Intelligenta skydd mot intrång i skyddsobjekt
– metoder och tekniker

ERLAND JUNGERT, FREDRIK LANTZ

FOI är en huvudsakligen uppdragsfinansierad myndighet under Försvarsdepartementet. Kärnverksamheten är forskning, metod- och teknikutveckling till nytta för försvar och säkerhet. Organisationen har cirka 1350 anställda varav ungefär 950 är forskare. Detta gör organisationen till Sveriges största forskningsinstitut. FOI ger kunderna tillgång till ledande expertis inom ett stort antal tillämpningsområden såsom säkerhetspolitiska studier och analyser inom försvar och säkerhet, bedömning av olika typer av hot, system för ledning och hantering av kriser, skydd mot och hantering av farliga ämnen, IT-säkerhet och nya sensorers möjligheter.

FOI
Totalförsvarets forskningsinstitut
Ledningssystem
Box 1165
581 11 Linköping

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

www.foi.se

FOI-R--1993--SE
ISSN 1650-1942

Metodrapport
Maj 2006

Ledningssystem

Erland Jungert, Fredrik Lantz

Intelligenta skydd mot intrång i skyddsobjekt

-- metoder och tekniker

FOI-R--1993--SE
ISSN 1650-1942

Metodrapport
Maj 2006

Ledningssystem

Utgivare	Rapportnummer, ISRN	Klassificering
FOI - Totalförsvarets forskningsinstitut Ledningssystem Box 1165 581 11 Linköping	FOI-R--1993--SE	Metodrapport
	Forskningsområde 4. Ledning, informationsteknik och sensorer	
	Månad, år Maj 2006	**Projektnummer** E7572
	Delområde 49 Breda projekt inom ledning, informationsteknik och sensorer	
	Delområde 2	

Författare/redaktör	Projektledare
Erland Jungert Fredrik Lantz	Erland Jungert
	Godkänd av Johan Mårtensson
	Uppdragsgivare/kundbeteckning FMV
	Tekniskt och/eller vetenskapligt ansvarig Erland Jungert, Fredrik Lantz

Rapportens titel

Intelligenta skydd mot intrång i skyddsobjekt -- metoder och tekniker

Sammanfattning

Intrång i olika skyddsanläggningar har på senare tid blivit allt vanligare. Syftet med intrånget kan vara att stjäla stöldbegärliga tillgångar, genomföra sabotage eller genomföra terrorhandlingar, men även att frita interner från en anstalt. Oftast är dessa anläggningar försedda med larm av varierande slag, såsom videokameror, andra typer av sensorer och detektorer. När intrånget sker och larmet går är det vanligen för sent att vidta några mer kraftfulla åtgärder för att förhindra detsamma. Eftersom i många fall stora värden står på spel, och då också kostnaderna för att bevaka dessa anläggningar är mycket stora, behövs åtgärder för att omintetgöra eller minska konsekvenserna av intrången. Den lösning som föreslås i detta arbete består av ett datorsystem försett med multipla sensorer, olika dataanalysfunktioner och beslutsstödshjälpmedel. Ett sådant system skall göra det möjligt att preventivt följa skeenden utanför anläggningarna med syftet att avgöra om misstänkta och onormala aktiviteter utgör del i någon plan för ett intrångsförsök. Upptäckten av sådana aktiviteter bör göra det möjligt att vidta lämpliga åtgärder. Detta ökar möjligheterna att antingen förhindra eller att åtminstone minska konsekvenserna av ett intrång.

Nyckelord

Intelligenta intrångsskydd, säkerhetsövervakning, hotanalys, situationsanalys, hotupptäckt, databrytning, informationsfusion, beslutsstöd, data brytning.

Övriga bibliografiska uppgifter	Språk Svenska
ISSN 1650-1942	**Antal sidor:** 36 s.
Distribution enligt missiv	**Pris: Enligt prislista**

Issuing organization
FOI – Swedish Defence Research Agency
Command and Control Systems
P.O. Box 1165
SE-581 11 Linköping

Report number, ISRN
FOI-R--1993--SE

Report type
Methodology report

Programme Areas
4. C4ISTAR

Month year
May 2006

Project no.
E7572

Subcategories
49 Interdisciplinary Projects regarding C4ISTAR

Subcategories 2

Author/s (editor/s)
Erland Jungert
Fredrik Lantz

Project manager
Erland Jungert

Approved by
Johan Mårtensson

Sponsoring agency
Swedish Defence Material Administration

Scientifically and technically responsible
Erland Jungert, Fredrik Lantz

Report title (In translation)
Intelligent Physical Protection Systems – methods and techniques

Abstract

Intrusions into different types of physical establishments have become more and more common. The purpose of such intrusions is generally theft, terror attacks and other types of criminal activities. Generally, the establishments subject to such intrusions are equipped with alarms using video cameras, sensors and other types of detectors to determine these activities. However, when the alarm goes off it is often too late to carry out any powerful counter activity to stop the attempts. As in many cases, large values are at stake and as the costs for watching the establishments are high, other means to stop the intruders to diminish the consequences are needed. The solution to this problem is to design and develop a computer system equipped with multiple sensors, algorithms for sensor data analysis and a set of decision support tools. The purpose is to prevent intrusion by observing the activities that occur outside the establishments and to quickly and effectively determine whether they can be considered suspicious or abnormal. Through the detection of such activities it will become possible to prepare for an intrusion in advance either by preventing it or to diminish its consequences.

Keywords
Intelligent Physical Protection System, threat detection, alarm assessment, security surveillance, threat analysis, situation analysis, information fusion, data mining, decision support.

Further bibliographic information

Language Swedish

ISSN 1650-1942

Pages 36 p.

Price acc. to pricelist

Innehållsförteckning

1. Introduktion

Preventiva skydd av skyddsanläggningar mot antagonistiska hot har under senare år kommit att bli alltmer nödvändiga. Anledningen till detta är att många olika typer av skyddsobjekt blivit utsatta för olika hot från terrorister eller medlemmar ur kriminella gäng men även andra typer av aktiviteter förekommer som samhället måste skydda sig mot. Till de senare hör bl a skadegörelse från olika grupper i samhället och där motiven kan vara religiösa eller politiska även om skadegörelse från ungdoms- och kriminella gäng också förekommer. I dessa sammanhang måste samhället agera och skydda såväl sina skyddsanläggningar som sina medborgare. Innehållet i denna rapport riktar sig därför till myndigheter, kommuner, länsstyrelser och andra organisation med krav på sig att bidra till utvecklingen av ett bättre skydd av samhällets olika skyddsobjekt. Arbetet riktar sig också till industrier och företag med intressen i design och utveckling av system för tillämpningar där skydd av skyddsobjekt står i fokus.

I detta arbete, som har gjorts på uppdrag av Försvarets materielverk (FMV), redogörs för ett antal möjliga lösningsansatser på ovanstående problem med syftet att på ett intelligent sätt skydda olika skyddsanläggningar från intrång av obehöriga. Detta skydd skall verka preventivt och vara aktivt i den meningen att avsikten är att stoppa förövarna i ett mycket tidigt skede av intrångsförsöket innan materiella eller personella skador har inträffat. Av betydelse är också att skyddet skall vara robust mot yttre störningar och mer tillförlitligt med avseende på sin förmåga än vad enskilda operatörer är sett över tiden. Observationen bakom detta är att i de flesta fall kommer intrången ofta som en blixt från klar himmel och när detta sker är det som regel försent för de ansvariga att hinna agera på ett adekvat sätt. Resultatet av detta blir att händelsen övergår i ett polisärende som löses i efterhand, ofta med stora konsekvenser för sakägare, enskilda personer och där förövarna i bästa fall blir ställda till svars för sina handlingar.

Eftersom dagens system, som bygger på olika typer av traditionella larmanordningar, inte kan förhindra intrång måste nya ansatser utvecklas som kan utgöra grunden för vad som kan betecknas som mer *intelligenta* ansatser. Med intelligent menas i detta sammanhang delsystem som bygger på metoder med förmågan att på olika sätt dra slutsatser ur insamlade data. Dessa data är oftast tids- och rumsberoende och genererade från olika sensorer som kräver en omfattande dataanalys. Till detta kommer också att sensordata är förknippade med osäkerheter som också måste hanteras av systemet. De mest centrala problemen blir därför att identifiera beteenden hos personer och fordon som uppehåller sig i, eller passerar området kring en anläggning, och som kan ses som avvikande ur ett perspektiv där en aktivitet är avvikande om den syftar till en icke tillåten handling. Med icke tillåten handling avses här en handling som kan utgöra del av en plan som syftar till ett otillåtet intrång i den aktuella anläggningen. Mot denna bakgrund diskuteras i denna rapport förutsättningarna för design, utveckling och demonstration av intelligenta system med preventiv förmåga att skydda skyddssanläggningar mot otillåtna intrång. I detta sammanhang diskuteras också vilka hänsyn som måste tas till skyddet av enskilda medborgares integritet.

Ett annat starkt motiv för att studera metoder för intelligenta intrångsskydd är att kostnaderna för övervakning av skyddsanläggningar är höga och att kraven från statsmakterna på att förbättra skydden i många avseenden har kommit att öka. De ökade kraven på mer omfattande skydd av skyddsanläggningar hänger samman med att hoten mot samhället i stort har ökat bl a som en följd av det ökande antalet terroristangrepp liksom också de allt allvarligare aktiviteterna från olika kriminella organisationer såsom MC-gäng och andra liknande organisationer. Syftet med detta arbete är därför att bidra till förbättrade skydd av skyddsanläggningar vilka är utsatta för ökande hot och där samhället har ett ansvar i att skydda dessa anläggningar.

2. Problemdiskussion

Sensorer kan tillsammans med tekniska beslutsstödssystem användas för att förbättra förmågan att upptäcka och identifiera hot mot skyddsvärda anläggningar, s k *intelligenta intrångsskydd*. I det här aktuella fallet är avsikten att belysa problematiken kring utveckling av beslutstöd för detektion av avvikelser från det normala runt skyddsvärda anläggningar. Vi talar i dessa sammanhang om *intelligenta intrångsskydd*. Hur hot mot skyddsvärda anläggningar ser ut kan ofta inte exakt definieras på förhand; det är därför lämpligt att låta systemet varna då händelser som avviker från det normala detekteras. Användaren kan sedan utnyttja tillgängliga beslutsstödssystem för att söka rätt på detaljer kring händelsen för att därigenom avgöra om den är att betrakta som ett potentiellt hot. I dessa sammanhang spelar naturligtvis också användarens egna erfarenheter av hotbedömning in. Tekniska beslutsstödssystem används inom många problemområden t.ex. för att ur stora datavolymer enklare hitta relevant information. Ett annat viktigt skäl för att använda tekniska beslutsstöd är att dessa kan användas för att sammanställa data från skilda datakällor i syfte att bilda underlag för bättre genomlysning av den aktuella hotbilden.

Systemets förmåga att avgöra arten av de registrerade onormala händelser som kan tänkas förekomma beror bl a på de sensorer som valts för uppgiften. Valet av sensorer styrs av flera externa faktorer såsom områdets storlek, klimatförhållanden och hotens art, men också av anläggningarnas skyddsbehov. Sensorerna kan vara avbildande eller registrera signaler, såsom ljud, från fordon, människor eller andra typer av objekt. Till detta kommer också att registrerade sensordata är behäftade med osäkerheter av olika slag. Intelligent intrångsskydd kräver användning av sensorer av varierande art för att uppnå den avsedda förmågan vid t.ex. varierande ljus- och väderförhållanden. Att från de olika sensorernas enskilda bild av läget korrekt sammanställa en sensorgemensam - och för uppgiften adekvat - bild är en central del av problemet i den uppgift som beskrivs här.

I många fall behöver inte avvikelser från det normala bero på omedelbara hot, utan kan bero t.ex. på att personer uppehåller sig inom området för att rekognoscera i avsikt att planera framtida brott. Man kan förvänta sig att personer som rekognoscerar troligen uppför sig annorlunda än de människor som normalt passerar eller uppehåller sig i området. Systemet skall således kunna upptäcka en person eller ett fordon som uppför sig avvikande, varefter sensorinformation med deras rörelser och beteenden skickas vidare till en operatör. Operatören kan sedan avgöra om det föreligger skäl att larma myndigheter med befogenhet att hantera situationen eller om beredskapen enbart skall höjas. Huvudsyftet bör därför vara att utveckla ett system för att ge operatörerna en tidig och tillförlitlig varning för potentiella intrång i en skyddsanläggning. I anslutning till en sådan uppgift kommer ett antal problem att uppstå av vilka kan nämnas identifiering av aktiviteter som kan utgöra hot mot skyddsanläggningar. Sådana aktiviteter kan utgöras av planläggnings-verksamhet som senare kan leda till intrång.

I dessa sammanhang behöver uppträdandet hos fordon och/eller människor studeras i syfte att kunna avgöra vad som är att betrakta som normalt respektive onormalt beteende hos dessa objekt. För att avgöra detta krävs att man har metoder för att avgöra vad som är normalt beteende, för att med ledning av denna information avgöra vad som är onormalt beteende hos en aktör. Problem som uppstår i dessa sammanhang berör:

- Hantering av stora datamängder från sensorer, där data på olika sätt kommer att behöva insamlas, analyseras och lagras.
- Stöd för automatisk informationshantering:
    - att hitta mönster i stora informationsmängder med hjälp av databrytning,
    - sammanvägning av data från många källor (datafusion),
    - hantering av osäker information.
- Utveckling av olika former av beslutsstödshjälpmedel, t. ex. för :
    - uppbyggnad och underhåll av lägesbeskrivningar för ökad situationsförståelse,

  - frågespråk för specifik informationsinsamling och användardialog,
  - stöd för situations- och hotanalys.
- Val av lämpliga sensorer.
- Utveckling av relevant systemarkitektur.

Exemplen på olika typer av skyddsvärda anläggningar som kan och bör skyddas med intelligenta intrångsskydd är stort och sådana anläggningar återfinns överallt i samhället se vidare avsnitt 4. I militära sammanhang kommer man att kunna utnyttja tekniken även vid internationella operationer.

Objekt, vid sidan av personer och fordon som kan vara av intresse av att kunna observera kan t ex vara:

- kameror och kikare,
- telekomutrustning,
- vapen och verktyg,
- störutrustning.

För att bestämma vad som är onormalt är avgörande för vilken information som skall samlas in. Detta är avhängigt vilka tekniska begränsningar som förekommer men också beroende av vad som med hänsyn till integritetsproblematiken tillåts att samlas in. Man kan oberoende av detta ändå formulera ett antal frågor vars svar kan ligga till grund för bedömning av om något beteende kan anses vara onormalt med hänsyn tagen till existerande information om vad som är normalt. Bland dessa frågor kan nämnas:

- Är tidpunkten för observationen rimlig?
- Är fordonet stulet?
- Har någon lins registrerats (till kamera eller kikare)?

Uppgiften är således att utifrån det ovannämnda ta fram metoder och tekniker med vars hjälp det blir möjligt att utveckla system som för skilda applikationer kan avgöra om vissa händelser kan utgöra initialskedena till olika hot som kan vara under planering och som kan förmodas bli satta i verket. Systemet måste därför, om inte helt förhindra, så i varje fall kunna mildra konsekvenserna av de förväntade händelserna. Andra skäl till varför intrångsskydd behövs är att i de fall då förövarna lyckas i sitt uppsåt bör systemet kunna mildra konsekvenserna av det genomförda intrånget. Detta kan ha till följd att de normalt stora kostnaderna som bli följden av ett intrång till del kan begränsas.

2.1 Beteendebestämning

Metoder för bestämning av normalt/onormalt beteende kan huvudsakligen vara av flera olika typer. Genom att flera metoder kan utnyttjas blir det möjligt att fusionera resultatet av dessa, d v s väga samman, resultatet för att erhålla en säkrare bedömning av beteendet hos ett fordon eller en person. Det blir då också möjligt att härigenom avgöra vad som kan betecknas som onormalt utifrån vad som kan betecknas som normalt. Metoder som kan komma till användning kan väsentligen hänföras till två huvudområden:

- Inlärningsmetoder
  - neuronnät,
  - klustringsmetoder.
- Kunskapsrelaterade metoder
  - Regelbaserade metoder,
  - Statistiska- sannolikhetsmetoder.

Till dessa huvudområden, som devis är överlappande, kan ytterligare ett antal metoder hänföras. Bland de exempel som nämns ovan kan nämnas att inom gruppen klustringsmetoderna återfinns metoder för databrytning som diskuteras vidare i avsnitt 3 liksom också regelbaserade metoder som kan hänföras till de kunskapsbaserade metoderna.

3. Teknikstöd

Det som här kallas teknikstöd för intelligenta intrångsskydd kommer att behöva vara av varierande slag. Främst inriktar sig dessa mot olika typer av beslutstöd, olika metoder för automatisk informationshantering samt mot olika typer av sensordatabehandling. Till detta kan även räknas andra typer stöd men dessa tre grupper får anses vara de mest fundamentala medan övriga är, om inte av mindre betydelse för problemet, så de ändå inte förknippade med några forskningsnära problem och kan därför förbigås i denna förstudie. Till den senare gruppen hör bl a olika databaslösningar.

3.1 Beslutsstöd

Beslutsstöd kan vara av många olika slag och det är inte möjligt att ge en komplett bild av alla tänkbara alternativ eftersom dessa till viss del kommer att vara tillämpningsberoende. Två grupper av central betydelse kan dock identifieras. Till dessa två huvudgrupper kan räknas de som på något sätt direkt leder till en ökad situationsförståelse och de som gör det möjligt för operatören att föra en dialog med systemet i avsikt att ta fram mer information om det aktuella läget. Den senare metoden kan betecknas som en indirekt metod för att förbättra situationsförståelsen. Man kan därför tala om direkta och indirekta metoder för beslutsstöd för att uppnå ökad situations- eller lägesförståelse. Med detta menas en förståelse av den situation eller det läge som råder och utifrån vilken användaren fattar beslut om vilka insatser som behöver genomföras för att lösa det aktuella problemet.

Lägesbild för situationsförståelse

Direkta metoder är att betrakta som helt automatiska och bidrar till att skapa, och i förlängningen underhålla, en lägesbild som över tiden och i rummet beskriver det aktuella läget. Ett system för stöd till lägesbildsgenerering kan bestå av olika bilder som beskriver situationen ur ett geografiskt perspektiv men kan också innefatta tabeller och listor med andra typer av information. Exempel på en geografiskt orienterad lägesbild framgår av figur 1. Ur denna lägesbild kan man bl a utläsa positionen för olika sensorer och observationsposter som finns återgivna i symbolisk form. En lägesbild av denna typ är, som synes, oftast knuten till någon form av karta som kan vara mer eller mindre högupplösande och som alternativt kan vara återgiven i två eller tre dimensioner. I andra sammanhang kan lägesbilden vara mer informerande och ange information av typ:

Fordon X har passerat punkt P flera gånger under olika nätter

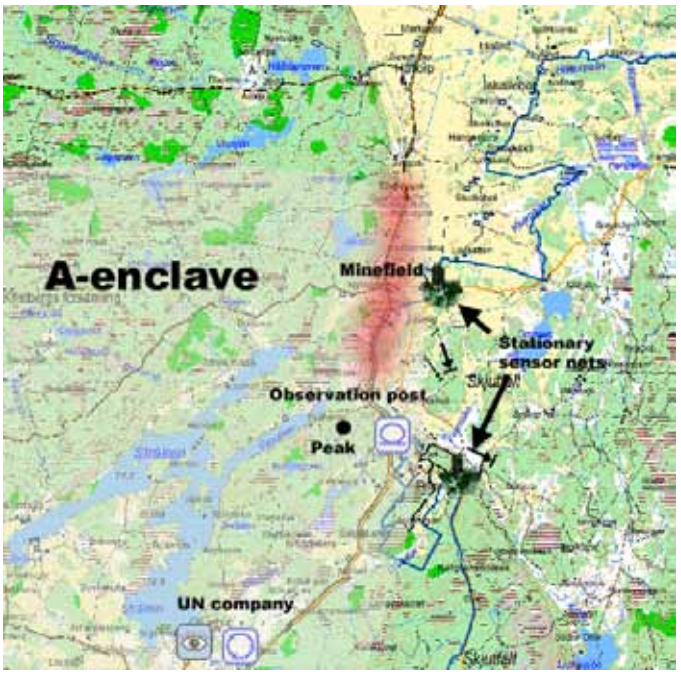
eller

Fordon Y är stulet

Självklart kan och bör denna information kombineras med en geografiskt orienterad lägesbild som kan peka ut fordonets senast observerade läge men också kan ange den färdväg som fordonet har använt. Användaren skall också kunna se fordonets eventuellt tidigare använda färdvägar. Slutsatsen av detta är att lägesbilden över tiden förser användaren med den information som behövs för att denne skall kunna fatta rimliga beslut om åtgärder som skall vidtas när så krävs. Grunderna för framtagning av denna information diskuteras vidare i avsnitt 3.2 om tekniker för automatisk informationshantering.

En geografisk lägesbild kan vara mer eller mindre högupplösande beroende på det rådande läget. Om läget är normalt kan man anta att man inte behöver uppmärksamma användaren på innehållet i bilden på samma sätt som när en särskild händelse inträffat. Inte heller behöver i sådana sammanhang användaren vara speciellt uppmärksam på lägesbilden; det räcker säkerligen med att denne kastar en blick på densamma lite då och då för att avgöra om allt går sin gilla gång. Så snart något inträffar bör användaren emellertid aktiveras och uppmärksammas på detta. Detta kan ske på flera sätt; t ex genom olika ljud men också genom att lägesbilden förändras och presenteras i en

högre upplösning. På detta sätt tydliggörs att operatören måste vidta någon eller några åtgärder med syfte att lösa eventuella problem för att sedan återgå till de normala arbetsrutinerna. Givetvis kan detta innefatta mer eller mindre omfattande åtgärder och ta mer eller mindre lång tid.



Figur 1. Exempel på geografiskt orienterad lägesbild omfattande förklaringar till förekommande symboler.

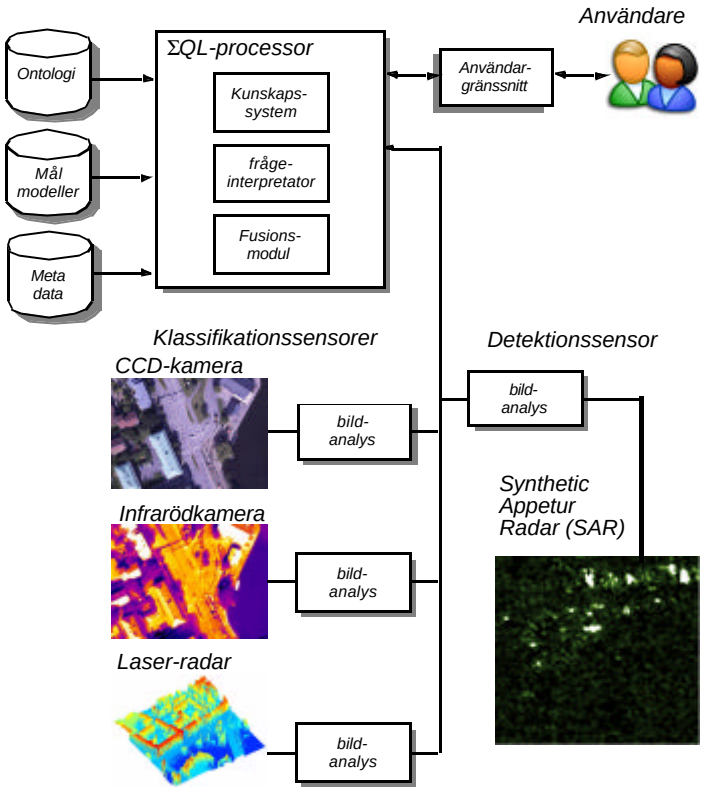
Frågesystem

Gruppen frågesystem kan räknas till indirekta beslutsstöd och med denna typ menas beslutsstöd där användaren kan föra en dialog med systemet i avsikt att ta fram ytterligare information av betydelse för hur den uppkomna situationen skall hanteras. Här finns många olika alternativ, av vilka några kan anses vara tillämpningsberoende. För att uppnå en hög grad av generalitet i vad avser metodiken för informationsinhämtning bör ett väl anpassat frågespråk vara det lämpligaste valet. Orsaken till detta är i första hand att frågor i ett frågespråk kan varieras på ett nästan obegränsat sätt utan att man behöver förändra programvaran. Ett annat skäl för att utnyttja ett sådant frågespråk hänger samman med att det är angeläget att kunna använda ett sådant i samband med metoder för databrytning (se avsnitt 3.2). Eftersom ett frågespråk är avsett för att inhämta data från multipla datakällor, ofta med heterogena datatyper, föreligger behov av att i vissa fall kunna fusionera olika delresultat. Vidare behövs stöd för att automatiskt låta systemet välja relevanta datakällor och fusionera framtagna delresultat. Av denna anledning talar vi inte här om något traditionellt frågespråk utan mera om ett mer omfattande system med olika inbyggda faciliteter. Hur ett sådant frågesystem skall vara designat för att kunna utnyttjas i detta sammanhang är därför inte helt klart och vidare studier av detta problem behöver göras även mot bakgrund av att man kan behöva tillgång till system på olika ambitionsnivå.

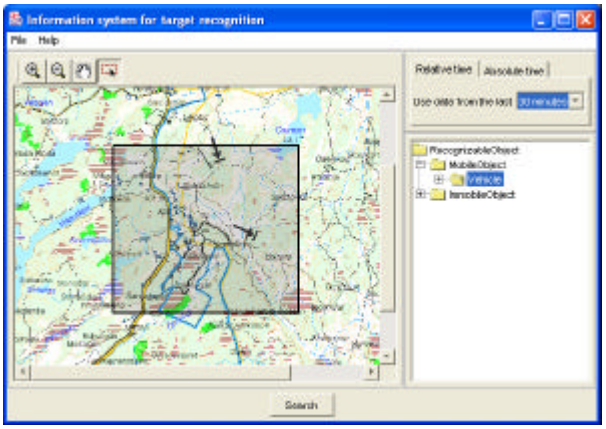
Vid FOI har utvecklats ett frågesystem, se t ex [Jungert05] eller [Chang04a], för att kunna ställa frågor mot multipla sensorer med heterogena data, se figur 2. Detta system skulle kunna användas för att föra en dialog mellan användare och system i avsikt att ge användaren en bättre kunskap om det aktuella läget vid en skyddsanläggning. Systemet besitter ett antal egenskaper som vanligtvis saknas i traditionella frågespråk. Dessutom kan frågor av mycket varierande slag ställas till frågesystemet [Chang04b]. Till de egenskaper som vanligen inte kan hänföras till frågespråk hör sensordataoberoende, d v s användaren kan ställa frågor utan att känna till vilka sensorer som kommer till användning genom att systemet självt väljer ut vilka sensor som är bäst lämpade för att besvara en fråga. Systemet kan också dels detektera olika mål och dels användas för igenkänning av dessa mål; vidare har systemet förmåga att automatiskt fusionera data från

multipla sensorer. De sensorer som för närvarande kan användas av ΣQL framgår av figur 2 men omfattar vid sidan av de i figuren angivna sensorerna också marksensorer, vilka kan användas för såväl detektering som igenkänning av mål.

Frågor i ΣQL kan vara både enkla och sammansatta. Enkla frågor kan specificeras av användare utan speciell datorerfarenhet. Sammansatta frågor kräver större kunskaper eftersom de också omfattar specificering av villkor där komplexa objektsamband också ingår. De enkla frågorna kräver endast att användaren genom det visuella användargränssnittet anger det aktuella geografiska område där man vill söka efter aktuellt objekt. Till detta kommer att användaren förutom aktuellt objekt också måste ange vilken tidpunkt som frågan avser. Slutligen måste användaren i en enkel fråga också ange vilka objekt som eftersöks; dessa kan t ex vara fordon eller människor. Det grafiska användargränssnittet för att ställa frågor av denna typ framgår av figur 3.



Figur 2. Systemöversikt över frågespråket ΣQL med vars hjälp man skulle kunna interagera med det intelligenta intrångsskyddssystemet.



Figur 3. ΣQLs användargränssnitt för enkla frågor.

Larmfunktioner

Larmfunktioner kan, åtminstone ytligt sett, betraktas som triviala exempel på beslutsstöd men i ett djupare sammanhang är dessa mer komplexa givet existerande sensorsystem, sensordataanalys-metoder och övriga analysmetoder. Två huvudtyper kan emellertid urskiljas, nämligen vad som här kallas realtidslarm och dialoglarm. Som framgår nedan har dessa två typer vissa delar gemensamma. Den stora skillnaden mellan dem består i att man i ett dialoglarm kan ställa frågor till systemet i avsikt att få tillgång till mer kvalificerad information medan informationen i ett realtidslarm är som den är. De två metoderna kan beskrivas enligt följande:

Realtidslarm

1. Systemet registrerar autonomt en eller flera onormala händelser i övervakningsområdet.
2. Händelserna rapporteras till operatören.
3. Operatören tar beslut om eventuella åtgärder.

Dialoglarm

1. Systemet registrerar autonomt en eller flera onormala händelser i övervakningsområdet.
2. Händelserna rapporteras till operatören.
3. Operatören ställer frågor för ökad förståelse.
4. Operatören tar beslut om eventuella åtgärder.

Självklart är det också så att en användare inte behöver invänta ett larm för att starta en dialog med systemet. Detta kan ske när som helst och under vilka omständigheter som helst, t ex om användaren i något skede upptäcker något avvikande i lägesbilden.

3.2 Tekniker för automatisk informationshantering

I detta avsnitt kommer metoder centrala för bestämning av ett objekts klasstillhörighet med avseende på normalt respektive onormalt beteende att diskuteras. De metoder som kan komma till användning för att lösa detta problem kan i huvudsak vara av två typer, eller i vissa fall en blandning av dessa, nämligen metoder som grundar sig på någon form av *inlärningsteknik* respektive metoder som är av mer *kunskapsorienterad* inriktning. Till detta kommer att i de sammanhang där flera olika metoder används blir det möjligt att väga samman resultatet av dessa. I dessa sammanhang talar vi om metoder för informationsfusion [Hall01], vilket också kommer att diskuteras vidare nedan.

Databrytning

Databrytning (eng. data mining) är ett omfattande teknikområde till vilket ett stort antal olika metoder brukar hänföras [Menas03], [Chen01]. Gemensamt för de flesta av dessa metoder gäller att de har sin grund i behovet att hitta mönster bland data i stora databaser. Ursprungligen ingick dessa databaser i vad som brukar kallas ’data warehousing’ där data kommer från, i första hand, dagligvaruhandeln och ofta omfattar information om kundernas köpvanor över kortare eller längre perioder i tiden. Syftet är att identifiera kundernas inköpsmönster i avsikt att öka den direkta marknadsföringen och försäljningen av vissa varor till olika kundkategorier. Oftast kräver detta genomsökning av mycket stora datamängder. Under senare tid har dessa metoder visat sig vara användbara även i andra sammanhang där mönster i data, som inte enkelt kan upptäckas på grund av de omfattande datamängderna, behöver synliggöras. Intelligenta intrångsskydd är ett problemområde där okända mönster i informationen behöver synliggöras, d v s då man behöver bestämma vad som är onormalt beteende utanför en skyddsanläggning. Som redan nämnts finns ett stort antal metoder att tillgå, se t ex också [Demsar06] som diskuterar mer konventionella metoder tillsammans med visuella, vilka skulle kunna vara användbara för identifiering av misstänkta objekt. Bland de metoder som troligen lämpar sig bäst för de problem som diskuteras här kan nämnas olika multivariata ansatser. Skälet till att dessa metoder kan anses mest tillämpliga är att vi söker bland objekt som innefattar ett relativt stort antal attribut och statusvärden. Med attribut menas här egenskaper som till exempel färg (på fordonet) längden hos en person etc. Statusvärden syftar på objektens beteende t ex hastighet, färdriktning etc. Genom att tillgängliggöra all denna

information blir det möjligt att beskriva objektet och dess uppträdande i relativt enkla termer och härigenom skapa olika kluster som bl annat kan svara mot normalt respektive onormalt beteende. Problemet här blir därför att bestämma till vilket kluster ett registrerat objekt hör. Detta är ett inte helt trivialt problem, eftersom man ofta stöter på gränsfall med oklar tillhörighet. Denna teknik tillhör gruppen inlärningsmetoder.

Kunskapsbaserade metoder

Kunskapsbaserade metoder grundar sig oftast på någon typ av teknik för slutsatsdragning. Oftast utnyttjar man i dessa sammanhang vad som kallas inferensregler med ett villkorsuttryck och en utförande del. Den senare utförs då villkoret är sant. Exempel på regler av detta slag är:

(fordon(a) har observerats i område(b) mer än 1 gång) => (markera fordon(a) som misstänkt)

*(*fordon(a) kör med en hastighet mindre 5 km/timmen *och* tiden är (02.00, 04.00)) => (markera fordon(a) som misstänkt)

*(*person(c) betraktar området(b) med kikare eller kamera)=> (larma operatör)

Dessa regler kan givetvis vara mer eller mindre formaliserade men ofta försöker man göra dem relativt läsbara för att göra hanteringen av reglerna enklare.

Datafusion

En teknik som är nödvändig för att samutnyttja olika typer av sensorer är *datafusion*. Datafusion är en process för att sammanställa data från olika källor eller tidpunkter i syfte att skatta eller förutsäga tillståndet hos något bestämt objekt. Ett objekts tillstånd kan beskriva både dess permanenta egenskaper och dess mer tillfälliga status, t.ex. typ och position hos ett fordon. Syftet med datafusion kan vara att få en kompletterande bild av objektet gentemot vad som kan fås med enbart en källa/sensor, att verifiera resultatet av en sensor med den andra, att få en mer säker skattning av det man redan har viss kunskap om, etc.

För att beskriva datafusion på ett överskådligt sätt brukar man dela upp datafusion i olika nivåer, med något olika uppgift och karaktär [Hall01]. I de fall de intressanta objekten är av förhållandevis enkel (icke-sammansatt) art, d v s ett fordon, en byggnad, etc., brukar man tala om datafusion på nivå 1. Ibland brukar man även kalla denna nivå för multisensor fusion då den huvudsakligen behandlar data från olika sensorer. Högre nivåers datafusion, nivå 2 och nivå 3, brukar benämnas som *situationsanalys* och *hotanalys* i militära sammanhang. Situationsanalysen brukar då sägas handla om att skatta och förutsäga objektens relationer och beteenden (en ”situation”), medan hotanalysen handlar om att försöka förutsäga vilka konsekvenser olika handlingar som kan utföras i situationen kan ha. Man brukar även inkludera en nivå 4, som behandlar anpassning av databehandling och datainsamling till det aktuella hotet. Ibland innehåller beskrivningen även en nivå 0, som då behandlar fusion på en mer signalnära nivå än vad nivå 1 representerar. I ett fall med bildgenererande sensorer kan fusion på nivå 0 t.ex. utgöras av sammanvägning av resultat i enskilda pixlar.

I ett intelligent intrångsskydd kan man betrakta det som fusion på nivå 1 att sammanställa en sensorgemensam bild av vilka personer och fordon som rör sig i det område man är intresserad av att bevaka. Däri ingår att bestämma den utrustning som fordonen eller människorna har, vilken typ av fordon det är och eventuell identifiering av bilnummer. Dessutom kan man, genom mer avancerad signalbehandling [Sidenbladh04], på denna nivå också identifiera vissa former av rörelser hos människor, t.ex. om de springer eller går. På nivå 2 följer en bestämning av deras beteende såsom normalt eller onormalt och värt vidare intresse. På nivå 3 utvärderas konsekvenserna av olika antagonistiska aktioner och egna handlingsplaner. I de flesta fall måste

fusion på nivå 2 och 3 ske i samverkan mellan det tekniska systemet och en operatör, då tolkning av situationen på denna nivå är alltför svår och viktig för att helt skötas av en automatisk funktion.

Datafusion och osäkerhetshantering

Datafusionsmetodik handlar i de flesta fall om att på ett korrekt sätt hantera de osäkerheter som är förknippade med aktuella data. Då man använder sensorer för att skatta något objekts tillstånd finns det alltid osäkerheter förknippade med resultatet, även om dessa i vissa fall är så små att de kan ignoreras eller på något annat sätt enkelt hanteras av en människa. Då hanteringen av osäkerheten i data ska ske automatiskt i en datafusionsprocess finns en mängd kända metoder för att göra detta på bästa sätt, även om metoder för de högre nivåernas datafusion, d.v.s. situationsanalys och hotanalys, inte är fullt så etablerade. Mycket ofta baserar sig datafusionsmetoder på *sannolikhetsteori,* där det s.k. *Kalman Filtret* [Anderson79], som baserar sig på antagandet att osäkerheterna är normalfördelade, är välkänt. Andra metoder baserar sig på *evidensteori* [Guan91] eller *oskarp logik* [Zimmerman91]. Även om olika metoder baserar sig på sannolikhetsteori från grunden kan sättet att beräkna, approximera och representera deras osäkerheter skilja sig åt. Därmed kan även beskrivningen av metoderna, samt deras egenskaper, styrkor och svagheter skilja sig åt.

Det är också vanligt att hantera osäkerhet om tillståndet hos ett objekt genom att tillfälligtvis behålla flera, sinsemellan uteslutande, hypoteser om vad tillståndet är. Senare inkommen information kan sedan användas för att avgöra vilken av hypoteserna som var den korrekta. Ett enkelt exempel kan vara att systemet tillfälligtvis, t.ex. beroende på ofullständig sensortäckning, kan ha svårt att avgöra vilken av två möjliga vägar en person valt att gå. Om båda möjligheterna/hypoteserna behålls tills vidare kan senare observationer användas för att avgöra vilken som var den korrekta.

Datafusionsarkitekturer

Ett av de val som måste göras när man hanterar sensorer i ett nätverk och fusionerar data från dessa rör den s.k. arkitektur som används för fusionen. Arkitekturen är ett sammanfattande namn på beskrivningen om vilken information som ska sändas i nätet och vilken bearbetning som ska ske i vilken nod i nätet. Den enklaste distinktion som i allmänhet görs behandlar existensen av en central nod där all fusion sker, eller om fusionsförmågan ska distribueras till alla sensorer/noder i nätet. I det senare fallet sammanställs delresultat, utgående från delar av den totala informationen, i sensorerna. Valet av arkitektur styrs i hög grad av den bandbredd som är tillgänglig för att överföra information mellan systemets noder. Fördelarna med att sköta fusionen i en central nod är att en sådan har bäst möjlighet att göra skattningar av omvärldstillståndet då den har tillgång till all information. Nackdelen är bl.a. att systemet blir känsligt för felfunktion i denna nod och att det kan krävas mycket stor beräkningskraft i den.

För intelligenta intrångsskydd gäller att om de kommunikationslänkar som finns mellan anläggningens sensorer, samt mellan sensorer och operatörsplats, är fasta länkar med hög bandbredd, så är förmodligen en central nod att föredra. Frågan om datafusionsarkitektur anknyter till frågan om vilken information som ska behandlas automatiskt av systemet och vilken information som kräver mänsklig interaktion. Samtidigt som användaren kan vilja ha en detaljerad bild av sensorernas resultat, kan det ibland vara fördelaktigt att låta fusion ske i sensornoder för att de ska kunna visa in varandra utan användarens medverkan.

Association

I alla de fall där man använder sensorer för att, under ett visst tidsintervall, följa mer än ett objekt uppträder problem med association mellan observationer av objekt från de olika mättillfällena, se figur 4. Med detta avses att positionering av flera objekt nära varandra tillsammans med sensorernas osäkerhet gör att det kan vara svårt att avgöra vilken observation vid ett aktuellt tillfälle som svarar mot en annan observation vid ett annat tillfälle. När man använder flera

sensorer för att skatta tillståndet hos ett objekt blir detta problem än mer komplicerat. Om mycket enkla sensorer används, som t.ex. enbart mäter positionen hos ett objekt, och dessutom alltför få sensorer används, kan problemet t.o.m. vara olösbart. Inom datafusionsområdet finns dock ett flertal kända tekniker för att hitta de bästa möjliga lösningarna med beaktande av osäkerheten. Lösningen underlättas av uppsättning av sensorerna så att deras synfält överlappar varandra, alternativt användningen av sensorer som kan mäta in distinkta karaktäristika hos objekten som kan användas för att känna igen objekten vid andra mättillfällen. Vid design av ett system för intelligent intrångsskydd är lösningen av associationsproblemet en förutsättning för systemets förmåga att detektera beteenden som är utsträckta i tiden eller som kräver information från mer än en sensor.

Figur 4. (a) En laserbild av en parkeringsplats. En viss bil är inringad. (b) Två visuella bilder av samma parkeringsplats och samma bil inringad. Metoder för association måste användas för att koppla samman bilen från de olika mättillfällena och från de olika sensorerna.

Fusion med kontextinformation

Även om datafusionssystem ofta hanterar olika former av sensordata, så är inte fusionen begränsad till att datakällorna är sensorer. Olika former av kontextinformation kan användas för att tolka den information som datafusionen genererar, men kan även användas för att förbättra skattningen eller för att anpassa databearbetningen till de aktuella förutsättningarna. Med kontextinformation avses här information om den miljö som sensorerna arbetar i, t.ex. väder eller geografi, information om vilka aktiviteter som pågår vid anläggningen, expertkunskap angående de hot som finns mot anläggningen och mycket mer. Hantering av kontextinformationen karaktäriseras framför allt av att det rör sig om information av starkt heterogen art och att säkerheten i informationen ofta delvis är oklar. Vid hantering av sensordata finns möjligheter att experimentellt fastställa osäkerheten hos sensorerna. Då informationen finns lagrad i olika databaser, som kanske är tillverkade för andra ändamål, eller i experters och användares huvuden kan inte systemet tillgodogöra sig informationen lika enkelt. De metoder som kan användas för fusion av olika former av kontextinformation av delvis oklar säkerhet är ofta annorlunda än de för fusion av sensorinformation och bygger på logiska regler snarare än sannolikhetsteori.

Enbart sensorinformation räcker inte till för att avgöra om systemet ska larma eller inte i de fall man vill använda systemet utanför ett skalskydd dit allmänheten har tillträde. System som är uppbyggda med avsikten att alltid larma då någon befinner sig på en viss plats eller då en sensorbarriär forceras, kräver inte något flexibelt utnyttjande av kontextinformation. Sådana enkla principer används ofta innanför ett skalskydd. Den begränsade ”intelligens” som ett sådant system kan uppvisa leder bl a till att användare måste delta i tolkningen av informationen i ett tidigt skede. Dessutom blir systemet okänsligt för förändrade omständigheter och därmed mycket svårt att

använda utanför det fysiska skalskyddet, där händelser inte går att kontrollera på samma sätt som innanför. Speciellt är kontextinformation nödvändig för att anpassa systemet till de hot som är aktuella mot de beteenden som är intressanta att detektera. Omständigheterna kan förändras i omgivningen till skyddsanläggningar på många sätt, både temporärt och permanent. Årstidsväxlingar påverkar sensorernas möjligheter, möjligheterna att ta sig fram i omgivningen kring anläggningen och - mycket allmänt - vad som är ett rimligt beteende. Tillfälliga förändringar i trafikrytmen eller vägarbeten påverkar i vilken hastighet det är rimligt att köra. Förändringar av arbetssätt eller ombyggnader av den egna anläggningen påverkar flödet av rörelser. Olika anläggningar har olika storlek på det område som måste övervakas.

Det är naturligtvis så att även olika former av det som här benämns som kontextinformation kan vara genererad av sensorer, i realtid eller i ett tidigare skede. T.ex. väder eller höjdinformation kommer i allmänhet från sensorer. Det är dock inte givet att denna information är tillgänglig för de sensorer som ingår i intrångsskyddet, om den är tillgänglig i en takt eller format som är användbar eller om systemet ö h t. kan ta hänsyn till informationen i den form som den finns tillgänglig. Därför kan många gånger användning av enklare former av informationen, t.ex. i form av användares översiktliga omdömen, vara en bättre möjlighet.

Förbättring av de skattningar som sensorerna ger kan i vissa fall fås genom att ta hänsyn till geografiska begränsningar hos objektens positioner eller rörelser. Anpassning av sensorerna för att uppnå bättre prestanda kan ske om man känner till t.ex. väder och ljusförhållanden, men anpassning kan även ske till specifika rörelser eller detaljer hos det man letar efter.

Användarbaserad fusion

I de fall en mänsklig operatör utför tolkningen av sensordata mer eller mindre direkt, t.ex. i form av ett bildflöde från en TV-kamera, sker mycket av datafusionen i operatörens huvud. En människa är många gånger mycket skicklig på att utföra datafusion, särskilt om datakällorna liknar de data vi normalt bearbetar via våra sinnen, t.ex. när data är ifrån enskilda, bildgenererande sensorer. Att sammanställa flera bilder från olika perspektiv, på andra våglängder än visuella eller då dataflödet är långt utsträckt i tiden, till en bild kan dock vara alltför krävande för en operatör. Om inte processen är fullt automatisk, krävs i dessa fall datorbaserat stöd för operatörens fusionsprocess. En av många viktiga frågor i detta sammanhang rör då presentationen av informationen och dess kvalitet/osäkerhet.

Datafusion och telekrig

I de fall en anläggning, t.ex. en flygplats, skall skyddas och sensorer används för att lösa den primära uppgiften finns det skäl att, förutom att skydda anläggningen i sig, också skydda dess sensorer från antagonistiska attacker (telekrigattacker). På en flygplats finns en stor mängd sensorsystem som används för att leda flygtrafiken. Dessa system kan bli utsatta för störning eller, om man har att göra med antagonister med tillgång till avancerad teknik, för vilseledning. Speciellt i kombination med intrång och fysiska attacker kan konsekvenserna av telekrigattacker bli allvarliga.

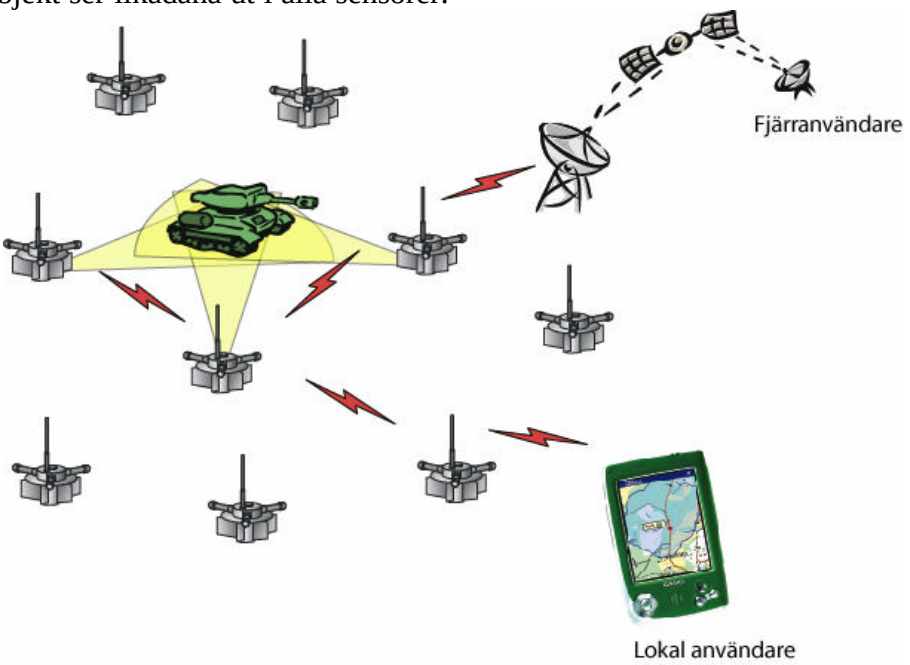
För att detektera att man är utsatt för vilseledning är det fördelaktigt att ha flera, redundanta sensorsystem som övervakar samma område. Då bilden hos dessa system avviker från varandra är det ett tecken på att ett av systemen kan vara under attack. Det är nämligen, som nämnts ovan, svårt att vilseleda alla sensorer samtidigt, och som en konsekvens ser därför enbart riktiga objekt likadana ut i alla sensorer. Om man har en normalbild över flygtrafikens beteende tillgänglig (som flygtrafikledarna har) kan också denna användas för detektion av onormalt beteende hos flygtrafiken. Principerna för att detektera onormalt beteende i flygtrafiken eller hos en sensor kan vara liknande som de som används för att hitta onormalt beteende i anläggningens omgivning. Därför är det naturligt att analysera båda dessa typer av hot mot verksamheten samtidigt. Förutom

fördelen vid detektion av attacken bidrar redundanta sensorsystem naturligtvis till förmågan att leda flygtrafiken vid sådana attacker.

Sensorer i nätverk

Genom att koppla sensorer samman i nät, se figur 5, genom kommunikationslänkar kan förmågan hos ett sensorbaserat övervakningssystem som helhet avsevärt förbättras i många olika avseenden. Den mest uppenbara förbättringen uppträder genom att informationen hos alla sensorer vägs samman till en sensorgemensam bild som är mer fullständig och säker än vad varje enskild sensor medger. En annan förbättring uppstår genom att man aktivt låter resultatet hos en sensor påverka beteendet hos en annan sensor, t.ex. genom att visa in den andra sensorns synfält eller anpassa den signalbehandling som sker till den första sensorns resultat. På detta sätt kan man t.ex. ägna mer datorkraft åt att förfina sin kännedom om egenskaper hos detekterade objekt istället för att börja om på nytt med varje enskild sensor. För intelligent intrångsskydd är tydliga exempel på en sådan påverkan att låta IR-barriärer eller tryckkänsliga marksensorer rikta in en kamera. Ett mer sofistikerat exempel vore att använda detektioner från en IR-kamera till att rikta in en lågljussensor (bildförstärkare). Man kan också minska risken för falska detektioner och/eller öka detektionssannolikheten genom att låta flera sensorer, kanske av olika typ, studera samma område. Detta beror på att ett intressant objekt ofta är synligt i mer än en sensor, medan olika former av brus eller bakgrundsfenomen många gånger är individuella för enskilda sensorer.

Med samma resonemang kan man motivera användning av flera, samtidiga sensorer i samma område för att motverka störning eller vilseledning mot de sensorsystem man använder. Det är nämligen svårt att störa eller vilseleda alla sensorer samtidigt, och dessutom på samma sätt, varför enbart riktiga objekt ser likadana ut i alla sensorer.



Figur 5: Idéskiss på ett sensornät bestående av akustiska och seismiska sensorer. Se [Holmberg04] för en utförlig beskrivning av ett sådant nät.

Databaser och sökmetoder

Stora data mängder kommer att behöva lagras i flera olika databaser, vilket beror på att data över långa perioder måste registreras och hanteras. Troligen kan dock kommersiella databassystem att kunna användas och därför kommer inget extra utvecklingsarbete att krävas för att lösa detta problem. Dessutom har man i kommersiella system också inbyggda sökrutiner varför inte heller detta kommer att kräva någon nyutveckling. Vad som kan vålla problem är de fall då osäker information, d v s sensorinformation eller information som extraherats ur sådan, behöver

analyseras. I dessa sammanhang måste systemen anpassas för hantering av sådan information eller också behövs tilläggsmoduler utvecklas.

3.3 Sensortyper

Val av sensorsystem för intelligent intrångsskydd

De sensorer som kan komma att användas för intelligent intrångsskydd är av varierande slag och har varierande egenskaper. I första hand är det bildgenererande sensorer som har bäst förmåga att bidra till ett system för intelligent intrångsskydd då dessa ger möjlighet till identifiering av möjligt hotfulla personer och fordon, samt deras aktiviteter. De vanligast förekommande sensorer som kan väljas för intrångsskydd, och för övervakning i samhället i övrigt, är främst kameror för visuellt ljus. Detta beror delvis på att det i allmänhet förutsätts att det är en människa som, utan något tekniskt stöd, ska söka i och tolka de bilder som sensorerna genererar. Sådana sensorer är väsentliga även för system för intelligent intrångsskydd. Det finns dock andra bildgenererande sensorer, med andra egenskaper, som kan komplettera kameror för visuellt ljus. Bland dessa är speciellt olika former av kameror för infraröda våglängder och ljusförstärkande kameror aktuella. Även laser eller radar kan komma i fråga, även om bildgenererande system för sådana våglängder idag är förhållandevis dyra och effektkrävande. Effektförbrukningen kan vara begränsande för mobila system för intrångsskydd. Givetvis förutsätter avancerade tillämpningar för intelligent intrångsskydd att bilder eller andra sensordata kan överföras till digitalt format. Detta måste ske i realtid om signalbehandling och datafusion ska kunna ske i realtid.

I enkla fall, där man omedelbart kan avgöra om hot förekommer genom att detektera att en person befinner sig på en viss plats eller passerar en viss gräns, så måste inte bildgenererande sensorer användas. Detta gäller t.ex. akustiska, seismiska eller elektromagnetiska sensorer. Även i mindre enkla fall kan dessa typer av sensorer ha en viktig roll att spela vid detektion, lokalisering och grov klassificering och kan användas för att rikta in bildsensorer. Akustiska sensorer kan t ex användas för att urskilja olika typer av fordon [Holmberg04].

De sensorer som är mest lämpliga för ett specifikt system för intelligent intrångsskydd beror på den anläggning som ska skyddas och på det hot som kan riktas mot anläggningen, d v s vilka angripare det är, vilken utrustning de har, vad som angriparen är ute efter och hur de beter sig. Skydd mot allmän skadegörelse skiljer sig naturligtvis ganska mycket mot skydd emot terrorism p.g.a. målet med aktionen, graden av planering, etc. Vilken hotbild som finns mot anläggningen bestämmer i sin tur vad man vill detektera hos människor eller fordon som rör sig omkring anläggningen. Detta betyder inte att system för det ena är värdelöst för skydd mot det andra, men att effektiviteten hos ett system där hotet har felbedömts kan vara begränsad. Speciellt gäller detta de fall där man använder sensorer som människor har svårt att tolka och automatiskt gör olika former av signalbehandling. En noggrann analys av de hot som riktas mot en anläggning måste därför göras för att systemet för intrångsskydd kunna designas och rätt sensorer skall kunna väljas. Anläggningens utseende påverkar vilka sensorer som är lämpliga genom att områdets storlek, geografi och väderförhållanden påverkar de sensorer som är lämpliga.

Förutom att sensorernas typ påverkas av hotets och anläggningens art, påverkas också sensorernas placering och antal i lika hög grad. I själva verket kan man naturligtvis inte välja typ eller antal sensorer utan att tänka på deras placering och vice versa.

Osäkerhet i sensordata

I de fall man använder sensorer för att skatta något objekts tillstånd finns det alltid osäkerhet förknippad med resultatet. Detta beror bl.a. på sensorernas fysikaliska begränsningar i upplösning, hur länge och ofta sensorerna kan observera de intressanta objekten och på approximationer och antaganden om objekten i signalbehandlingen. Även i de fall objekten beter sig eller ser ut ungefär som man förväntar sig, leder avvikelserna ändå till mindre felaktigheter och att resultatet måste

tolkas som osäkert. Dessutom påverkar osäkerheter i bestämningen av sensorernas positioner och i deras riktningsbestämning osäkerheten i de data som kan levereras. Slutligen kan användningen av sensorer i en miljö eller andra förutsättningar de inte är avsedda för leda till att data måste tolkas som mer osäkra än annars.

Styrning av sensorer för intelligent intrångsskydd

Eftersom de sensorer som kan användas för intelligent intrångsskydd skiljer sig åt i sina styrkor är det ofta fördelaktigt att låta informationen från vissa sensorer påverka andra sensorer. En förhållandevis enkel styrningsmetod är då att använda detektioner gjorda av enklare sensorer för att rikta in och fokusera bildgenererande sensorer. Dessa kan då göra en mer omfattande granskning av området för detektionen. Detta medför att t.ex. en kamera har större möjligheter att identifiera de objekt som kameran är avsedd för. Sådan styrning kan också användas för att begränsa användningen av kameror, både av kostnadsskäl och för att försäkra tillståndsmyndigheter om att kameraövervakning inte utförs utan anledning. Överföring av information mellan sensorer i syfte att styra beteendet kan också med fördel ske mellan bildgenererande sensorer av samma typ. Om en sensor av en viss typ har registrerat ett objekt kan information om objektets utseende i detta våglängdsband föras över till en sensor av samma typ, vilket medför att den andra sensorn kan anpassa sin signalbehandling för att öka detektionssannolikheten och/eller minska falskdetektionsrisken. För att anpassningen ska kunna ske i realtid krävs att det finns enkla modeller av de aktuella sensorerna. Detta behövs för att kunna förutsäga resultatet av eventuella förändringar i realtid. En omfattande beskrivning av styrning av sensorer ges i [Grahn05].

Aktuella sensorer

Möjligheterna för sensorer att utföra sina uppgifter beror bl a på den miljö de skall verka i. I t.ex. urban miljö finns ofta en mängd störande fenomen som inte finns i lantlig miljö. I en rapport [Svensson04] om sensorer i urban miljö finns en övergripande beskrivning av en mängd sensorsystems egenskaper i denna miljö.

Elektrooptiska sensorer

Bland de elektrooptiska sensorerna (EO-sensorer) räknas sensorer som registrerar värme eller ljus. Detta kan vara reflekterat från t.ex. sol eller måne, men också genererat av objekten själva. Dessa sensorer kan användas för detektion, följning, klassificering och identifiering av intressanta objekt. Bildgenererande elektrooptiska sensorer är de enda sensorer som kan användas för identifiering av de intressanta objekten och som är aktuella i ett system för aktivt intrångsskydd. I dagsläget kan inte en sådan funktion skötas automatiskt, utan det krävs en mänsklig användare för att uppnå robust identifiering. Förmågan till klassificering och identifiering beror i första hand på sensorns upplösning, avståndet till objektet, signal till brus förhållandet för objektet, på objektets detaljrikedom och på vädret. Dessutom måste eventuell rörelse hos objekten vara så liten att den inte medför oskärpa i bilden.

Kameror för visuellt ljus är de EO-sensorer som har bäst möjlighet till klassificering och identifiering. Regn och dimma påverkar naturligtvis en visuell kamera på samma sätt som det mänskliga ögat. Automatisk identifiering av människor är endast möjligt under gynnsamma omständigheter. Identifiering kräver därför i allmänhet operatörsassistans.

För att uppnå förmåga för sensorsystemet att klassificera eller känna igen olika former av fenomen även i mörker, krävs användning av andra bildgenererande sensorer än de som är känsliga i det visuella våglängdsbandet. I dessa fall kan man använda lågljussensorer, s.k. bildförstärkare, eller IR-sensorer.

En bildförstärkare förstärker det visuella ljus som finns tillgängligt, men fångar även upp viss värmestrålning. På natten är ljuset oftast reflekterat månljus, men då månljuset inte är tillgängligt

så kan atmosfärens luminiscens och eventuellt stjärnljus räcka för att ge goda bilder. En sådan modern bildförstärkare har goda möjligheter till att detektera och klassificera människor eller fordon på avstånd som är aktuella för aktivt intrångsskydd om vädret så medger. Identifiering av människor kräver gynnsamma omständigheter och mänsklig assistans för en robust funktion. Automatisk identifiering av fordon via dess bilnummer kan vara möjligt. Detta beror på de faktiska förutsättningarna vid den aktuella anläggningen. Bildförstärkarens prestanda begränsas i huvudsak av samma saker som begränsar en kamera för visuellt ljus, t.ex. av dimma eller dis. Även mycket svaga ljuskällor syns väl på långt avstånd, varför t.ex. ficklampor eller fotoblixtar är omöjliga att dölja på avstånd som är aktuella för aktivt intrångsskydd.

Olika typer av IR-sensorer är känsliga på olika våglängdsband. Dessa brukar benämnas med kort-, mellan- respektive långvågiga IR-sensorer. Beroende på det våglängdsband som en IR-sensor är känslig för, regerar den olika mycket på den värme som objekten utstrålar själv eller som den reflekterar från andra ljus- och värmekällor. En IR-kamera på det långvågiga våglängdsbandet är, i förhållande till andra EO-sensorer, bra på att detektera egengenererad värmestrålning från t.ex. människor. Denna är förhållandevis bra på att se igenom dimma, rök och dis. En kortvågig IR-kamera är mer känslig för reflekterad solstrålning och därmed mer känslig för dåligt väder. Bilderna från en kortvågig IR-kamera är dock mer detaljrika och mer lika de för visuellt ljus, varigenom de är enklare att tolka för en människa.

Även om de olika elektrooptiska sensortyperna har något olika potential vad gäller detektion, identifiering etc., är det många gånger signalanalysen som är den bestämmande faktorn för sensorsystemets prestanda. Det är alltså lika mycket signalanalysen som bestämmer prestandan hos ett system för intelligent intrångsskydd som det är sensorernas typ. I [Sidenbladh04] visas på möjligheter att urskilja mänskliga rörelser från andra rörelser. Det finns också metoder som t.o.m. bör gå att använda för att genom automatisk bildanalys bestämma vissa mänskliga beteenden, t.ex. om en person springer eller går, även om dessa inte är färdigutvecklade i dagsläget.

Akustiska sensorer

Akustiska sensorer för intelligent intrångsskydd fångar upp ljud som fenomen i omgivningen ger upphov till. Däribland finns fordon eller människor som intrångsskyddet är intresserat av, men det finns naturligtvis även en mängd andra ljudkällor som utgör en ointressant och störande bakgrund för systemet. Dessa sensorer kan, åtminstone sammankopplade i nätverk, bidra med detektion, följning och viss klassificering av intressanta objekt. Naturligtvis kan mikrofoner användas för ren avlyssning av personers samtal. Användningen av akustiska sensorer på ett sådant sätt är dock mycket känslig och bör undvikas. Om det inte är mänskligt tal som sensorerna ska användas för att registrera, utan kanske fordonstrafik, kan olika former av signalbehandling användas för att ta bort möjligheterna att identifiera samtalets innehåll och personerna som talar. För en mer utförlig beskrivning av akustiska sensorer för fordonsdetektion se [Habberstad02]. Exempel där systemen används för positionsbestämning i en svår miljö kan ses i [Sidenbladh05]. Sensorernas förmåga avtar med avståndet och påverkas också negativt av regn, snö och vind (beroende på vindens riktning och objektens position relativt sensorn). Däremot påverkas inte sensorerna av ljusförhållanden, d.v.s. tiden på dygnet eller dimma.

Seismiska sensorer

Seismiska sensorer för intelligent intrångsskydd fångar upp ljudets spridning i marken. De kan främst användas för detektion och viss klassificering, samt i vissa fall för följning om de är sammankopplade i nätverk och markens sammansättning medger detta. En beskrivning av prestanda hos ett sensornät med seismiska och akustiska sensorer finns i [Holmberg04]. Seismiska sensorer har kraftigt varierande räckvidd beroende på markens sammansättning, men är i övrigt okänsliga för ljus- och väderförhållanden. Speciellt är det övergångar mellan olika marktyper som försvårar ljudets utbredning och inte minst beräkningen av ljudkällans position. Detta begränsar möjligheterna att använda seismiska sensorer för följning. Dessutom kan det vara svårt att

bestämma lämpliga positioner för sensorerna då marksammansättningen och dess konsekvenser för ljudutbredningen är svår att bedöma utan experiment. Då markens egenskaper påverkar ljudutbredningen påverkas prestandan även av tjäle. Den viktigaste påverkan av tjäle är emellertid att det kan vara svårt att få sensorerna att ha tillräcklig markkontakt då marken närmast sensorn stelnar. Vissa former av seismiska sensorer måste skyddas mot regn.

Radar

Anledningar till radarns stora popularitet och framgång inom militära tillämpningar är dess goda förmåga vid svåra ljusförhållanden, svårt väder och på långa avstånd. En radar kan också, beroende på typ, användas för såväl detektion som följning och klassificering. Det finns ett stort antal typer av radar, men endast ett fåtal av dessa är relevanta för ett system för intelligent intrångsskydd. För intelligent intrångsskydd är de radar som används många gånger av enklare art och de används för att detektera och lokalisera rörliga objekt inom ett visst område, t.ex. krypande människor. I [Garcia01] och [Nelander05] ges exempel på radar med frekvenser på 10 eller 24 GHz som används för detta ändamål. Sådana system kan användas för att visa in optiska sensorer för identifiering och bör även kunna medverka till följning. Viss klassificeringsförmåga uppges i [Nelander05]. Radarns goda egenskaper på mycket stora avstånd erbjuder ingen konkurrensfördel när den ska användas för intelligent intrångsskydd.

Jämfört med t.ex. akustiska sensorer eller digitala TV-kameror är en radar ofta dyrare och mer effektkrävande. Detta gäller speciellt om radarn ska användas för klassificering och är bildgenererande. Vid högre frekvenser, ca 300 GHz , kan radar användas för klassificering på upp till 500 meters avstånd [Svensson04]. Lägre frekvens innebär samtidigt längre våglängd, vilket medför sämre möjligheter till klassificering och identifiering. Individuella fordon kan inte identifieras automatiskt idag. Andra experimentella system kan användas för att generera bilder genom väggar eller för att hitta dolda vapen [Nilsson05]. En översikt över system på mikrovågsområdet ges i [Nelander05].

Laser

Bildgenererande lasersystem används främst för klassificering av objekt, där de har mycket goda prestanda. Eftersom systemet är aktivt, d.v.s. själv emitterar det ljus som sedan mottas efter reflektion i omgivningen, blir inte systemen lika känsliga för omgivningens egenskaper som passiva, optiska sensorer. Den höga upplösning som systemen har medför också begränsningar i laserns synfält, vilket gör att systemet blir mer effektivt om det kan visas in av andra sensorer och därmed inte måste användas för att söka efter objekten. Tekniken är oberoende av ljusförhållanden, men känsligheten dämpas av dimma eller regn. Vissa system kan användas på mycket långa avstånd, över 10 km.

En typ av lasersensor som är mycket intressant för intelligent intrångsskydd och som inte är begränsat till spaning i små områden är optikspanare eller retroreflexdetektorer [Svensson04]. Dessa kan användas till att detektera optik från kikare, eller reflexer från CCD-kameror eller andra elektrooptiska sensorer som används för spaning emot anläggningen. Idag har tekniken kommit längst inom detektion av system som opererar på det synliga eller nära infraröda våglängdsområdet, medan tekniken för detektion av IR-sensorer är något mindre mogen. En kort sammanfattning av teknikläget inom optikspaning kan fås genom [FMV03].

Signalspaningssensorer

Med signalspaningssensorer avses i detta fall sensorer som kan användas till att spana efter aktiva signaler från sensor- och kommunikationssystem som inte tillhör intrångsskyddet eller anläggningen. Förutom sensorer för optikspaning som diskuterats ovan, skulle det kunna vara aktuellt att spana efter användningen av mobiltelefoner eller annan kommunikationsutrustning. Detta kräver dock tillstånd och sensorer med sådan förmåga kan därför inte användas i ett intelligent intrångsskydd för att detektera hot mot olika anläggningar.

Andra sensorer

Förutom de sensortyper som diskuterats ovan finns några av enklare art som t.ex. IR-barriärer, stängsellarm eller hydrauliska, tryckkänsliga sensorer. Dessa system kommer inte att diskuteras vidare i denna rapport. För en utförligare beskrivning av dessa och liknande sensorer hänvisas till [Garcia01] och [Nastell02].

4. Aspekter på intelligent intrångsskydd

Intelligenta intrångsskydd kan vara av varierande slag beroende på vilken typ av anläggning som avses. Två huvudgrupper av anläggningar kan identifieras. Dessa har här kallats för *fristående anläggningar* samt *knutpunkter i olika infrastrukturer*. Knutpunkter är av speciellt intresse eftersom t ex attentat/inbrott mot sådana anläggningar troligen kommer att ha större konsekvenser än motsvarande aktioner mot mellanliggande länkar, t ex elkraftledningar, skulle kunna få. Av denna anledning kommer vi här inte att diskutera sådana länkar. Inte heller kommer vi att diskutera järnvägsstationer, tunnelbanestationer eller sådana delar av flygplatser som ankomst och avgångshallar. Detta hänger samman med att dessa typer leder till alltför komplexa problem som i hög grad berör problem relaterade internt skydd av skyddsanläggningar, vilket inte behandlas i detta arbete. För övrigt gäller för flygplatser att där redan existerar olika typer av interna säkerhetsskydd. Gemensamt för dessa kategorier är också att i dessa anläggningar rör sig, åtminstone periodvis, stora mängder människor, vilket leder till mycket komplexa problem; speciellt vid analys av sensordata. Komplexiteten i samband med förekomsten av stora människomassor vid dessa anläggningar har varit vägledande för att i nuläget välja bort dessa anläggningar.

4.1 Tillämpningsberoende problem

En typ av problem att studera i relation till olika tillämpningar är hur annan information än sådan som kommer från sensorer skall nyttiggöras, detta för att erhålla en bättre beskrivning av den allmänna hotbilden. Exempel på sådana informationskällor är bl a underrättelser, kriminalstudier och rapporter från tjänstenätverk, agenturer och nyhetsbyråer av olika slag [Garcia01]. Genom denna typ av tilläggsinformation kan beredskapen kring anläggningen vid behov höjas och som en konsekvens av detta bör också aktivitetsgraden i systemet öka. Hur dessa rapporter skall hanteras är givetvis avhängig deras karaktär. Vissa av dessa rapporter kan vara av specifik typ riktade mot en specifik anläggning och kan i sådana fall likställas med information inhämtad från någon sensor. I sådana fall måste operatören naturligtvis agera på motsvarande sätt.

Andra iakttagelser av intresse i samband med olika skyddstillämpningar berör frekvensen av registrerade avvikande händelser. I de fall där man har registrerat många olika onormala händelser runt en anläggning och där frekvensen av dessa kanske ökar, samtidigt som man inte kan hitta några samband mellan de olika aktiviteterna bör man undersöka om ökningen i sig är att betrakta som att något onormalt är under uppsegling; detta oberoende av om något mönster kan identifieras. En annan indikation som har beröring med detta är t ex om flera likartade händelser har registrerats utan att man kan se något samband dem emellan. Frågan är då vilka konsekvenser detta kan förväntas ha på händelseutvecklingen. Även i dessa samanhang bör man betrakta det inträffade som del i något onormalt som kan tänkas utvecklas till ett framtida hot. Till detta kan ytterligare en tolkning läggas nämligen att objektet är utsatt för flera antagonistiska hot samtidigt.

Annan information än den information som direkt avser objekt som detekteras och som kan vara av betydelse är vad som i andra sammanhang brukar kallas för kontextuell information d v s information om omgivningen. Detta kan också gälla väderinformation eftersom den kan påverka registreringen av sensordata men även hur läget i övrigt skall tolkas, t ex det är mindre troligt att någon har en picnic om det regnar. Emellertid, avses med kontextuell information inte bara omgivningen kring anläggningen utan man bör även inkludera omfattningen av den omgivande trafiken t ex hur många fordon brukar passera vid en viss given tidpunkt samt också väder och ljusförhållanden. D v s den person som är ute för att spana väljer hellre att göra detta när trafikintensiteten är som störst och helst mitt på dagen.

Omgivningen kan också omfatta information av typen, vilka accessvägar leder fram till anläggningen, var är man inte synlig i förhållande till övervakningskamerorna etc. Detta problem diskuteras och vidare ur mer generell bemärkelse i [McEntire04].

En annan viktig fråga är om man har missat någon viktig händelsetyp i systemutvecklingsprocessen. Även i detta fall gäller att man bör fortsätta att analysera data för att öka kunskapen om vad som kan betraktas som onormalt. D v s endast genom ständiga förbättringar av systemet kommer det att vara möjligt att hålla det i gott operativt skick.

Av intresse, att studera vidare, är om det kommer att vara möjligt att utveckla ett intrångsskydd med olika skyddsnivåer, d v s ett system med olika skal där intrång i ett yttre skal kommer att medföra enbart en svag reaktion på en onormal händelse med intrång i något inre skal bör ge en mycket kraftfullare reaktion.

För att få en adekvat bild av kraven på systemet måste även experter och användare intervjuas. En sammanställning av dessas kunskaper erbjuder sina egna svårigheter. När systemen blir tillräckligt komplexa kan det vara svårt för utomstående att ställa de rätta frågorna. Experter och systemanvändare kan ha många års yrkeserfarenhet bakom sig. Att ta fram de kunskaper som finns med enkla intervjuer visar sig ofta svårt. Även bortsett från de välkända problem som kan uppstå vid insamling av experters kunskap, och för vilkas lösning det finns många ansatser t.ex. [Christoffersen03], kan kunskapen vara mycket känslig och omfatta information som de inte vill delge någon. En del av en lösning kan då vara att tillhandahålla databaserade verktyg för att användare eller säkerhetsansvariga själva skall kunna specificera vad de vill att systemet ska leta efter.

En slutsats av diskussionen ovan är att även om det finns många likheter hos de system som ska skydda olika anläggningar så krävs viss ny analys och datagenerering för varje anläggning som ska skyddas. Olika anläggningar, hot, kostnadskrav etc. leder till delvis olika system. Vid utveckling av nya system för intelligent intrångsskydd kan det dessutom vara lämpligt att bygga systemet i olika etapper, med olika grad av verklighetskrav i de olika etapperna.

4.2 Falsklarm

En fråga av betydelse är vad som menas med falsklarm. Å ena sidan kan man med detta mena att man registrerat ett antal olika händelser som klassats som onormala och där under den efterföljande tiden inget intrångsförsök har skett. Den väsenligaste frågan blir då huruvida detta skall tillmätas någon vikt överhuvudtaget. Två skäl kan ligga bakom ett falsklarm, dels kan ett planerat intrångsförsök ha blivit inhiberat på grund av ökad aktivitet från skyddsorganisationen dels kan ett annat alternativ vara att en operatör misstolkat informationen i systemet, d v s att det inte rör sig om någon onormal händelse. Dessutom kan det röra sig om en onormal händelse utan att det för den skull behöver vara ett hot som ligger bakom, d v s det är inget riktigt falsklarm. Det senare är naturligtvis önskvärt ur förövarens synvinkel eftersom denne inte vill dra uppmärksamheten till sig. Det är svårt att avgöra vilket av dessa skäl som är det troliga.

En annan fråga som relaterar till detta är hur lång tid som får anses vara rimlig innan man kan anse att det inte föreligger något hot som en konsekvens av de registrerade händelserna. Förhållandet är dock att båda fallen är att betrakta som falsklarm även om man inte alltid kan påvisa detta. Emellertid bör man ständigt fortsätta att analysera inkommande information för att uppnå ökad kunskap om vad som är onormalt beteende. I övrigt bör man observera att för många larm utan synbarliga konsekvenser, falska eller inte, kan leda till att användarna förlorar tilltron till systemet. I det motsatta fallet d v s om systemet sällan eller aldrig går igång kan detta leda till att operatörerna inte blir tillräckligt erfarna systemanvändare men även då förlorar tilltron till systemet. Detta kan medföra att operatörerna fattar felaktiga beslut i något avseende eller värre underlåter att fatta något beslut alls.

4.3 Fristående anläggningar

Med fristående anläggningar avser här anläggningar av typ förråd av olika slag, fångvårdsanstalter, kärnkraftverk, offentliga byggnader, men också historiska byggnader såsom slott och kyrkor kan

räknas hit, även om de senare troligen inte löper samma risk för att bli utsatta för antagonistiska hot som de övriga.

4.4 Knutpunkter i infrastrukturella nätverk

Exempel på knutpunkter i olika infrastrukturer är, förutom de som nämnts ovan, väsentligen också anläggningar för överföring av bl a el och gas. Vad beträffar de senare så förekommer inte så många sådana nätverk i Sverige ännu. I elöverföringssammanhang gäller att de känsligaste delarna återfinns bland ställverk och olika kraftverksanläggningar såsom vatten- och kärnkraftverk. Konsekvenserna av ett förstört ställverk genom exempelvis ett terroristangrepp kommer att vara mer omfattande än de risker som tas av angriparna. Mot denna bakgrund kan man säga att skyddsbehovet för sådana anläggningar är stort.

4.5 Systemutvecklingsmiljö

För att kunna utveckla och värdera system för intrångsskydd av den karaktär som diskuteras i denna rapport, kan ett flertal tekniker för datainsamling och datagenerering användas. Ofta är en kombination av tekniker nödvändig för att visa att en avsedd systemfunktion uppnåtts till en rimlig kostnad och på rimlig tid. En teknik som kan komma ifråga är (naturligtvis) insamling av sensordata med verkliga sensorer vid en anläggning av den typ som systemet är avsett att skydda. Samtidigt som detta är den bästa tekniken för att försäkra sig om att problemets svårigheter inte vare sig underskattas eller överskattas, kan det visa sig svårt att genomföra fullt ut då kostnaden kan vara stor eller man kan stöta på problem med integritetsfrågor, se kap. 5. Andra svårigheter kan uppträda när man vill iscensätta ett händelseförlopp av den art man vill skydda ifrån, eftersom de anläggningar man vill skydda är i dagligt bruk och driften inte får störas av informationsinsamling för forsknings- eller utvecklingsändamål.

Insamling av verkliga sensordata måste sannolikt kompletteras av simulering av sensordata och relevanta händelser, samt intervjuer av experter och användare av dagens system för intrångsskydd. Simulering av händelser och sensordata har i detta sammanhang fördelar då man inte måste störa arbetet på aktuella anläggningar eller behöver söka tillstånd för sin datainsamling. Dessutom kan man vid simulering återupprepa händelsen under något skilda förutsättningar, varför en bredare analys av händelsen kan göras. Naturligtvis måste simuleringsmodellen som används vara tillräckligt verklighetstrogen. För att kunna genomföra trovärdiga simuleringar av alla ingående sensorer krävs stor erfarenhet av dessa.

4.6 Områdeslitteratur

Litteratur som beskriver området finns ännu så länge i ganska begränsad omfattning eftersom problemområdet är relativt nytt. I den förekommande litteratur som på ett allmänt plan diskuterar skydd av olika anläggningstyper finns ett arbete av Garcia [Garcia01]. Emellertid finns inte intelligenta intrångsskydd omnämnda i detta arbete. Även om olika sensortyper diskuteras så sker ingen diskussion om metoder för sensordataanalys, sensordatafusion eller hur beslutsstöd skall komma till användning. Man kan, detta till trots, se detta arbete som en bra introduktion till området intrångsskydd, eftersom skyddsproblematiken diskuteras på ett ingående sätt i övrigt.

I Svenska kraftnätsrapport [Nastell02] beskrivs ett antal experiment som genomförts med ett antal olika sensorer, bl a övervakningskameror, markkablar och IR-barriärer. Ett antal experiment har genomförts under varierande betingelser, bl a olika väder- och ljusförhållanden. Proven som genomfördes var avsedda för manuell övervakning och omfattade således inte några försök till att automatisera detektering och igenkänning av olika objekt för att avgöra om dessa uppträdde på något onaturligt sätt. Dessa experiment kan ses som mycket intressanta och i grunden ett viktigt steg på vägen mot ett mer intelligent system.

Connell m fl [Connell04] visar hur man genom att analysera videosekvenser kan bestämma spåret hos ett fordon för att i ett senare skede kunna avgöra uppträdande är avvikande. I Woods m fl

[Woods05] beskrivs ett händelseberoende system med förmåga till samarbete mellan människa (operatör) och system med syftet att genomföra vad som kallas säkerhetsspaning (security surveillance), där målet är att identifiera händelser av onormal karaktär för att undvika falska larm. En händelse betraktas som en förändring över tiden eller dess motsats, d v s som en brist på förändring när en sådan förväntas. Ytterligare ett arbete av visst intresse är [Stauffer00], som beskriver en metod som genom inlärningsmönster ger stöd för realtidspårning av olika objekt och som har delvis samma målsättning som i [Connell04]. Ett annat arbete med liknande inriktning återfinns i [Seibert06]. Här är utgångspunkten förmågan att detektera, klassificera och spåra händelser i och omkring hamnar.

5. Integritetsfrågor

Då man vill övervaka områden omkring skyddsvärda anläggningar finns alltid risken att oskyldiga människor blir registrerade av den sensorutrustning som används. Detta kan uppfattas som integritetskränkande av enskilda eller organisationer. För att väga intresset av integritetsskydd för allmänheten mot intresset av att ha ett gott skydd för skyddsanläggningarna finns en omfattande lagstiftning. Denna behandlar i första hand användningen av kameror och ljudinspelningar, men gäller egentligen all utrustning som kan användas för att identifiera individer och deras förehavanden.

Det reglerna säger är att man, med vissa undantag som inte har relevans [1] för intelligent intrångsskydd, endast får utföra permanent övervakning i brottförebyggande syfte. Om det ändamål man har i åtanke är i linje med lagstiftningen bedöms av Länsstyrelsen, vilka utfärdar tillstånd för övervakning. Det är ofta svårt att få tillstånd till övervakning av områden dit allmänheten har fritt tillträde. Om området däremot är inhägnat är läget ett annat och tillstånd krävs inte. Dock måste man alltid anmäla att man övervakar ett område till Länsstyrelsen, varvid de naturligtvis har möjligheten att bedöma om tillstånd krävs eller inte.

Regelverket säger också att övervakning av skyddsobjekt får ske utan att man måste ansöka om tillstånd. Precis som tidigare måste man anmäla detta till Länsstyrelsen och det krävs också att syftet är brottsförebyggande. Enligt [Nastell02] är det också klart att olika Länsstyrelser har olika tolkning av lagstiftningen och tillstånd kan krävas av vissa Länsstyrelser, men inte av andra. Lagstiftningen skiljer också på system som lagrar bilder för möjlighet till senare åtkomst och de system där bilden enbart kan betraktas i realtid. Det är svårare att få tillstånd till system där bilderna lagras.

Förutom vanliga kameror som registrerar visuellt/optiskt ljus gäller lagstiftningen lika för alla kameror som registrerar infraröda våglängder. I de fall man kan identifiera en person med en radarsensor eller en lasersensor torde samma lagstiftning gälla även här. I dessa fall är det emellertid enkelt att tänka sig sensorer som inte kan användas för identifiering utan endast för att avgöra att den bild som genereras innehåller en människa, kanske dennes längd och andra relativt grova karaktärsdrag, eller om någon springer i bilden etc. Vad lagstiftningen säger angående sådana sensorer är idag oklart. Detta gäller också i de fall då man kan garantera att sensorerna är placerade på ett sådant sätt att identifiering inte är möjlig, t.ex. på tillräckligt långt avstånd.

Förutom de fall där man av fysikaliska skäl inte kan identifiera en individ finns andra tekniska möjligheter att begränsa möjligheterna till identifiering av individer på bilderna. På FOIs avdelning för sensorteknik har ett koncept tagits fram för detta, s.k. integritetsskyddad övervakning [Sidenbladh05]. I korthet går konceptet ut på att med signalbehandlingsmetoder maskera alla individer i bilden för att omöjliggöra identifiering av en obehörig användare, samtidigt som man analyserar bilden för att extrahera den information som är tillräcklig för att utföra uppgiften. T.ex. skulle det ibland kunna räcka att man detekterar att personer i bilden springer. I dagsläget är detta enbart ett koncept som bedöms möjligt att utveckla, men som inte har testats eller prövats av någon tillståndsmyndighet.

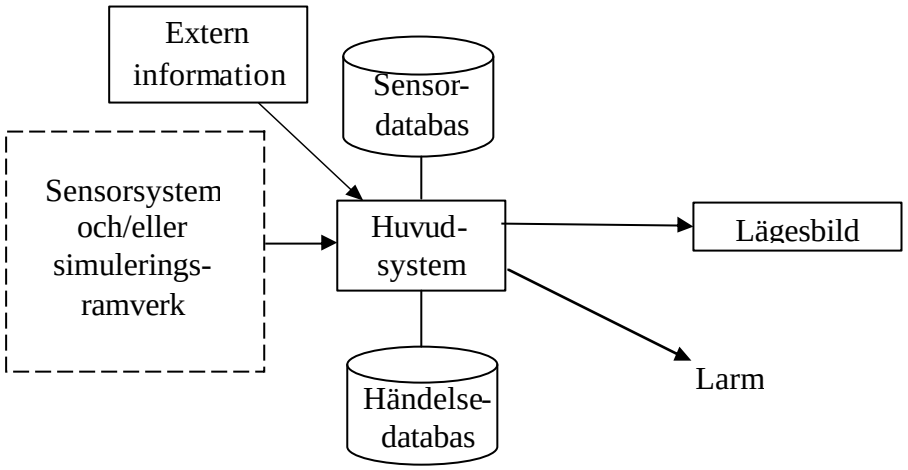
Sammanfattningsvis kan upprepas att värdet av allmänhetens rätt till skydd mot integritetskränkning måste vägas emot skyddsbehovet för skyddsobjektet. Om en ansökan kan göra trovärdigt att skyddseffekten med ett nytt tekniskt system är tillräckligt stort för den aktuella anläggningen och att vederbörlig hänsyn tas till allmänhetens integritet, bör en sådan ansökan ha goda möjligheter att bli beviljad. Det slutgiltiga avgörandet av hur dessa värden ska avvägas är emellertid politiskt och inte tekniskt. Problemet kan undvikas helt genom att använda data som är

[1] Det kan t.ex. röra sig om övervakning på kasinon eller trafikövervakning av vägverket.

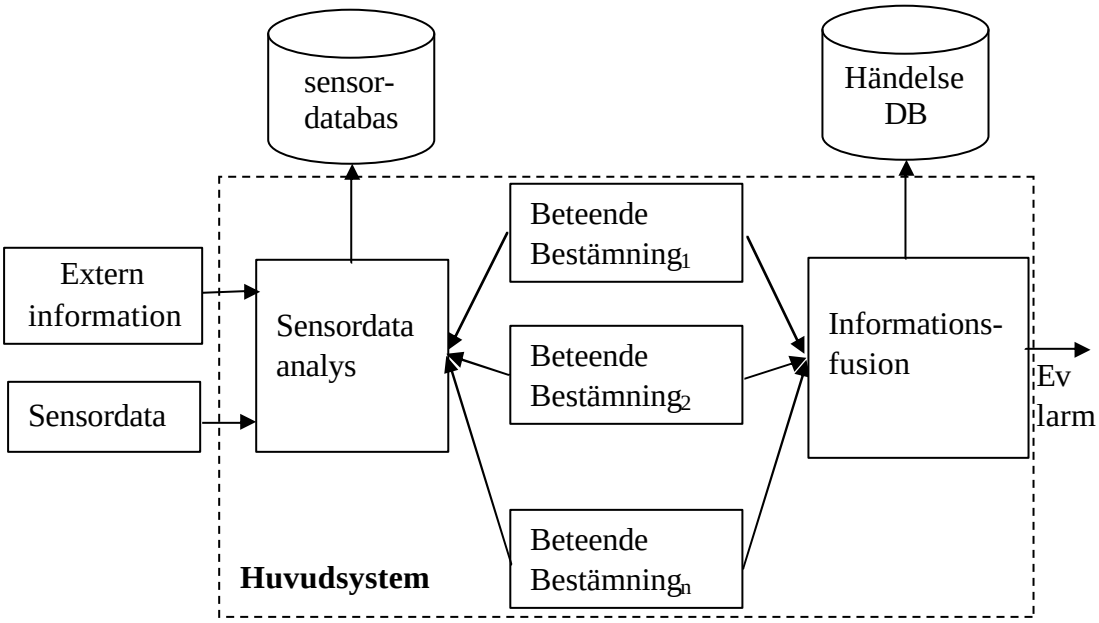
simulerade eller insamlade med de medverkandes samtycke. Nyttan med ett system för aktivt intrångsskydd kan då tydliggöras utan att någons integritet riskerar kränkas. Därefter finns också bättre möjligheter att göra avvägningen mellan nytta och integritetskrav.

6. Systemstruktur

Systemstrukturen hos ett möjligt intelligent system för intrångsskydd framgår av figur 6. Indata till detta system kan komma antingen från ett sensorsystem eller från ett simuleringsramverk med simulerade sensordata. Det senare fallet kan utnyttjas för systemutveckling då behovet av att kunna kontrollera formerna för systemet föreligger. De till systemet inkommande data tas om hand av huvudsystemet och lagras i en sensordatabas. Data analyseras efterhand och den resulterande informationen lagras därpå i händelsedatabasen. Denna information kan sedan analyseras vidare m a p tid och rum för att bestämma eventuellt pågående onormala händelser. Då någon onormal händelse registrerats kan ett larm skickas till operatören. I lägesbilden visualiseras efterhand information om olika händelser, som dock inte behöver vara onormala utan behöver bara återger det aktuella läget för att ge operatören en bild av detta. Extern information kan vara underrättelse information av olika slag t ex information om stulna bilar eller om andra händelser som är relevanta i samband med analysen av i övrigt registrerade data.



Figur 6. Systemöversikt



Figur 7. Grundläggande metodbeskrivning avseende onormalt beteende

Insamlade sensordata skall i ett första steg analyseras m a p sitt innehåll. Detta första steg inkluderar inte bestämning av de olika registrerade objektens beteende, utan avser bestämning av objekten, deras attribut och statusvärden såsom hastighet och färdriktning över tiden, men också

olika typer av objektsamband. I anslutning till denna analys kan också extern information komma till användning. Bestämning av olika aspekter på beteenden sker i ett därpå följande steg, d v s genom att använda multipla metoder blir det möjligt att bestämma en mängd olika aspekter av vad som kan betecknas som onormalt beteende, vilket framgår av figur 7. Beteendebestämningen kan bestå av flera metoder i enlighet med vad som diskuterats tidigare. I ett slutligt steg kan resultatet av de olika metoderna fusioneras. Resultatet av informationsfusionssteget lagras i händelsedatabasen och i de fall något onormalt registrerats utgår också ett larm.

Eftersom tids- och rumsaspekter spelar en central roll i systemet kommer metoder för att hantera sådana aspekter att behöva utnyttjas. Metoder lämpliga för detta kan vara grundade på logiska beskrivningar av de registrerade objekten. Andra aspekter som behöver beskrivas är olika objektsamband över tid och rum. Metoder som lämpar sig för dessa beskrivningar kan vara så kallade ontologier, vilka numera är en vanligt förekommande metodik. I [Little05] beskrivs rumsligt och temporalt anpassade ontologier som primärt syftar till användning i krishanteringssammanhang i samband med informationsfusion. Det är troligt att sådana typer av ontologier även lämpar sig väl för de problem som diskuteras här.

7. Sammanfattning

I denna rapport har grundläggande krav på intelligenta intrångsskydd diskuterats. Sådana intrångsskydd kan sägas vara del i ett mer omfattande område, som här kallas för intelligenta skyddsfunktioner, som även kan innefatta besläktade tillämpningar såsom internt skydd av järnvägstationer. I det arbete som beskrivs i denna rapport, och som utgör en förstudie, ligger emellertid fokus på de behov som kan identifieras i anslutning till intelligenta intrångsskydd för olika typer av skyddsanläggningar.

Bland de mest centrala problemområdena som har identifierats återfinns utveckling av sensorsystem, beslutstödssystem, samt också av en mängd olika typer av analysmetoder. Till de senare hör metoder för analys av sensordata, metoder för bl a databrytning, metoder för bestämning av beteenden hos misstänkta objekt, samt också behov av att utveckla metoder på hög nivå för informationsfusion, för att slutligen avgöra om en systemoperatör skall larmas då ett potentiellt hot kan föreligga. Samtliga dessa delar måste belysas för att möjliggöra utveckling av system för skydd av skyddsanläggningar.

Integritetsproblem kommer att uppstå i anslutning till både utveckling och användning av den typ av system som har skisserats i detta arbete. Mot denna bakgrund måste hänsyn tas till problem relaterade till allmänhetens behov av integritetsskydd. Därför måste speciella hänsyn tas redan i systemutvecklingsfasen. Den lösning som föreslås för att eliminera integritetsproblemen i systemutvecklingsfasen är därför att genomföra systemutvecklingen i en simulerad miljö med användning av främst simulerade data, men också av data som inhämtats under kontrollerade former. En sådan kraftfull simuleringsmiljö finns redan tillgänglig vid FOI i Linköping. Detta gör det möjligt att på helt laglig grund utveckla system av detta slag. En konsekvens av användningen av denna simuleringsmiljö blir också att systemen kan testas och demonstreras under realistiska former. Till detta kommer att också att man, ur ett integritetsperspektiv, kan visa på vilka konsekvenser blir för allmänheten då systemen tas i bruk. Detta gör det således möjligt att redan tidigt visa på vilka eventuella integritetskränkningar som enskilda individer kommer att ställas inför under systemets användning.

Till sist anser vi att det är fullt möjligt att realisera system av denna typ och applicera dem på ett antal realistiska tillämpningar som samhället kan ha behov av för att skydda sig mot. Främst för skydd av skyddsanläggningar, vilket är det primära syftet för denna studie, men också för att skydda individer mot potentiella antagonistiska hot och angrepp.

8. Slutsatser

Nyttan av ett system för intelligent intrångsskydd för skydd av skyddsvärda anläggningar är flerfaldig. Genom att ett intelligent intrångsskydd kan arbeta dygnet runt under alla väderförhållanden utan att förtröttas kommer behovet av vaktpersonal/operatörer att kunna hållas nere. Därigenom kommer också övervakningskostnader för samhälle, industri och andra användarorganisationer att kunna begränsas. Vidare kommer det att bli möjligt att begränsa skadorna av ett intrång genom att det intelligenta intrångsskyddet kan bidra till tidig upptäckt av intrångsförsöket. Därmed kan den tillgängliga tiden för beslutsfattande förlängas men även preventiva åtgärder kan genomföras. Detta gäller både vid själva intrångsförsöket som vid rekognosering inför ett intrångsförsök. Många gånger är det försent att reagera när väl hoten sätts i verket, men med ett intelligent intrångsskydd kan man tidigt registrera aktiviteter som i ett senare skede kan leda till brottsliga intrång.

I samhället finns ett stort antal objekt av varierande typ som måste skyddas mot brottsliga aktiviteter eller mot olika typer av terrorhandlingar. Skydd av dessa anläggningar kostar årligen samhället stora belopp. Det är därför angeläget att förhindra aktiviteter av dessa slag. Vinsterna av att implementera och utnyttja system med intelligent intrångsskydd bedöms vara stora och behovet av denna typ av system kan förväntas öka i en nära framtid. Av denna anledning kan man anta att svensk industri är intresserad av att delta i utvecklingsarbete för att ta fram system av denna typ. Detta gäller speciellt eftersom system av detta slag kommer att kunna användas globalt och att det därför finns en omfattande marknad för produkter av detta slag.

Möjligheterna att realisera system av intelligenta intrångsskydd är beroende av att ett antal forskningsfrågor, till vilka bl a hör problem kring databrytning och informationsfusion. Vidare är det nödvändigt att för att system av detta slag skall vara användbara, även i ett längre perspektiv, arbete ständigt bedrivs för att identifiera nya typer av aktiviteter och händelser, som kan utgöra hot mot anläggningarna. Kunskaper om sådana aktiviter måste därför införas i systemets kunskapsdatabas. Detta är ett förhållande som gäller alla typer av kunskapsbaserade system och som därför inte är unikt i detta sammanhang.

System för intelligenta intrångsskydd kommer att kunna realiseras. Emellertid måste man konstatera de problem som behöver lösas för att göra dem användbara inte är triviala. Av denna anledning är fortsatt forskning nödvändig även i ett längre perspektiv. Detta hindrar dock inte att man under relativt kort tid kan genomföra ett utvecklingsprojekt, se projektförslaget i Appendix, på rimligt kort tid, där resultatet utgörs av en demonstrator som snabbt kan produktifieras.

Vid FOI i Linköping finns kompetens bl a inom områdena sensorteknik, informationsfusion samt beslutsstöd och systemutveckling. Det finns därför goda förutsättningar att vid FOI utveckla en realistisk demonstrator för intelligent intrångsskydd av skyddsanläggningar.

Referenser

[Anderson79] Anderson, B. D. O., Moore, J., B., *Optimal Filtering*, Prentice Hall, Englewood Cliffs, N. J., USA, 1979.

[Chang04a] Chang, S.-K., Costagliola, G., Jungert, E., Orciuoli, F., *Querying Distributed Multimedia Databases Data Sources in Information Fusion Applications*, IEEE Transaction on Multimedia, Vol. 6, No. 5, 2004, 587-702.

[Chang04b] Chang, S.-K., Jungert, E., Li, X., *A progressive Query Language and interactive Reasoner for Information Fusion*, in Journal of Information Fusion, Elsevier,http://www.sciencedirect.com/science?_ob=MImg&_imagekey=B6W76-4HG69VD-1-1N&_cdi=6618&_user=641931&_orig=browse&_coverDate=11%2F02%2F2005&_sk=999999999 &view=c&wchp=dGLzVzz-zSkzV&md5=e47a7b7ca530432d6ef8c5abc38d8b09&ie=/sdarticle.pdf.

[Chen01] Chen, Z., *Data Mining and Uncertain Reasoning- An Integrated approach*, John Wiley & sons, New York, NY, 2001.

[Christoffersen03] Christoffersen, K., Blike, G., T., Woods, D., D., *Discovering the Events Expert Practitioners Find Meaningful in Dynamic Data Streams*, Cognitive Systems Engineering Laboratory, Institute for Ergonomics, Ohio State University, Columbus, OH., USA, 2003.

[Connell04] Connell, J. H.,Senior, A. W.,Hampapur, A.,Tian, Y.,Brown, L.,Pankanti, S.: *Detection and tracking in the IBM PeopleVision system*, Proceedings of the 2004 IEEE International Conference on Multimedia and Expo, ICME 2004, 27-30 June 2004, Taipei, Taiwan, pp 1403-1406.

[Demsar06] Demsar, U., *Data Mining of Geospatial Data: Combining Visual and Automatic Methods*, Doktorsavhandling, Inst. för Fotogrammetri ach Geoinformatik, KTH, 2006.

[FMV03] *Teknisk Prognos Fotonik*, FMV Analys 21841/10115:03, 2003.

[Garcia01] Garcia, M. L., *The Design and Evaluation of Physical Protection Systems*, Butterworth and Heinemann, Boston, 2001.

[Grahn05] Grahn, P., Grönwall, C., Herberthson, M., Kaijser, T., Lantz, F., Strömberg, D., Ulvklo, M., *Sensor Control in NCW, Problem description and important areas*, Technical report, FOI-R--1860--SE, 2005.

[Guan91] Guan, J., Bell, D., A., *Evidence theory and its applications Volume 1*, Elsevier, 1991.

[Habberstad02] Habberstad, H., Kullander, F., *Fältförsök med akustiska och seismiska givare för fordonsdetektion*, Metodrapport, FOI-R--0703--SE, 2002.

[Hall01] Hall, D. L., Llinas, J. (Eds.), *Handbook of Multisensor Data Fusion*,CRC Press, New York, 2001.

[Holmberg04] Holmberg, M., Lauberts, A., Lennartsson, R. K., *Slutrapport för projektet Interaktiva adaptiva Marksensornät*, FOI användarrapport, FOI-R—1450—SE, December 2004

[Jungert05] Jungert, E., Folkesson, M., Fransson, J., Horney, T., Lantz, F., Silvervarg, K., *Ett frågebaserat beslutsstödssystem för nätverksbaserade ledningssystem*, FOI rapport, FOI-R—1787—SE, September 2005.

[McEntire04] McEntire, D. A., Myers, A., *Preparing Communities for disasters: issues and processes for government readiness*, Journal of Disaster Prevention and Management, Vol. 13, No. 2, 2004, pp 140-152.

[Menas03] Menas, J., *Investigative Data Mining for Security and Criminal Detection*, Butterworth and Heinemann, Boston, 2003.

[Nelander05] Nelander, A., Erickson, R., *Systemanalys flexibla mikrovågssystem*, Teknisk Rapport, FOI-R--1865--SE, 2005.

[Nilsson05] Nilsson, S., Axelsson, D., Gustafsson, M., Jänis, A., Kjellgren, J., Sume, A., Örbom, A., *Teknisk värdering av nya sensorförmågor för strid i bebyggelse, Årsrapport 2005*, FOI teknisk rapport, FOI-R—1862—SE, December 2005.

[Little05] Little, E. G., Rogova, G. L., *Ontology Meta-Model For Building A Situational Picture Of Catastrophic Events*, Proceedings of the international conference on Information Fusion, Philadelphia, PA, July, 2005.

[Seibert06] Seibert, M., Rhodes, B. J., Bomberger, N. A., Beane, P. O., Sroka, J. J., Kogel, W., Kreamer, W., Stauffer, C., Kirschner, L., Chalom, E., Bosse, M., Tillson, R., *SeeCoast port Surveillance*, Proceedings of SPIE Vol. 6204: photonics for Port and Harbour Security II, Orlando, FL, USA, April 18-19, 2006.

[Sidenbladh04] Sidenbladh, H., *Detecting human motion with support vector machines*, IAPR International Concerence on Image processing, Vol. 2, pp. 188-191, 2004.

[Sidenbladh05] Sidenbladh, H., Ahlberg, J., Klasén, L., *New Systems for Urban Surveillance*, User report, FOI-R--1668--SE, 2005.

[Stauffer00] C. Stauffer and W. Grimson, *Learning pattern of activity using realtime tracking, IEEE Trans. Pattern Anal. Machine Intell.*, vol. 22, no. 8, pp. 747–757, Aug. 2000.

[Svensson04] Svensson, L., Ahlberg, J., Axelsson D., Habberstad, H., Jonsson, N-H., Jänsis, A., Kariis, H., Kjellgren, J., Murdin, D., Nilsson, S., Svedin, J., *Inledande studie Sensorer för urban miljö*, Underlagsrapport, FOI-R--1420--SE, 2004.

[Nastell02] Nastell, P., *Realiserbarhetsstudie Teknisk och Personell Bevakning*, Svenska Kraftnät, Slutrapport, 2002-05-30.

[Woods05] Woods, D. , McNee, S. , Davis, J., Morison, A., Maughan, P., and Christoffersen, K., *Event Template Hierarchies as Means for Human-Automation Collaboration in Security Surveillance*, Human Factors and Ergonomics Society Annual Meeting, Orlando, FL, September 26-28, 2005,

[Zimmermann91] Zimmermann, H.-J., *Fuzzy set theory and its applications*, Kluwer Academic Publishers, 1991.

Appendix

Förslag till projektplan

Allmänt
Projektet syftar till att demonstrera principerna för intelligent intelligent intrångsskydd av olika typer av skyddsanläggningar. Målsättningen med projektet (steg 1 och steg2) är att utveckla en prototyp för detta ändamål. Projektet kommer att genomföras i två steg. Mellan steg 1 och steg 2 görs en utvärdering och en eventuell ominriktning av projektet. För att inte nuvarande lagrum skall förhindra genomförandet av projektet kommer data som behövs för utveckling och demonstration av prototypen att insamlas genom intervjuer med användare och säkerhetsexperter men också med sensorer under kontrollerade former vid lämpliga skyddsobjekt.

För utveckling av prototypen kommer det vid FOI utvecklade simuleringsramverket MOSART att utnyttjas, vilket kan behöva viss anpassning. Eftersom det kan antas att olika myndigheter till viss del har olika behov kommer det att bli nödvändigt att genomföra anpassade demonstrationer som svarar mot de olika behoven. Simuleringen av prototypen kommer att genomföras i steg 2 av projektet.

Steg1: Konceptutveckling
Projekttid: 4 månader
Delmoment:

Intervjuer av användare och säkerhetsexperter.
Identifiering av lämpliga sensortyper.
Identifiering av sensormodeller för simuleringsmiljö samt av lämpliga metoder för sensordataanalys.
Identifiering av lämpliga tillämpningar för demonstration av det slutliga systemet.
Framtagande av konceptlösning.
Utarbetande av projekt- och kostnadsplan för projektsteg 2.
Avrapportering.

Steg 2: Prototyputveckling
Projekttid: ca 12 månader
Preliminära delmoment:

Anpassning av simuleringsmiljö.
Implementering av sensormodeller och metoder för sensordataanalys.
Utveckling och implementering av beslutsstöd.
Utveckling av metoder för databrytning.
Prototyputveckling/integration.
Insamling av relevanta data för test och demonstration.
Utvärdering.
Avrapportering.
Demonstration.