exempel på möjlig vidareutveckling, och istället har fokus lagts på att bygga en mer

² C TaUtvsekt/MSS

grundläggande modell för att kunna utvärdera dennas lämplighet och undersöka möjligheterna att använda det framtagna verktyget för insamling av data, vilka skulle kunna användas för att finjustera modellen. De parametrar som valts ut kan alltså ses som mycket generella, varför en modell byggd på enbart dessa parametrar antagligen inte kan ge så bra resultat som en modell som är anpassad för ett specifikt scenario, vilket föreslogs av den militäre experten. Dock bör en implementation av denna förenklade modell ge svaret på frågan om det överhuvudtaget är möjligt att använda sig av denna form av teknik inom markstriden, samt att identifiera problem som måste lösas innan en eventuell framtida applikation som är fullt användbar kan utvecklas.

De framtagna parametrarna bygger i mångt och mycket på eget tänkande, intervjuer med experten från Markstridsskolan, samtalet med representanten från EMW, samt på parametrar som använts eller föreslagits inom liknande områden av andra forskare.

Det som till största delen torde påverka fiendens val av handlingsalternativ är hur mycket nytta fienden tror att de får ut av att slå till mot de olika målen, något som överensstämmer med principen om att välja det alternativ som maximerar den förväntade nyttan (Jaynes, 2003). Av den anledningen har parametern som i detta arbete valts att kallas för ett måls attraktionskraft tagits med, vilken alltså kan ses som fiendens förväntade nytta av att anfälla ett visst mål. Attraktionskraften hos ett mål kommer i modellen betraktas som beroende av det aktuella målets skyddsvärde, den typ av mål som det aktuella målet är en instans av, samt typen av fiendestyrkor. Detta bygger på antagandet att olika typer av fiendestyrkor skiljer sig åt i lämplighet att anfälla olika typer av mål.

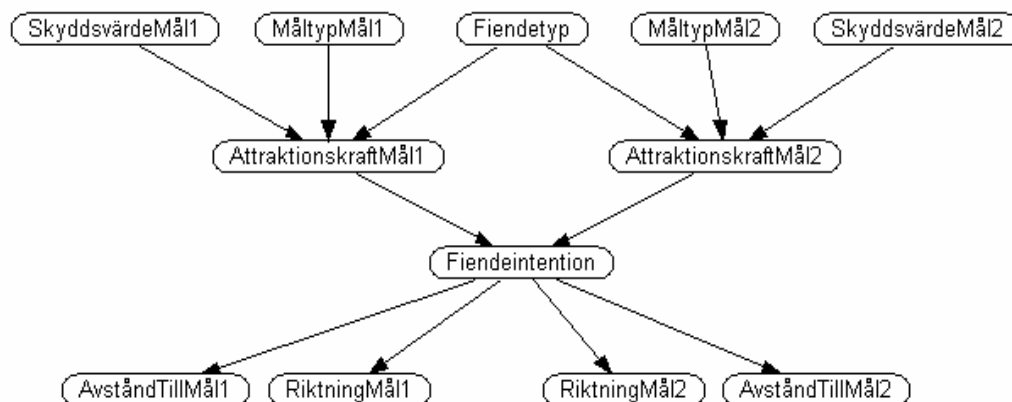
Ytterligare en parameter som torde påverka nyttan med att anfälla ett mål är hur starkt målets försvar är. Denna parameter har dock valts att tills vidare inte tas med i modellen. Anledningen till detta är att parametern attraktionskraft då skulle få en mycket större betingad sannolikhetstabell vilket skulle leda till väldigt mycket arbete enbart med att fylla denna tabell med betingade sannolikheter. Om modellen skulle fånga alla aspekter i verkligheten som påverkar nyttan av att anfälla ett mål skulle antagligen otaliga fler parametrar tillkomma, rent beräkningsmässigt borde det gå att hantera relativt många parametrar, men då krävs en lösning på problemet med att fylla de betingade sannolikhetstabellerna med data. Detta arbete kan inte göras manuellt för en nod med så många föräldranoder som attraktionskraft då skulle få, utan kräver att de betingade sannolikheterna kan sättas automatiskt på något sätt.

De olika målens attraktionskraft ses som de parametrar som påverkar fiendeintentionen. Modellen utgår alltså från antagandet att fienden tänker rationellt genom att maximera den förväntade nyttan med sitt handlande.

Fiendeintentionen antas påverka den spatiala parametern avstånd till mål och den temporala parametern riktning. Detta borde vara ett korrekt antagande eftersom fienden måste komma nära ett mål för att kunna attackera det, och därmed också röra sig mot målet. Om fienden inte ska attackera målet finns det fortfarande en viss möjlighet att denne befinner sig nära målet och/eller att denne rör sig mot målet, men sannolikheten är mindre än i det fall då fienden verkligen valt att anfälla målet. Brynielsson et al. (2005) vilka tagit fram ett verktyg för att försöka prediktera framtida trupprörelser bygger de inferenser som dras på parametrarna rörelse och hastighet, med vilket de fått goda resultat. Detta är ett tecken på att den temporala aspekten är viktig att ta hänsyn till.

Det resonemang som förts ovan om de olika parametrarna och deras kausala samband leder fram till den fullständiga modellen, vilken byggts som ett bayesianskt nätverk. I

modellen som kan ses i figur 5.6 visas det generella bayesianska nätverk som skapas ifall det finns två olika mål som fienden kan anfalla. När modellen implementeras antar de olika noderna såsom attraktionskraftMål1 istället riktiga namn som till exempel attraktionskraftStockholm, men i figuren visas alltså ett generellt nätverk.



Figur 5.6 Generellt bayesianskt nätverk då det finns två alternativa mål

5.3 Implementation av modellen i GTSIM

För att bland annat kunna utvärdera den bayesianska modellen har det tidigare konstaterats att denna bör förses med ett grafiskt användargränssnitt. Av den anledningen har den bayesianska modellen utvecklats som en integrerad del i GTSIM (Ground Target Simulator), vilket är ett simuleringsramverk utvecklat på Ericsson Microwave Systems i syfte att användas som en testbädd vid utveckling av nya metoder och koncept för just sensor- och informationsfusion (Warston och Persson, 2004). GTSIM är utvecklat i Java varför även den bayesianska modellen och integreringen av denna i GTSIM programmerats i Java. Som tidigare beskrivits har ett befintligt Java-API från tillverkaren Norsys använts för att konstruera det bayesianska nätverket.

Simulatorn emulerar olika typer av sensorer och informationskällor inom ett spatialt utspritt multisensorsystem för övervakning av markläget inom det nätverksbaserade försvaret (Warston och Persson, 2004). Av den anledningen är GTSIM utformat som ett multitrådat program som har möjlighet att köras distribuerat på olika datorer sammankopplade i ett LAN, genom att använda så kallad *remote invocation* i CORBA. Det faktum att GTSIM bygger på CORBA och är multitrådat gör att det blir betydligt mer komplext att integrera nya funktioner i GTSIM än om det varit byggt på en icke-distribuerad arkitektur.

Lägesbilden som GTSIM skapar kan antingen presenteras mot en vanlig kartbild eller genom att läsa in olika så kallade *shapes* från en avancerad kartdatabas. Kartdatabasen ger möjlighet att använda sig av vägnätet vilket i kapitel 3.3 gjordes som en avgränsning för att förminska rörelsefriheten för fiendeförbanden och därmed begränsa antalet handlingsalternativ.

5.3.1 ScenarioGenerator

För att kunna skapa och presentera scenarion med de egenskaper som önskas har modifieringar och tillägg gjorts till *ScenarioGenerator* vilket är ett av de olika

ingående paketen i GTSIM. Tidigare kunde rutter för olika markbaserade förband samt för flygande sensorer såsom UAV:er³ och aerostater⁴ skapas i denna, men nu finns det även möjlighet att skapa olika typer av mål samt att definiera ett skyddsvärde för de olika målen. Målens koordinater, typ och skyddsvärde kan sedan väljas att sparas undan till en fil för att senare läsas in i presentationsprogrammet. De olika mål som nu kan skapas är av typen artilleriförband, underhållsförband samt skytteförband. Alla dessa är implementerade som stillastående mål, det vill säga att de inte har möjlighet att förflytta sig.

5.3.2 VehiclePackage

När det gäller hanteringen av fordon sker denna i paketet *VehiclePackage*. Där finns sedan tidigare klasser och metoder för att generera trafik i form av både egna, fiendliga och neutrala markbaserade fordon, i allt från obepansrade jeepar till tunga stridsvagnar. Dessa fordon kan sedan associeras med en av de rutter som skapats tidigare. Det finns möjlighet att skapa flera olika grupper av förband vilka körs som separata trådar och där kommunikationen med presentationsprogrammet sker via CORBA, vilket ger möjlighet att distribuera ut dessa grupper på olika datorer i nätverket. Antalet tillgängliga typer av fordon har i denna version reducerats till tre för att kunna kopplas samman med stridsvagns-, pansarskytte- och skytteförband, vilket utgör de fiendetyper som tagits med i modellen. Ett annat tillägg som har gjorts till detta paket är att lägga till möjligheten att pausa alla fordon för att kunna låta en användare mata in sina skattningar av sannolikheten för fiendens olika handlingsalternativ. Själva pausningen märks av i presentationsskiktet men den faktiska pausningen av fordonstrådar med mera sköts i detta paket.

5.3.3 SensorPackage

SensorPackage är uppbyggt på ungefär samma sätt som *VehiclePackage*, men här handlar det istället om utsättandet av olika typer av sensorer, samt associering av flygrutter till dessa. Här finns också klasser och metoder för att definiera hur långt de olika sensorerna kan se, test av om objektet som sensorn försöker se befinner sig i ett skogsområde, och så vidare. Även här sker kommunikationen med presentationsprogrammet med hjälp av CORBA. Eftersom det väsentliga i detta arbete inte är sensordatafusionen utan de högre abstraktionsnivåerna situationsanalys och hotanalys sågs vid utvecklingsarbetet det faktum att objekten måste upptäckas av sensorer innan de presenteras för användaren som en nackdel, därför skapades en form av supersensor som kan se alla enheter var de än befinner sig.

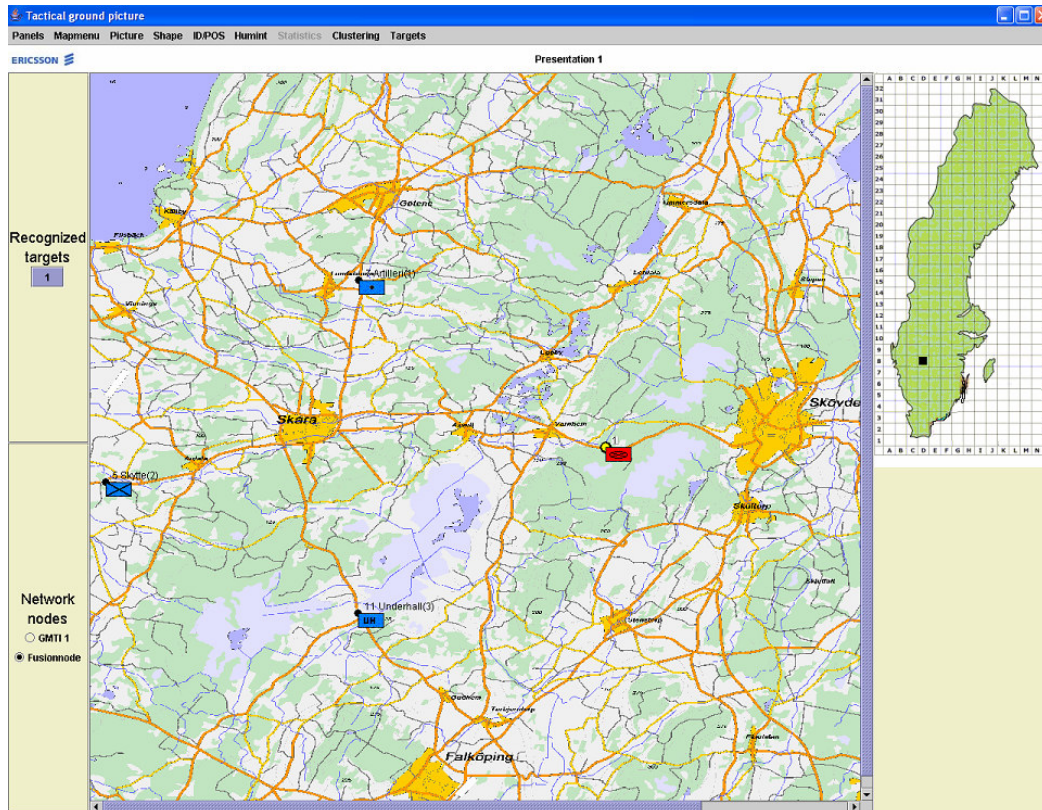
5.3.4 PresentationPackage

I presentationsprogrammet, vars klasser är definierade i *PresentationPackage* fusioneras data från de olika sensorerna samman till en gemensam lägesbild. Här har modifieringar gjorts så att det finns möjlighet att från en fil läsa in de statiska målen med dess sammanhörande egenskaper, som tidigare skapats i *ScenarioGenerator*. Dessa statiska mål presenteras sedan i den lägesbild som användaren ser för att denne visuellt ska kunna få en uppfattning om var fiendeförbanden förhåller sig till de egna målen. Ett exempel på en lägesbild med ett antal inlästa mål och ett fiendeförband kan ses i figur 5.7.

³ Unmanned Aerial Vehicle (UAV) är som namnet antyder en obemannad flygande farkost

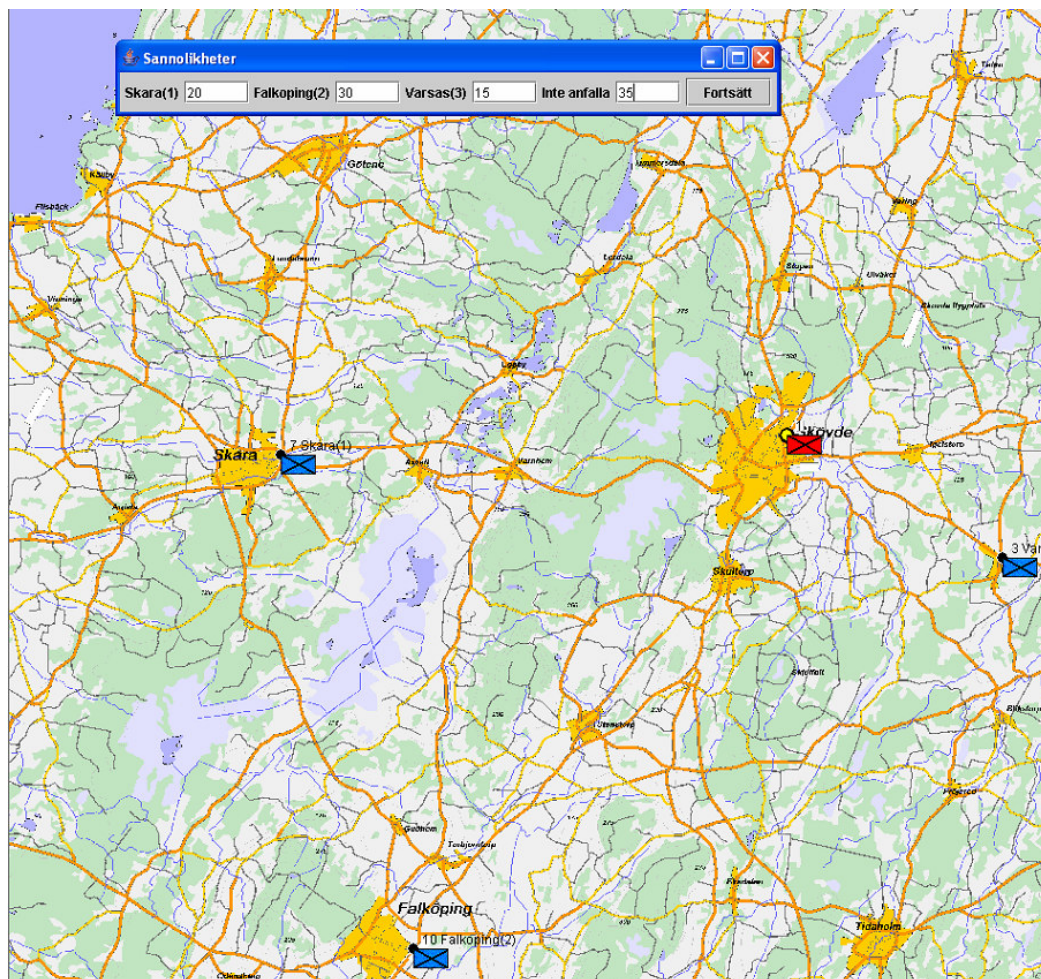
⁴ Aerostat är en typ av luftballong vilken i detta fall är utrustad med sensorer

Genomförande och resultat



Figur 5.7 Exempel på en lägesbild med en fiendeenhet och tre potentiella mål

Vidare finns det numera i presentationsprogrammet möjlighet att generera ett bayesianskt nätverk, där inferenser sedan dras för hur sannolika fiendens olika handlingsalternativ är, vilket beskrivs utförligare i stycke 5.3.5. Dessutom finns det numera möjlighet att pausa uppspelningen av ett scenario, detta för att programmet ska kunna användas till datainsamling, genom att en användare ska kunna mata in den sannolikhet som denne skattar för fiendens olika handlingsalternativ vid en viss tidpunkt i scenariot. Det går att välja på att simuleringen automatiskt ska pausas vid varje passerad vägpunkt eller att simuleringen manuellt pausas genom en knapptryckning då användaren tycker att programmets utdata skiljer sig ifrån de skattningar av sannolikheten som användaren gör. Ett exempel på en pausad simulering med tillhörande ruta för skattning av de olika sannolikheterna återfinns i figur 5.8.



Figur 5.8 Exempel på en pausad simulering med tillhörande dialogruta

5.3.5 BayInferencePackage

Om användaren väljer att skapa ett bayesianskt nätverk läses de olika handlingsalternativen in dynamiskt från presentationskiktet, det vill säga att om till exempel de två statistiska målen Stockholm och Södertälje lästs in genereras ett bayesianskt nätverk genom att skapa en instans av klassen *ConstructBN*, där noden fiendeintention får de möjliga tillstånden: anfalla Stockholm, anfalla Södertälje, samt inte anfalla. Noden fiendetyper får tillstånden stridsvagnsförband, skytteförband och pansarskytteförband i enlighet med vad som tidigare sagts i rapporten. När det gäller parametrarna attraktionskraft, skyddsvärde, måltyp, avstånd och riktning skapas för varje parameter n stycken noder, där n betecknar antalet handlingsalternativ (exklusive alternativet att inte anfalla). När de möjliga tillstånden för de olika noderna blivit satta är nästa steg att lägga till länkar mellan de olika noderna i enhetlighet med det generella nätverk som visades i figur 5.6. Med detta gjort läses betingade sannolikhetstabeller in för de olika noderna. När det gäller noderna fiendetyper, skyddsvärde och måltyp spelar värdet på dessas betingade sannolikhetstabeller inte någon roll eftersom det i dagsläget alltid läses in fullständig information om målens olika egenskaper och om fiendeförbanden. Om det i framtiden införs en osäkerhetsfaktor för dessa egenskaper kommer deras betingade sannolikhetstabeller spela en stor roll, men eftersom de nu aldrig behöver användas har ingen energi lagts

Genomförande och resultat

på att få dem rätt, varför värdet på dessa betingade sannolikheter fördelats uniformt mellan de olika tillstånden för dessa noder.

De övriga betingade sannolikhetstabellerna är mycket viktiga eftersom det är värdet på dessa i kombination med hur nätverket är uppbyggt som påverkar de resultat som fås ut av det bayesianska nätverket (Wang et al., 2002), det vill säga posteriorisannolikheten för noden fiendeintensions olika tillstånd. När dessa betingade sannolikhetstabeller ska sättas finns det därför två alternativ, att låta experter inom domänen sätta de olika sannolikheterna eller att basera dem på statistik hämtad från verklig data (Onisko och Druzdzal, 2003). Eftersom det inte funnits någon tillgång till verklig data skickades ett frågeformulär ut till Markstridsskolan, där militär expertis fick komma med åsikter om vilka typer av mål de olika sorternas fiendestyrkor kunde tänkas attackera, samt så fick expertisen bedöma attraktionskraften på en skala mellan 1 och 9 för alla kombinationer av tillstånd på parametrarna skyddsvärde, måltyp samt fiendetyper. Det bedömda värdet på attraktionskraften har sedan gjorts om, så att till exempel en 9:a ger en väldigt hög sannolikhet för att attraktionskraften är stor, en liten sannolikhet för medel och en väldigt låg sannolikhet för att attraktionskraften är liten. Anledningen till att experten inte fick bedöma attraktionskraften på detta sätt redan från början var att det kan kännas ganska onaturligt att sätta denna typ av sannolikheter för någon som inte är väl insatt i hur betingade sannolikhetstabeller fungerar.

De typer av mål som experten föreslog var artilleriförband, underhållsförband samt skytteförband. Ett artilleriförband bedöms (vilket även kan ses i tabell 5.4) som ett lämpligt mål för ett stridsvagnsförband, medan ett underhållsförband är ett lämpligt mål för ett pansarskytteförband, och där ett skytteförband i sin tur utgör ett lämpligt mål för ett fiendligt skytteförband.

Skyddsvärde	Måltyp	Fiendetyper	Stor	Medel	Liten
Högt	Artilleriförband	Stridsvagnsförband	0,80	0,15	0,05
Högt	Artilleriförband	Skytteförband	0,25	0,60	0,15
Högt	Artilleriförband	Pansarskytteförband	0,55	0,30	0,15
Högt	Underhållsförband	Stridsvagnsförband	0,55	0,30	0,15
Högt	Underhållsförband	Skytteförband	0,55	0,30	0,15
Högt	Underhållsförband	Pansarskytteförband	0,80	0,15	0,05
Högt	Skytteförband	Stridsvagnsförband	0,25	0,60	0,15
Högt	Skytteförband	Skytteförband	0,80	0,15	0,05
Högt	Skytteförband	Pansarskytteförband	0,25	0,60	0,15
Mellan	Artilleriförband	Stridsvagnsförband	0,70	0,20	0,10
Mellan	Artilleriförband	Skytteförband	0,20	0,40	0,40
Mellan	Artilleriförband	Pansarskytteförband	0,40	0,40	0,20
Mellan	Underhållsförband	Stridsvagnsförband	0,40	0,40	0,20
Mellan	Underhållsförband	Skytteförband	0,40	0,40	0,20
Mellan	Underhållsförband	Pansarskytteförband	0,70	0,20	0,10
Mellan	Skytteförband	Stridsvagnsförband	0,20	0,40	0,40

Genomförande och resultat

Mellan	Skytteförband	Skytteförband	0,70	0,20	0,10
Mellan	Skytteförband	Pansarskytteförband	0,20	0,40	0,40
Lågt	Artilleriförband	Stridsvagnsförband	0,25	0,60	0,15
Lågt	Artilleriförband	Skytteförband	0,05	0,15	0,80
Lågt	Artilleriförband	Pansarskytteförband	0,05	0,15	0,80
Lågt	Underhållsförband	Stridsvagnsförband	0,10	0,30	0,60
Lågt	Underhållsförband	Skytteförband	0,10	0,30	0,60
Lågt	Underhållsförband	Pansarskytteförband	0,25	0,60	0,15
Lågt	Skytteförband	Stridsvagnsförband	0,05	0,15	0,80
Lågt	Skytteförband	Skytteförband	0,25	0,60	0,15
Lågt	Skytteförband	Pansarskytteförband	0,10	0,30	0,60

Tabell 5.4 Sannolighetstabellen för noderna av typen attraktionskraft

När det gäller noden avstånd har olika indelningar av avstånden prövats fram, i syfte att åstadkomma en fungerande modell. Dessa har ändrats allteftersom, samt finjusterats i samband med en demonstration av systemet för en militärt insatt person (se kapitel 5.4). Avstånd är egentligen en kontinuerlig parameter men eftersom Netica inte kan hantera detta måste den delas upp i ett antal diskreta tillstånd. Den betingade sannolighetstabellen för noden avstånd återfinns i tabell 5.5.

Fiendeintention	0-3000	3001-5000	5001-8000	8001-12000	12001-15000	15001-20000	20001-25000	>25000
Anfalla X	0,25	0,20	0,15	0,13	0,12	0,07	0,05	0,03
Anfalla övriga	0,02	0,04	0,06	0,08	0,10	0,20	0,25	0,25
Inte anfalla	0,01	0,03	0,06	0,08	0,12	0,15	0,25	0,30

Tabell 5.5 Sannolighetstabellen för nod X av typen avstånd

Noden riktning har i dagsläget bara försetts med två tillstånd, mot och från. Ursprungligen var det tänkt att dessa skulle delas upp i finare nivåer, men eftersom denna grova indelning visat sig fungera bra har den fått vara kvar. Det är dock värt att notera att den grova indelningen gör att det finns en potentiell möjlighet att ”lura” modellen, genom att först försöka röra sig bort från målet som ska anfallas och sedan ändra riktning så sent som möjligt, men då fienden väljer att börja röra sig mot målet sticker sannolikheten snabbt upp för målet, varför det ändå gör det svårt att åstadkomma denna form av vilseledning.

Fiendeintention	Mot	Från
Anfalla X	0,70	0,30
Anfalla övriga	0,50	0,50
Inte anfalla	0,20	0,80

Tabell 5.6 Sannolighetstabellen för nod X av typen riktning

Genomförande och resultat

Den betingade sannolikhetstabellen för noden fiendeintention är problematisk att sätta eftersom både antalet föräldranoder och antalet tillstånd varierar beroende på antalet möjliga handlingsalternativ som läses in. Givet att det finns n stycken olika handlingsalternativ (exklusive alternativet att inte anfälla) finns det också n stycken olika noder med attraktionskraft. Eftersom var och en av dessa noder har tre stycken möjliga tillstånd (stor, medel och liten attraktionskraft) består den betingade sannolikhetstabellen för fiendeintention av 3^n rader. Vid två och tre handlingsalternativ är storleken hanterbar (nio respektive tjugosju rader) men eftersom storleken på tabellen växer exponentiellt blir det snabbt ohållbart att manuellt sätta de betingade sannolikhetstabellerna för noden fiendeintention. Möjligtvis går det att skapa en algoritm som på ett smidigt sätt automatiskt genererar en rimlig sannolikhetstabell, men eftersom detta klart är utanför detta arbetes problemställning har valet gjorts att begränsa antalet potentiella mål till tre. Ett annat alternativ skulle också kunna vara att från början fördela sannolikheterna uniformt mellan de olika tillstånden och sedan använda riktig data, exempelvis från historiska militära scenarion för att lära sig utifrån dessa data och på så sätt använda dessa för att förändra sina betingade sannolikhetstabeller.

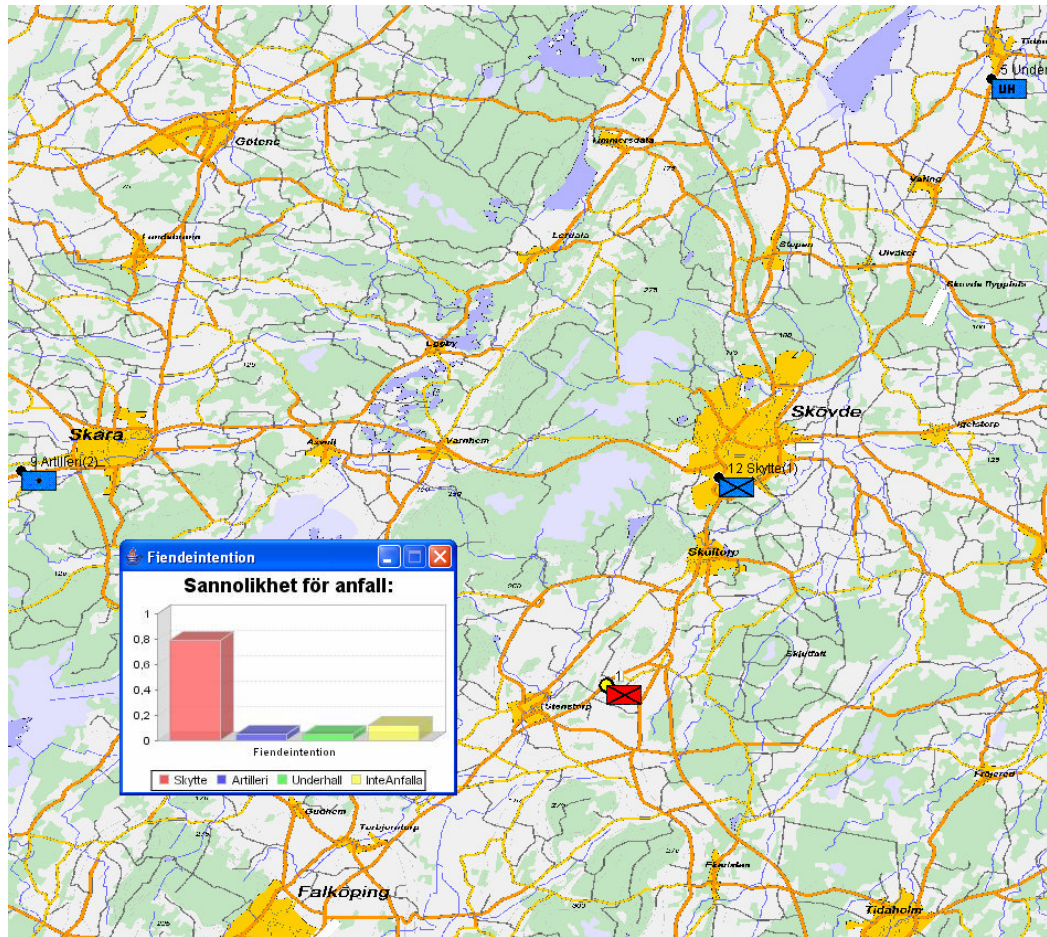
För att få fram den betingade sannolikhetstabellen för fiendeintention då det finns tre potentiella mål fick även här en expert från Markstridsskolan hjälpa till. Då det förutsattes att militära experter känner sig mer bekväma i situationen att fördela ut trupper än att ange värden i en sannolikhetstabell presenterades situationer där det fanns tre stycken olika mål med kända attraktionskrafter. För varje kombination av attraktionskrafter hos de olika målen fick experten fördela ut nio extra försvarsenheter mellan de olika målen (vilka alla hade ett grundförsvar från början). Fördelningen av dessa enheter mellan målen översattes sedan till värden på betingade sannolikheter på samma sätt som för attraktionskraft. Den riktiga tabellen är egentligen betydligt större än tabell 5.7 eftersom det till exempel kan vara mål 3 som har en stor attraktionskraft och mål 1 och mål 2 har en liten attraktionskraft, men då sannolikheterna blir desamma har denna redundanta information plockats bort, läsaren får istället titta på den rad där ett mål har stor attraktionskraft och två mål har liten attraktionskraft, oavsett vilken aktuell instans av ett mål som det råkar vara.

Attraktionskraft mål 1	Attraktionskraft mål 2	Attraktionskraft mål 3	Anfalla mål 1	Anfalla mål 2	Anfalla mål 3	Inte anfälla
Stor	Stor	Stor	0,30	0,30	0,30	0,10
Stor	Stor	Medel	0,35	0,35	0,15	0,15
Stor	Stor	Liten	0,40	0,40	0,05	0,15
Stor	Medel	Medel	0,40	0,20	0,20	0,20
Stor	Medel	Liten	0,40	0,20	0,10	0,30
Stor	Liten	Liten	0,60	0,10	0,10	0,20
Medel	Medel	Medel	0,25	0,25	0,25	0,25
Medel	Medel	Liten	0,30	0,30	0,10	0,30
Medel	Liten	Liten	0,40	0,10	0,10	0,40
Liten	Liten	Liten	0,10	0,10	0,10	0,70

Tabell 5.7 Sannolikhetstabellen för fiendeintention (tre mål)

Genomförande och resultat

När det bayesianska nätverket är färdigskapat sparas det undan, varpå det kompileras av den klass som drar inferenser. I nästa steg läses de egenskaper som påverkar de olika målens attraktionskraft in, det vill säga tillstånden på parametrarna skyddsvärde, måltyp och fiendetyper. Därpå skapas en separat tråd som var femte sekund läser av fiendestyrkans position, räknar ut om fiendestyrkan rör sig mot eller från de olika målen samt drar inferenser om sannolikheten för att de olika målen ska anfallas. Dessa sannolikheter presenteras för användaren i form av ett stapeldiagram som alltså uppdateras med jämna intervall. Ett exempel på detta kan ses i figur 5.9 nedan.



Figur 5.9 Exempel på lägesbild med tillhörande stapeldiagram

Den skapade tråden körs till användaren väljer att stoppa den. Den kod som har utvecklats för att åstadkomma ovanstående beskrivning kan sammanfattas med den övergripande pseudokod som återfinns i figur 5.10.

```

läsInHandlingsalternativ()
skapaNät()
sättBetingadeSannolikheter()
kompileraNät()
läsInEgenskaper()
while (not stoppad) do
    for i ← 1 to antalMål do
        beräknaAvstånd(EUKLIDISKT, i)
        sättAvstånd(i)
        beräknaRiktning(i)
        sättRiktning(i)
    end
    draInferenser()
    uppdateraDiagram()
end

```

Figur 5.10 Pseudokod för implementationen av det bayesianska nätverket

I pseudokoden går det att se att avståndet som beräknas fram är euklidiskt. Det går även att beräkna avståndet utifrån det allmänna vägnätet genom att detta läses in från shape-lagren varpå en algoritm som bygger på A* söker reda på den kortaste vägen till de olika målen. Denna algoritm är tagen från ett annat projekt som bygger på GTSIM. Anledningen till att den euklidiska formen av avståndsmätning används som standard är att avståndet utifrån vägnätet beräknas felaktigt vid vissa punkter på lägesbilden, troligtvis på grund av fel i shape-lagren. Detta får till konsekvens att fienden kan bedömas vara på väg bort från ett mål när den egentligen närmar sig, vilket kan få effekter på sannolikhetsberäkningarna för en stund. Även den euklidiska avståndsmätningen kan ställa till vissa problem eftersom en fiende kan närma sig ett mål rent euklidiskt sett, trots att denne egentligen rör sig bort från målet (och vice versa) eftersom fienden följer en väg. Om det framtagna verktyget i framtiden ska användas till mer realistiska tillämpningsområden vore det därför på sin plats att åtgärda så att avståndsmätningen utifrån vägnätet fungerar precis som den ska.

5.4 Utvärdering av modellen

Utvärderingen av modellen sker i två steg, vilket har nämnts tidigare i rapporten. Det ena steget är att undersöka hur väl de sannolikheter som ges som utdata av modellen stämmer överens med ”verkligheten”. Detta görs bland annat genom att demonstrera modellens utdata för ett antal olika scenarion för en militär expert och be denne att bedöma de skattade sannolikheter som presenteras av programmet. Det andra steget är att utvärdera vad tilltänkta användare tycker om själva det grafiska verktyget, samt vad de anser om den funktionalitet som verktyget erbjuder. Utöver detta vore det även intressant att höra vad potentiella framtida användare av verktyget vill ha för extra funktionalitet tillagd för att de ska kunna få så stor nytta som möjligt av verktyget.

5.4.1 Utvärdering av den framtagna modellen

För att kunna göra en utvärdering av den modell som gjorts är det lämpligt att de sannolikheter som ges som utdata i ett visst scenario jämförs med en militär experts skattningar av sannolikheterna för samma scenario. Av den anledningen har det utvecklade programmet försetts med en möjlighet att pausa uppspelningen av de olika scenarierna så att en expert kan mata in dennes skattningar av sannolikheten för fiendens olika handlingsalternativ, vilket har beskrivits tidigare i rapporten. Utvärderingen kan därför ske på två sätt: det första alternativet är att de skattade sannolikheterna hela tiden presenteras för experten så att denne kan pausa manuellt när denne tycker att sannolikheterna avviker från det förväntade och mata in den sannolikhet som experten tycker är mer rimlig. Det andra alternativet är att dölja de skattade sannolikheterna för experten och att scenariot pausas automatiskt vid vissa i förväg utvalda vägpunkter.

Vid en utvärdering med en militär expert⁵ från Markstridsskolan framkom att de parametrar som nu finns med i modellen alla är relevanta för vilket handlingsalternativ som fienden kan tänkas välja, det vore dock önskvärt att komplettera den med en parameter som säger något om målets stridsvärde, det vill säga hur starkt dess försvar är. I dagsläget är de olika målen och fiendeförbanden representerade som förband med ospecificerad storlek. Detta gör enligt experten att alternativet ”inte anfalla” för en militär expert blir det troligaste i nästan alla scenarion eftersom styrkeförhållandena är mycket viktiga att beakta innan ett anfall görs. Om inte fiendestyrkan är numerärt eller på annat sätt styrkemässigt överlägsen är det väldigt ovanligt att anfalla. På grund av detta gjordes ingen riktig skattning av olika handlingsalternativ med denne expert eftersom denne menade på att så länge som styrkeförhållandena inte är kända så måste det troligaste handlingsalternativet vara att inte anfalla, i nästintill alla situationer.

Utöver tillägget med styrkeförhållanden ansågs modellen i övrigt som enkel och bra. Ytterligare parametrar som skulle kunna göra modellen än mer realistisk i framtiden diskuterades också, exempel på sådana ansågs till exempel vara huruvida ett mål är isolerat eller ej och om det finns några mineringar utlagda. På de internationella uppdrag som våra styrkor ofta befinner sig på är det också vanligt att det inte bara finns en motpart, utan snarare flera stycken. Dessa byter ofta lojalitet och handlar ofta inte efter militära mönster utan mer svåröversägligt. Om det på något sätt skulle gå att få med liknande saker i en framtida modell skulle det vara mycket värdefullt men är antagligen oerhört komplext. Sammanfattningsvis ansåg denne alltså att modellen var bra men borde kompletteras med en parameter som beskrev styrkeförhållandena. På sikt skulle en stor mängd parametrar kunna läggas till modellen och skapa ett verktyg som är mer situationsanpassat och arbetar med kritiska sårbarheter. Detta skulle kunna få till följd att olika typer av effekter, såsom att ett förband är ytterst sårbart då det börjar få slut på drivmedel, kan avspeglas i modellen.

Vid samtal med en annan militärt kunnig person framkom även där att storleken på förbandet bör spela roll för modellens skattningar av sannolikheten för de olika handlingsalternativen. Med denne gjordes även en uppspelning av ett scenario där han fick information om att försvaret var lika stort vid alla de olika potentiella målen. Uppspelningen pausades vid ett antal vägpunkter där han fick skatta sannolikheten för de olika handlingsalternativen, varpå dessa bedömningar lagrades undan. Vid en

⁵ C TaUtvsekt/MSS

jämförelse med de sannolikheter som modellen skattat vid samma vägpunkter visade sig överensstämelsen vara överraskande god, med tanke på att modellen i dagsläget är så pass grov som den är och att ingen finjustering gjorts av de betingade sannolikheterna. Givetvis kan inte alltför generella slutsatser dras på jämförelse av ett enda scenario, men vid fem av de sex vägpunkter som scenariot bestod av, överensstämde den militärt kunnige personens skattningar om den inbördes ordningen mellan sannolikheterna för de olika handlingsalternativen med inferensmotorns skattningar. Procentuellt sett skiljde sig skattningarna en del åt, men det intressanta är knappast om sannolikheten är 7 % eller 10 % för att ett mål ska anfallas, utan snarare om det är hög eller låg sannolikhet för det. Någon närmare utvärdering av modellen än så här har inte gjorts eftersom fokus ligger på att empiriskt undersöka möjligheterna för att bygga modellen snarare än att jämföra dess utdata med experters skattningar.

5.4.2 Utvärdering av det framtagna verktyget

När det gäller det framtagna verktyget var kommentarerna mycket positiva. Den militäre experten ansåg att det antagligen inte är så användbart under förloppet för en snabbt uppkommen situation eftersom besluten då måste tas mycket snabbt och det snarare är erfarenhet och magkänsla som bedömningarna grundar sig på än sannolikhetsberäkningar. Däremot såg han en stor potential att använda verktyget i planeringsskedet av olika operationer, då det i detta läge är mycket intressant att kunna spela igenom olika tänkbara scenarion för att kunna tänka igenom alternativa framtida händelseutvecklingar i förväg.

När det gällde frågan om verktyget sett utifrån ett datainsamlingsperspektiv ansåg experten att det är bra att låta pausningen ske automatiskt vid varje vägpunkt, istället för att visa modellens utdata och endast pausa manuellt då modellens skattningar inte stämmer överens med användarens. Anledningen till detta är att han ansåg att det på det här sättet finns en möjlighet att i lugn och ro tänka efter istället vid varje situation istället för att det annars finns en risk för att någon viktig avvikelse inte uppmärksammas på grund av att användaren inte hinner tänka efter på samma sätt.

Samtalet med den andre militärt kunnige personen hade också positiva tongångar. Denne såg en rad potentiella användningsområden för det framtagna verktyget, speciellt vid en vidareutveckling av detta. Ett mycket intressant förslag var att utföra precis den typ av datainsamling som verktyget i dagsläget kan användas till, men att dessutom komplettera utrustningen med en bandspelare, där användaren vid varje ny bedömning av de olika sannolikheterna får redogöra för hur denne tänker när han/hon skattar sannolikheten för fiendens olika handlingsalternativ. På detta sätt skulle det gå att analysera och dokumentera på vilka grunder en person gör sina bedömningar och till exempel använda detta som ett steg i utbildningen för nyinryckta befäl på lägre nivåer.

5.5 Finjustering av modellen

För att kunna finjustera den framtagna modellen kan små justeringar göras av de betingade sannolikhetstabellerna. Eftersom det framtagna verktyget kan användas för att samla in data är det lämpligt att undersöka möjligheterna att använda insamlad data till att få modellens utdata att efterlikna de sannolikheter som en mänsklig beslutsfattare har skattat för samma situation. Genom att använda ett verktyg för *känslighetsanalys* går det att identifiera de parametrar som med minsta möjliga förändring kan anpassa modellen att ge de önskade resultaten (Chan och Darwiche,

2002). Ett exempel på ett verktyg som kan utföra denna typ av analys är SamIam⁶ (Sensitivity Analysis, Modeling, Inference And More), vilket som namnet antyder är kapabelt att utföra mycket mer än bara känslighetsanalys.

Eftersom den framtagna modellen behöver kompletteras med åtminstone parametern styrkeförhållande/storlek på förband för att kunna ge tillförlitliga predikteringar av fiendeintentionen finns det ingen större anledning att finjustera den framtagna modellen, men en beskrivning kommer ändå här att göras av hur de betingade sannolikheterna hos en utökad modell skulle kunna finjusteras.

5.5.1 Identifiering av lämpliga ändringar

För att det framtagna nätverket ska kunna göra bedömningar som är mer lika den mänskliga användarens behöver dess betingade sannolikhetstabeller alltså uppdateras. Detta kan göras genom att i exempelvis SamIam importera det bayesianska nätverk som skapas för det aktuella scenariot, då scenariot presenteras i GTSIM. Nästa steg är att ändra till *Query Mode* i SamIam, samt att mata in de fakta som var kända vid den aktuella vägpunkten i scenariot, det vill säga typen av fiendeförband, de olika måltyperna, målens olika skyddsvärden, avstånden till de olika målen, om fienden hade riktningen mot eller från de olika målen samt de övriga parametrar som implementerats i en framtida modell. Med detta gjort väljs i SamIam att göra en känslighetsanalys för noden fiendeintention. Genom att sätta en *restriktion* (constraint) på posteriori-sannolikheten för ett tillstånd som är önskvärt att förändra för en viss fråga kan SamIam hjälpa till med att hitta de förändringar av de betingade sannolikhetstabellerna som krävs för att med minsta möjliga förändring justera nätverket så att det klarar av att uppfylla den satta restriktionen. De föreslagna ändringarna presenteras då av SamIam, vilka kan godkännas om de ser lämpliga ut, varpå de betingade sannolikhetstabellerna uppdateras. För att kunna göra dessa förändringar i programkoden krävs det manuella ändringar, men detta är lätt gjort eftersom det i programmet går att se exakt vilka rader i de olika betingade sannolikhetstabellerna som behöver förändras.

⁶ <http://reasoning.cs.ucla.edu/samiam/>

6 Relaterat arbete

I detta kapitel positioneras det gjorda arbetet i förhållande till andra arbeten inom samma problemområde. Vidare jämförs likheter och skillnader mellan övriga arbeten och detta examensarbete, både när det gäller problemställning och tillvägagångssätt.

6.1 Enhanced Situation Awareness using Random Particles

I det arbete som är utfört av Brynielsson et al. (2005) presenteras ett generiskt verktyg för att prediktera framtida trupprörelser. Genom att använda ett GIS (geografiskt informationssystem) för att kunna beräkna trupperns rörelsehastighet i olika former av terräng på ungefär samma sätt som skett i GTSIM i detta arbete, har ett dynamiskt bayesianskt nätverk använts för att prediktera fiendens trupprörelser. Ett dynamiskt bayesianskt nätverk kan ses som ett antal sammankopplade bayesianska nätverk, där var och ett av de olika nätverken representerar en viss tidsperiod (Brynielsson et al., 2005). Ett dynamiskt bayesianskt nätverk kan därför användas för att göra en modell av en domän som förändras över tid. Med andra ord fångas i deras arbete den temporala aspekten på ett bättre sätt än vad som gjorts i detta arbete, vilket endast baserar sannolikhetsberäkningarna för fiendens olika handlingsalternativ på den nuvarande lägesbilden, med undantag för parametern riktning vilken även baseras på föregående tidsperiod. Det vore bättre att basera sannolikhetsberäkningarna på ett flertal tidssteg bakåt i tiden, varför det skulle kunna tänkas vara lämpligt att i framtiden använda ett dynamiskt bayesianskt nätverk även här. För att kunna beräkna sannolikhetsdistributionen för en enhets framtida position har en metod som Brynielsson et al. (2005) kallar för slumpmässiga partiklar tagits fram, vilken bygger på tekniken partikelfiltrering.

Även om det finns likheter mellan mitt och arbetet som Brynielsson et al. (2005) gjort, så finns det också stora skillnader. De bryr sig till exempel inte om olika mål och liknade utan bygger sannolikhetsberäkningarna på enbart enhetens rörelseriktning och dess hastighet. I båda arbetena görs alltså prediktering av var olika enheter kommer att befinna sig i framtiden men Brynielsson et al. (2005) gör det genom att endast koncentrera sig på ovanstående parametrar medan jag försöker beräkna vilket av ett antal olika handlingsalternativ som fienden kommer att välja i framtiden, beroende på vilken nytta fienden kan erhålla av de olika handlingsalternativen kombinerat med parametrarna avstånd och riktning till de olika målen.

Något som kan vara värt att notera är de fälttest som gjorts av deras verktyg under en stor militärövning. En del av den feedback som gavs av de operatörer som testade systemet är att de på sin nivå inte i dagsläget har till uppgift att försöka prediktera framtiden utan istället rapportera vad som har hänt och vad som för tillfället händer. Dock trodde operatörerna att funktionaliteten i systemet passar beslutsfattare på en högre nivå mycket bra (Brynielsson et al., 2005). Detta är erfarenheter som antagligen gäller för även detta arbete.

6.2 Representation and Recognition of Uncertain Enemy Policies Using Statistical Models

Detta är namnet på ett arbete skrivet av Suzić (2003), som även har publicerat ett antal andra rapporter inom detta ämne. Han har använt sig av ett bayesianskt nätverk för att representera kunskap om fienden (i form av dennes doktrin med mera) och

Relaterat arbete

kombinerat detta med ett dynamiskt bayesianskt nätverk som drar inferenser baserat på data från sensorer, såsom fiendeposition. Nätverket är alltså tänkt att dra inferenser om vilket sätt fienden troligtvis kommer att handla på i framtiden, baserat på dels data om var fienden befinner sig och dels på den kunskap som finns om fiendens doktrin. Den framtagna modellen har sedan använts för simuleringar av ett antal olika scenarion i MATLAB⁷.

Arbetet är på sätt och vis likt det arbete som presenteras i denna rapport, i och med att syftet i båda fallen är att försöka förutsäga fiendens framtida handlingar. Tillvägagångssätten skiljer sig dock åt i den mån att jag i mitt arbete lagt ett stort fokus på den grafiska simuleringen av de olika scenariona och att den framtagna modellen ska kunna finjusteras med hjälp av den datainsamling som det framtagna verktyget erbjuder. Suzić (2003) har istället valt att fokusera på användandet av extra information i form av kunskaper om olika fiendedoktriner. Detta är ett mycket intressant område eftersom det drar nytta av alla de fördelar som den höga nivån hotanalys i informationsfusionsprocessen erbjuder.

I en eventuell fortsättning på det arbete som presenterats i denna rapport skulle det kunna vara mycket givande att kombinera den nuvarande modellen med extra information som kan hämtas ifrån databaser (såsom till exempel olika fiendedoktriner).

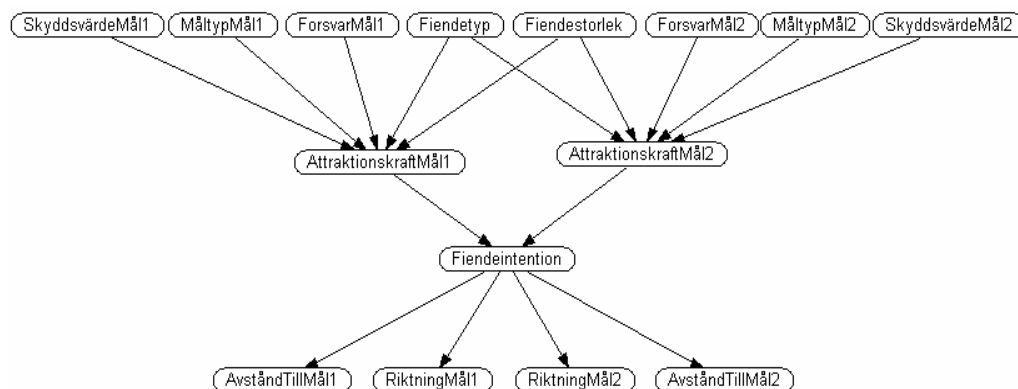
⁷ <http://www.mathworks.com/products/matlab/>

7 Slutsatser

I detta kapitel presenteras en sammanfattning av de resultat som arbetet resulterat i, samt så ges olika förslag på framtida arbeten.

7.1 Modellen

Den har visat sig fullt möjligt att bygga en modell som bygger på bayesiansk hypotesprövning (i detta fall i form av ett bayesianskt nätverk) för att prediktera vad fienden har för intentioner. Den modell som tagits fram är ett första försök och behöver kompletteras för att vara verkligt användbar (framförallt med parametern styrkeförhållande/förbandsstorlek) men visar tydligt de möjligheter som denna teknik erbjuder. Modellen i sig är inte svår att komplettera, då det svåra inte har varit att ta fram själva modellen utan snarare att implementera modellens olika parametrar i GTSIM. Eftersom det mesta arbetet nu är gjort borde det dock inte vara några problem med att i GTSIM erbjuda möjligheten att definiera till exempel styrkeförhållanden, då detta bör kunna göras på samma sätt som målets skyddsvärde kan definieras, då ett scenario skapas idag. Om parametern styrkeförhållande/förbandsstorlek implementeras kan det resulterande nätet se ut som i figur 6.1 för ett scenario med två alternativa mål. Observera dock att denna parameter inte är implementerad i dagsläget utan att nätet idag ser ut som i figur 5.6.



Figur 6.1 Generellt bayesianskt nätverk då det finns två alternativa mål och med tillägget att målet har ett definierat försvar och fienden en storlek

Övriga parametrar som militära experter under arbetets gång har påpekat kan vara viktiga för vad fienden har för intentioner, är huruvida de olika målen är isolerade eller ej, samt vilka andra typer av försvar som finns vid målen, såsom mineringar med mera. Önskemål har också framkommit på att göra modellen mer dynamisk för olika situationer, genom att identifiera olika typer av kritiska sårbarheter.

En sak som visat sig vara svår vid skapandet av modellen, som kan ställa till problem om modellen görs större i framtiden, är att fylla vissa av dess betingade sannolikhetstabeller med data. Attraktionskraft som i verkligheten antagligen påverkas av betydligt fler parametrar har i detta arbete endast haft tre föräldranoder, men om en så realistisk modell som möjligt skulle byggas skulle antalet föräldranoder antagligen bli större (till exempel styrkan på målets försvar och storleken på fiendeförbandet). Dessa parametrar skulle också kunna anta ett antal möjliga tillstånd, vilket skulle kräva än större betingade sannolikhetstabeller för attraktionskraft. Rent beräkningsmässigt är detta troligtvis inga problem, men däremot blir det ansträngande att fylla tabellen med relevanta värden. Med en del möda skulle detta antagligen vara

möjligt ändå, eftersom det bara behöver göras en gång, men det skulle ändå vålla besvär att med hjälp av experter ta fram alla de värden det handlar om.

Än mer problematiskt är det dock med parametern fiendeintention. Storleken på den betingade sannolikhetstabellen för denna parameter är dynamisk eftersom den är beroende av antalet möjliga handlingsalternativ. Som tidigare konstaterats består denna tabell av 3^n handlingsalternativ plus alternativet att inte anfälla. Skulle det som ett exempel finnas åtta potentiella handlingsalternativ skulle detta därför leda till en tabell på mer än 6500 rader. Eftersom antalet handlingsalternativ beror på antalet mål som användaren anser det rimligt att fienden kan tänkas anfälla så är det inte säkert att antalet handlingsalternativ kan bli så stort, men å andra sidan är det också troligt att parametern attraktionskraft egentligen ska kunna anta ett större antal tillstånd än de tre tillstånd som kan antas i dagsläget. Om antalet möjliga tillstånd för attraktionskraft ökar till exempelvis fem leder detta till att storleken på tabellen istället uppgår till 5^n rader, där faktorn alltså svarar mot antalet tillstånd hos attraktionskraft. Beräkningsmässigt skulle detta antagligen inte leda till annat än att beräkningarna tar lite längre tid, men för att skapa en tabell vars storlek kan förändras dynamiskt på detta sätt krävs det att värdena i den betingade sannolikhetstabellen kan sättas automatiskt med någon algoritm, istället för att en människa manuellt ska behöva sitta och mata in värdena.

En annan lösning på problemet skulle kunna vara att börja med betingade sannolikhetstabeller där värdena från början är uniformt fördelade mellan de olika modernas tillstånd. Genom att använda data från riktiga fall skulle då nätverket kunna lära sig från dessa data och på så sätt förändra sina betingade sannolikheter utifrån vad det lärt sig. Funktioner för att göra denna typ av lärande finns inbyggda i många av de program som finns tillgängliga, däribland Netica. Det problematiska med denna lösning är därför att få tillgång till denna form av data, dock borde det vara möjligt att använda sig av data från gamla krigsscenario, som till exempel olika scenarion från andra världskriget, även om krigsföringen inte ser ut på samma sätt idag. Ett alternativ till detta är att använda den teknik som har beskrivits för att finjustera modellen utifrån insamlad data. Denna typ av justeringar är dock troligtvis svåra att göra på en modell där de betingade sannolikhetstabellerna är helt felaktiga, utan är istället tänkt att användas för de sista små justeringarna av de betingade sannolikhetstabellerna för att modellen ska bli så bra som möjligt.

I detta arbete valdes tidigt en inriktning mot den bayesianska metodiken, vilket fick till följd att bayesianska nätverk använts för att implementera modellen som ska förutsäga fiendens intentioner. Det är dock viktigt att tillägga att implementationen i GTSIM inte alls är särskilt beroende av att inferensmotorn bygger på bayesianska nätverk. Detta gör att det finns möjlighet att implementera inferensmotorn så att den istället bygger på exempelvis Dempster-Shafer och på så sätt använda mycket av den kod som skrivits i detta arbete för att utvärdera en helt annan teknik än bayesianska nätverk.

7.2 Det grafiska verktyget

Det grafiska verktyget som kan användas för att spela upp olika händelseförlopp (det vill säga olika scenarion), beräkna sannolikheten för olika handlingsalternativ med hjälp av modellen som fungerar som inferensmotor, samt att samla in data för vad användaren bedömer de olika sannolikheterna till, vilket i sin tur kan användas för att finjustera modellen, fungerar mycket bra. Grunden till verktyget fanns redan från början i form av GTSIM, men det är också mycket ny funktionalitet som har

implementerats, framförallt skapande och inläsning av mål (handlingsalternativ), sannolikhetsberäkningar, samt funktioner för att använda verktyget för att samla in data.

Dessa nya funktioner som implementerats i GTSIM har, enligt militärt insatta bedömare, flera olika potentiella användningsområden. Genom att komplettera datainsamlingsverktyget med en bandspelare går det att analysera och dokumentera på vilka grunder en användare gör olika bedömningar och på så sätt använda verktyget i utbildningssyfte. Ett annat tillämpningsområde kan med en del modifieringar vara att använda verktyget i planeringsfasen av en militär operation. GTSIM är från början en mycket kraftfull testbädd för att testa olika nya tekniker och koncept inom informationsfusion och detta gör att tillägg såsom möjligheten att skapa olika typer av mål samt en inferensmotor för beräkning av olika sannolikheter kan ligga till grund för en rad olika ytterligare påbyggnader.

7.3 Förslag på framtida arbete

Då detta arbete har lett fram både till en fungerande implementation av ett bayesianskt nätverk för att prediktera fiendens framtida handlande, samt ett verktyg för att finjustera den framtagna modellen, finns det två olika vägar att gå när det gäller framtida arbete. Den ena vägen är att försöka vidareutveckla modellen genom att byta ut det bayesianska nätverket mot exempelvis ett dynamiskt bayesianskt nätverk och på så sätt lägga större vikt vid den temporala dimensionen, eller att göra modellen mer realistisk genom att lägga till parametrar såsom styrkan på försvaret vid de olika målen i enlighet med det förslag som presenterats i figur 6.1. Ett annat sätt att utveckla den framtagna modellen på är genom att kombinera den med extra information inläst från databaser på ungefär samma sätt som beskrivits i kapitel 6.2. Det vore också av intresse att försöka generera de potentiella handlingsalternativen automatiskt (till exempel genom terränganalys) för att operatören själv ska slippa försöka analysera var fienden kan tänkas anfälla. Det är dock viktigt att komma ihåg att modellen ska finnas som ett stöd för beslutsfattaren, den kan aldrig ersätta någon beslutsfattare.

Den andra alternativa vägen är att fortsätta arbetet med den del av verktyget som kan användas till datainsamlande. Genom att samla in en stor mängd data från olika simuleringar som presenteras för olika experter kan undersökningar göras av hur samstämmiga experterna är vid sättandet av olika betingade sannolikheter samt vid skattningar av posteriori-sannolikheter om vad fienden kommer att göra i framtiden. Om det visar sig att experter sätter väldigt olika sannolikheter eller att till och med samma expert sätter olika sannolikheter för ett och samma scenario som presenteras för denne vid två olika tillfällen kan det vara värt att fundera över hur tillförlitlig modellen egentligen kan bli. Det vore också av stort intresse att utvärdera hur känslig en realistisk modell är för små förändringar av de betingade sannolikheterna. Om det räcker med små förändringar för att resultaten ska ändras väldigt mycket är detta ett tecken på att modellen inte är så stabil som det vore önskvärt.

Utöver dessa förändringar av modellen eller av verktyget för datainsamling finns det även mycket annat att gå vidare med, i dagsläget finns det exempelvis bara en fiendeenhet att ta hänsyn till då sannolikhetsberäkningarna görs, men vad händer om det finns flera tusen enheter? För att kunna lösa sådana problem behöver det antagligen finnas möjlighet att programmet själv kan klustra ihop enstaka fiendeenheter till större förband, på exempelvis plutons-, kompani- eller bataljonsnivå, beroende på vilken nivå som studeras.

Tack

Jag vill först och främst tacka min handledare Mikael Johannesson för all den tid och allt det engagemang som han lagt ned på detta arbete. Ett stort tack vill jag också rikta till min sambo Marie och min familj för allt stöd jag fått under arbetets gång.

Vidare vill jag tacka min examinator Lars Niklasson, Håkan Warston (EMW) samt överstelöjtnant Lennart Ottosson (MSS) för alla era förslag, åsikter och er konstruktiva kritik.

Utan synpunkter från personer som Joel Brynielsson (Nada/KTH), Erik Lindberg (FOI) samt Robert Suzić (FOI) skulle detta arbete inte ha haft samma inriktning som det nu har fått, tack för er hjälp och för era värdefulla kommentarer.

Slutligen vill jag också tacka Marc Romanycia och Brent Boerlage på företaget Norsys för er hjälp med teknisk support och med licenser för Netica.

Jag vill dock klargöra att de personer som nämnts ovan inte på något sätt kan hållas ansvariga för eventuella fel i detta examensarbete. Alla de slutsatser, påståenden och eventuella felaktigheter som förekommer i denna rapport är enbart mina egna.

Fredrik Johansson

Juni 2005

Referenslista

- Arnborg, S., Artman, H., Brynielsson, J. & Wallenius, K. (2000) Information Awareness in Command and Control: Precision, Quality, Utility. *Proceedings of the Third International Conference on Information Fusion*, 25-32.
- Askelin, J.-I. (2001) Utan fusion stannar beslutscirkeln, *Framsyn*, 2, 24-25.
- Balasubramanian, P., Nochur, K., Henderson, J.C. & Millie Kwan, M. (1999) Managing Process Knowledge for Decision Support. *Decision Support Systems* 27, 1, 145-162.
- Borges, M., Pino, J. & Valle, C. (2005) Support for decision implementation and follow-up. *European Journal of Operational Research*, 160, 336-352.
- Brynielsson, J. (2002) A Decision-Theoretic Framework Using Rational Agency. *Proceedings of the 11th Conference on Computer-Generated Forces and Behavioral Representation*, 459-463.
- Brynielsson, J. & Arnborg, S. (2005) Refinements of the Command and Control Game Component. Manuskript.
- Brynielsson, J., Engblom, M., Franzén, R., Nordh, J. & Voigt, L. (2005) Enhanced Situation Awareness using Random Particles. *Proceedings of the Tenth International Command and Control Research and Technology Symposium*.
- Chan, H. & Darwiche, A. (2002) When do Numbers Really Matter? *Journal of Artificial Intelligence Research*, 17, 265-287.
- Cruz, A. & Beliakov, G. (1996) On the interpretation of certainty factors in expert systems. *Artificial Intelligence in Medicine* 8, 1, 1-14.
- Das, B. (1999) *Representing Uncertainties Using Bayesian Networks*. Teknisk rapport från Information Technology Division Electronics and Surveillance Research Laboratory. DSTO-TR-0918
- Davies Withers, S. (2002) Quantitative methods: Bayesian inference, Bayesian thinking. *Progress in Human Geography* 26, 4, 553-566.
- Försvarsmakten (2002) *Militärstrategisk doktrin*. Fälth & Hässler, Värnamo.
- Heckerman, D. (1999) A Tutorial on Learning with Bayesian Networks. *Learning in Graphical Models*, MIT Press, Cambridge, MA.
- Hogg, R. & Tanis, E. (1997) *Probability and statistical inference*. 5th edition. Prentice Hall, Upper Saddle River, New Jersey.
- Hållmats, J. (2002) *Demo for Decision Support in a Military Scenario*. Magisteruppsats från Uppsala Tekniska Högskola. UPTEC F 1401-5757.
- Ivansson, J. (2002) *Situation Assessment in a Stochastic Environment using Bayesian Networks*. Magisteruppsats från Linköpings Universitet. LiTH-ISY-EX-3267-2002.
- Jaynes, E. T. (1985) Bayesian Methods: General Background. In *Proceedings Volume, Maximum Entropy and Bayesian Methods in Applied Statistics*, 1-25.
- Jaynes, E. T. (2003) *Probability Theory: The Logic of Science*. Cambridge University Press.
- Jensen, F. V. (1996) *An introduction to Bayesian Networks*. UCL Press Ltd, Gunpowder Square, London.

- Jönsson, L., Neider, G., Schubert, J. & Svensson, P. (1998) *Informationsfusion i den taktiska underrättelseprocessen*. Försvarets forskningsanstalt.
- Lindberg, E. (2002) *Bayesiansk hypotesprövning för utvärdering av fiendens handlingsalternativ*. Magisteruppsats från Kungliga Tekniska Högskolan. TRITA-NA-E02070.
- Onisko, A. & Druzdzal, M. (2003) Effect of imprecision in probabilities on the quality of results in Bayesian networks: An empirical study. *Working Notes of the European Conference on Artificial Intelligence in Medicine (AIME-03) Workshop on Qualitative and Model-based Reasoning in Biomedicine*, 45-49.
- Raiffa, H. (1968) *Decision Analysis: Introductory Lectures on Choices under Uncertainty*. Addison-Wesley, Reading, MA.
- Runqvist, A. (2004) *Threat Evaluation. An Application for Air Surveillance Systems*. Magisteruppsats från Uppsala Universitet. UPTEC IT 04 003.
- Russell, S. & Norvig, P. (2003) *Artificial Intelligence: A Modern Approach*. 2nd edition. Prentice Hall, Upper Saddle River, New Jersey.
- Shafer, G. (1990). Perspectives on the theory and practice of belief functions. *International Journal of Approximate Reasoning*, 3, 1-40.
- Starr, C. & Shi, P. (2004) *An Introduction to Bayesian Belief Networks and their Applications to Land Operations*. Teknisk rapport från Land Operations Division Systems Sciences Laboratory. DSTO-TN-0534.
- Suzić, R. (2003a) Representation and Recognition of Uncertain Enemy Policies Using Statistical Models. *Proceedings of the NATO RTO Symposium on Military Data and Information Fusion*.
- Suzić, R. (2003b) Generic Representation of Military Organisation and Military Behaviour: UML and Bayesian Networks. *Proceedings of the NATO RTO Symposium on C3I and M&S Interoperability*.
- Svensson, P. & Schubert, J. (2003) Kaos eller överläge hänger på fusionen. *Framsyn*, 6, 50-52.
- Tversky, A. & Kahneman, D. (1974) Judgement under uncertainty: heuristics and biases. *Science*, 185, 1124-1131.
- Wallenius, K. (2004a) Support for Situation Awareness in Command and Control. *Proceedings of the Seventh International Conference on Information Fusion*, 2, 1117-1124.
- Wallenius, K. (2004b) *Generic Support for Decision-Making in Management and Command and Control*. Licentiatuppsats från Kungliga Tekniska Högskolan. TRITA-NA-0410.
- Wang, H., Rish, I. & Ma, S. (2002) Using Sensitivity Analysis for Selective Parameter Update in Bayesian Network Learning. *Proceedings of the 2002 AAAI Symposium on Information Refinement and Revision for Decision Making*.
- Warston, H. & Persson, H. (2004) Ground surveillance and fusion of ground target sensor data in a network based defense. *Proceedings of the Seventh International Conference on Information Fusion*, 1195-1201.
- Westberg, R. (2001) *Decision Support for Naval Command and Control Systems*. Magisteruppsats från Kungliga Tekniska Högskolan.