Ubikvitära omgivningar

Kandidatavhandling i datateknik
Åbo Akademi
Fakulteten för naturvetenskaper och teknik

Michael Wessman
Handledare: Johan Lilius

6.4.2016

Referat

Ubikvitära system sägs vara den tredje vågen inom datoranvänding, där första vågen var stordatorer, och andra vågen som vi nu befinner oss i är persondatorer. Vad ubik teknik försöker genomföra är ett sätt att placera datorerna i bakgrunden av våra liv, så att människor kan fokusera på uppgiften som ska göras, och inte behöva oroa sig över de verktyg som ska användas. Denna avhandling presenterar hur vi kan tillämpa ubik teknik i arbetsvärlden, specifikt kontorsmiljön, för att öka bekvämligheten för de anställda och sänka energikostnader, med hoppet att det ökar produktiviten.

Nyckelord: Ubikvitär, Smart kontor, Intelligent miljö, Sensorer

Innehåll

1 Inledning

I September 1991 skrev Mark Weiser en artikel om datorernas framtid. Enligt Weiser så kommer persondatorerna som vi använder i dagens värld att försvinna och smälta in i bakgrunden av våra liv. Små mikrodatorer kommer implementeras i vanliga hushållsapparater och maskiner, som sedan sammankopplas i ett nätverk. Weiser valde att kalla dessa datorer *ubikvitära* (eng. *ubiquitous*) [1].

För 25 år sedan när Weiser skrev artikeln så hade man inte teknologin att förverkliga hans teorier om osynliga datorer. Inom de senaste åren har mikrodatorer däremot blivit tillräckligt snabba att effektivt kunna användas för att skapa ett ubikt nätverk. Idag har vi redan mikrodatorer inbyggda i termostater och strömbrytare, m.m. Men vad vi inte har är ett nätverk till vilket alla apparater i en byggnad sammankopplas för att skapa en smart, omgivande och energieffektiv miljö.

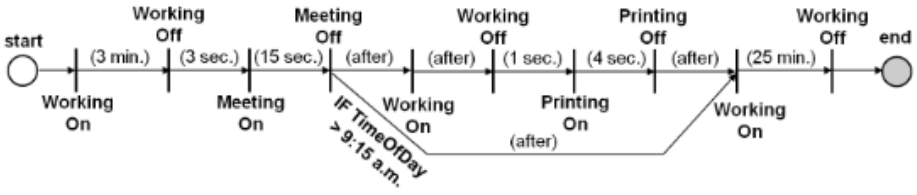
I dagens kontor finns redan många automatiserade apparater, t.ex. lampor som släcker av sig själva när inga rörelser sker i området, eller termostater som håller en bestämd temperatur i rummet. Ett problem är ändå att apparaterna inte anpassar sig till omgivningen eller människors preferenser. Med hjälp av ubikvitär teknik kan man skapa en intelligent miljö som anpassas enligt information som samlas upp av sensorer.

2 Intelligent miljö

Intelligenta miljöer (eng. *intelligent environment*) är omgivningar som använder sig av olika sensorer, både analoga och digitala, för att analysera omgivningen, spara informationen och anpassa sig till behoven som uppstår. En av de vanligaste sensorerna som används i kontors-experiment är visuella sensorer, d.v.s. kameror [2].

2.1 Visuella sensorer

Med visuella sensorer kan man mäta flera variabler som läge och tillstånd personerna i omgivningen befinner sig i. Med hjälp av kameror och en databas kan man skapa en *handlingskarta* (eng. *action map*) som analyserar en persons vanliga beteende, och kan sedan hjälpa personerna med påminnelser om glömda uppgifter, eller föreslå pauser om man arbetat för länge [3]. En handlingskarta som kan ses i figur 1 fungerar effektivt eftersom människor har tendens att utföra sitt arbete på basis av vanor. Så när det intelligenta systemet lärt sig vilken tid man kommer på jobb, när och hur länge man tar kaffepauser, kan systemet aktivt hjälpa till med att släcka lamporna, lägga datorn i sovtillstånd och låsa dörren till rummet. För att skapa handlingskartorna behöver man ett inlärnings-system som samlar information från sensorerna om individernas



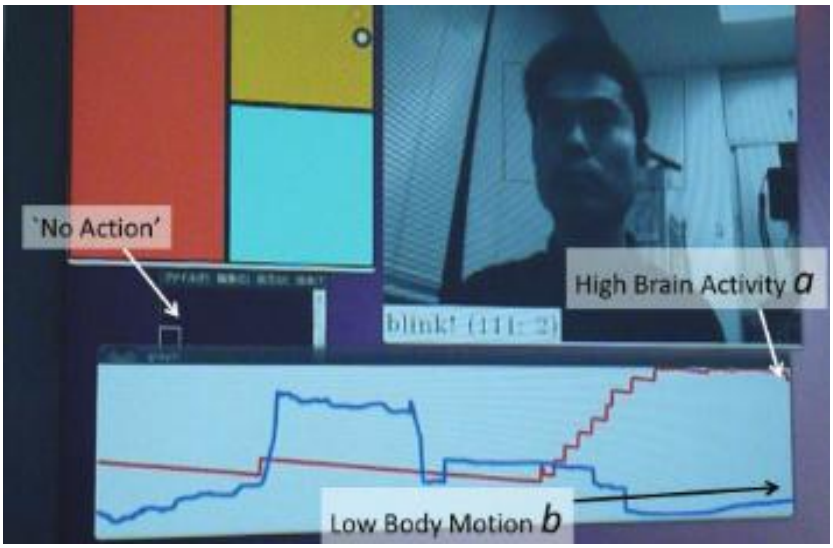
Figur 1 - Visualisering av en handlingskarta för en person [3].

positioner inom byggnaden. Detta forutsätter att en viss position sammankopplas till en viss aktivitet, t.ex. att befinna sig i kafferummet räknas som vilopaus. Det krävs också ett ansiktsigenkänningssystem så att man kan skilja de anställda i byggnaden från varandra. När systemet samlat tillräckligt information om omgivningen används en inlärnings-algoritm för att analysera vanliga beteenden av individerna. Algoritmen identifierar flera variabler, som hur länge en specifik handling tar för en viss person, och vilka handlingar som brukar ske direkt efter varann.

Visuella sensorer är bara en av många informationskällor inom ett ubikt nätverk, vilket betyder att informationen som samlas visuellt måste kunna integreras med de andra sensorerna i algoritmen. Det betyder inte endast att information från olika källor måste kunna beräknas av samma algoritm, utan även att de kan kombineras för att skapa noggrannare förutsägelser av användarna [4].

2.1.1 Förbättring av livskvaliteten

Visuella sensorer används inte endast för att öka produktiviteten eller sänka energikostnaderna. I Japan har man experimenterat med att öka livskvaliteten för människor som arbetar på kontor. Vad de skapat är en s.k. smart kontorstol som reagerar på varierande sätt, beroende på informationen som den visuella sensorn samlar upp från människors ansikten. Denna smarta kontorstol har döpts till Owens Luis, ett namn som uttalat i japanska betyder "en uppmuntrande stol" [5][6]. Owens Luis-systemet beräknar trötttheten och koncentrationen av sina användare med att analysera rörelser och ansiktsuttryck.



Figur 2 - kamera som analyserar rastlöshet samt hjärnaktivitet [4].

I figur 2 ser man hur systemet analyserar koncentrationen hos individer, där rörelser beräknar rastlöshet och längden samt frekvensen av blinkande beräknar hjärnaktivitet. Owens Luis-stolen reagerar sedan beroende på situationen; om hjärnaktiviteten samt rörelsefrekvensen är låga så gungas stolen för att väcka personen, och om hjärnaktiviteten samt rörelsen är hög så lutas stolen bakåt för att försöka få personen att fokusera sig på sitt arbete.

Det finns också flera andra apparater förutom Owens Luis stolen som används för att öka livskvaliteten i kontor. Kraftiga LED-lampor med varierande färgtemperaturer används för att väcka de anställda. Högtalare används också för att spela varierande bakgrundsmusik beroende på skicket av människorna i kontoret. Dessutom har man arom-generatorer som släpper ut olika dofter, som t.ex. kaffe ifall någon visar sig vara trött. Detta är bara ett antal exempel på de många varierande apparater som kan kopplas till ett ubikt nätverk för att skapa upplevelsen av en äkta intelligent miljö.

2.1.2 Visuell analys för distansmöten

Möten är en viktig del av varje företags verksamhet, och i dagens läge hålls många möten på distans genom audiovisuella program. Eftersom mötesdeltagarna inte är i samma rum så finns det många naturliga interaktioner som man kan gå miste om. Ansiktsuttryck och kroppsspråk berättar mycket om personers fysiska tillstånd och därför är det viktigt att analysera dem så att inga missförstånd sker.

I ett experiment har man testat en algoritm som läser av ansiktet på personen som deltar i mötet på distans i realtid och delar informationen med resten av deltagarna [7]. Blicken är huvudsakligt fokus för uppmärksamhet och huvudspårning används för att upptäcka sociala signaler som nickningar eller leenden. Problem uppstår fortfarande i kodsystem för ansiktsuttryck p.g.a. olikheter i personers utseende och subtila uttryck. Det är därför man också följer kropps-ställningar. På samma sätt som man spårar huvudet så följer man kroppsspråket, där olika ställningar genererar ett visst meddelande. Till exempel när någon sitter rak i ryggen så räknas det som hög uppmärksamhet.

Förutom visuella signaler så kan fokus för uppmärksamhets-systemet också upptäcka icke-verbala ljud. Gäspningar och suckar är viktiga icke-verbala ljud att upptäcka, men systemet fokuserar också på tonhöjden och energin av personers tal. Med hjälp av detta kan man hitta de personer som visar dominans och ledarskap under möten. Eftersom tekniken för att upptäcka människors aktivitet under möten inte är viktig, så har det inte skett mycket forskning gällande ämnet. När algoritmer eventuellt blir bättre på att upptäcka ansiktsuttryck, så kommer forska mera om hur information från kameror kan till tillämpas.

2.2 Optiska sensorer

Inom de senaste åren har de flesta företag arbetat hårt för att motverka energikrisen med att skapa en grön och hållbar utveckling. Inom industrier finns det många olika sätt att minska användningen av energi, men på kontor finns det inte mycket som kan ändras förutom ljus, värme och användning av apparater. Detta har potential att kosta en hel del arbetstid ifall de anställda måste tänka på omgivningen och ändra sina arbetsvanor p.g.a. det.

Med smarta kontorssystem kan man skapa en energieffektiv omgivning som håller produktiviteten och de anställdas bekvämlighet uppe. För att förverkliga denna miljö så krävs ett inbyggt automationssystem med sensorerna kopplade till det. Ljus anses vara en av de viktigaste variablerna när det gäller energisparande inom intelligenta omgivningar. Med hjälp av ljussensorer kan man optimera användningen av ljus, t.ex. att ha lamporna lågt på om det är tillräckligt ljust ute, eller att dra för gardinerna ifall det är för ljust ute [8]. Lamporna aktiveras sedan automatiskt beroende på vem som anlänt till byggnaden. Med hjälp av visuell eller RFID-identifieringssystem, vet systemet exakt vem som anlänt till byggnaden och kan sedan tända lamporna i personens kontor till den ljusstyrkan som föredras.

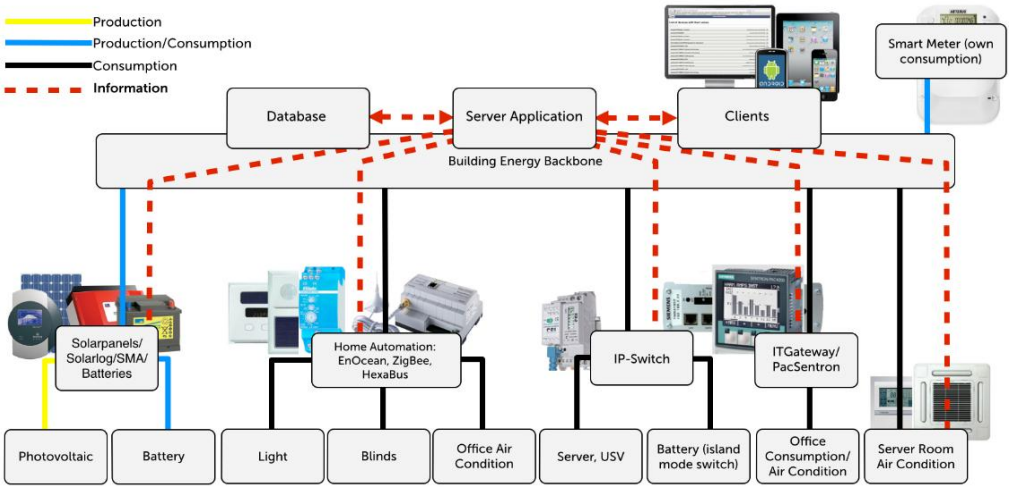
Som det nämndes i föregående kapitel så anpassar sig dessa system också till användarnas preferenser för bekvämlighetens skull. Ifall systemet gör något fel så kan användarna manuellt ändra ljusstyrkan i kontoret. Denna ändring sparas i systemets databas så att man får exakt information om vem som ändrade ljusstyrkan, och till vilket värde. Förutom energioptimering av lampor kan man också använda sensorer för

ventilering och värme. Med en koncentrationsmätare för koldioxid kan man automatisera ventileringen att aktiveras när koldioxidmängden når en viss punkt. Värme fungerar med en termometer som har en låg- och högpunkt. När temperaturen i kontoret når lågpunkten aktiverar man värme, och när det når högpunkten så stängs det av. När det är mellan båda punkterna så försöker systemet hålla temperaturen till användarnas föredragna temperatur. Lågpunkten och högpunkten är också relativa beroende på användarnas preferenser.

2.3 Intelligent elnät

Den tekniska framgången av förnybar energi ger möjligheten åt vanligt folk att generera sin egen rena energi. Med ett *intelligent elnät* (eng. *smart grid*) som använder sig av solpaneler kan man skapa ett lokalt kraftverk som genererar energi till en intelligent byggnad.

Eftersom man genererar sin egen energi så måste man vara medveten om hur mycket energi behövs och vart det används. Med en prognosalgoritm för elkonsumtion kan man bestämma när toppvärden för konsumtion nås under arbetsdagarna. Algoritmen kan också bestämma hur länge den laddar bärbara datorer och mobiltelefoner så att onödig laddning på fulla batterin inte sker. Med hjälp av ett batteri kan man spara energi ifall det är dåligt väder och solpanelerna inte får tillräckligt ljus, eller om överkonsumtion sker under en lång dag. Om batterierna är fullt laddade och inte används så kan överskottsenergin t.ex. gå till att ventilera serverrummen mera än normalt, eller skickas ut till samhället för extra ekonomisk vinst. Varje apparat i nätverket får sin egen etikett som beskriver mängden av energi som krävs för apparaten att uppehållas utan att problem uppstår.



Figur 3 - En översikt över ett nätverk som använder intelligent elnät [9].

Bordsdatorer behöver t.ex. energi dagen runt under arbetstider, medan kylskåp kan hålla sin bestämda temperatur med 15 minuter energi per timme. I figur 3 har vi en översikt över hur sensorerna, servern, databasen och apparaterna kopplas till ett nätverk, samt hur produktionen och konsumtionen av energi används inom byggnaden. Systemet fungerar i realtid och kan anpassa sig omedelbart till ändringar från alla apparater i nätverket.

All data från sensorerna används i realtid men sparas också i databasen, så att det kan hämtas och användas vid behov. Server applikationen har information om användarna i byggnaden; vem de är, vart deras kontor är, m.m. och information om apparaterna och vart de befinner sig i byggnaden. Smarta mätaren är instrumentet som mäter produktionen och konsumtionen av energi, och kommunicerar sedan med energimätnings företag för bokföring. Mätaren gör det också möjligt att bestämma när det behövs extern-energi ifall konsumtionen är högre än produktionen. En skedulerare används för att hämta energi-priser

periodiskt för att köpa den billigaste energin ifall behovet uppstår. Sedan har man en koordinator som sammankopplar alla ovannämnda apparater så att de kan lättare kommunicera med varandra och dela information [9][10].

3 Platsbaserad teknik

För att en omgivning ska kunna definieras som en intelligent miljö måste den ha verktygen att anskaffa kontextuell information. I föregående kapitel diskuterades det hur man samlar information med hjälp av olika sensorer, men i detta kapitel diskuteras olika sätt att samla information om användarnas och objektens positioner. Jämfört med sensorer har användningen av platsbaserad teknik en väldigt låg kostnad. GPS är den populäraste tekniken för lokalisering, men eftersom det inte fungerar effektivt inomhus och har väldigt låg noggrannhet så måste man använda sig av andra system för kontor. Metoderna som vanligen används för att spåra positioner är *RFID* (eng. *Radio-frequency identification*) och Wi-Fi-signaler från telefoner.

3.1 RFID

RFID användes ursprungligen för identifikation av objekt inom logistik-branschen, men nyligen har man tagit denna teknik och applicerat den på lokalisering av människor och objekt. Det finns två olika RFID-tekniker: passiv RFID som inte har någon intern strömkälla och får sin energi elektromagnetiskt från RFID-läsaren, och aktiv RFID som oftast är batteridriven och utsänder sin egen signal som en radiofyr. Lägger man

aktiva RFID-märken i taket och passiva märken i golvet så får man bestämda koordinater för omgivningen.

RFID-märken för personer kan ta formen av små chipp och kan användas som nyckelringar eller ID-kort. Informationen man samlar från individers positioner kan användas för många ändamål. Systemet har enkla funktioner som redan nämnts i kapitel 2.1 som att öppna dörrar eller tända lampor när personen är i närheten. I byggnader med hög säkerhet kan man lättare auktorisera de anställda i högre positioner utan att de måste autentisera sig själva konstant. Detta kan spara en stor del tid och pengar ifall man inte behöver använda sig av fingeravtrycksläsare eller pinkoder längre; istället krävs det endast att RFID-märket är med personen. Man kan dessutom använda RFID för att bevisa att man varit närvarande i olika situationer som möten och seminarier.

Det är inte bara människor som kan spåras med hjälp av RFID. Positionen av olika objekt och apparater i en byggnad spelar en stor roll, inte endast av säkerhetsskäl, utan också för skilja individuella apparater. I ett kontor kan man t.ex. ha flera bärbara datorer av exakt samma modell, och med hjälp av RFID-märkning kan man lätt identifiera vilken dator som hör till vilken användare [11].
[TO-DO]

4 Säkerhet och integritetsskydd

Eftersom ubikvitära system baserar sig på att koppla flera apparater till samma nätverk uppstår det flera säkerhetsproblem, t.ex. vilka användare som har tillgång till vilka apparater och hur man kan skydda nätverket från externa hot. Förutom problem med säkerhet uppstår det också problem med personlig integritet. Sensorer som följer användarna visuellt och genom olika platsbaserade tekniker via telefoner och ID-brickor väcker oro hos många. Att ha ett nätverkssystem som följer upp och sparar information om användaren konstant kan leda till att de anställda känner sig obekväma. Detta kan påverka arbetsmotivationen negativt för många, vilket sedan direkt påverkar produktiviteten.

I detta kapitel diskuteras olika lösningar för att skydda användarna från interna och externa störningar, samt att vänja de anställda till den nya omgivande tekniken.

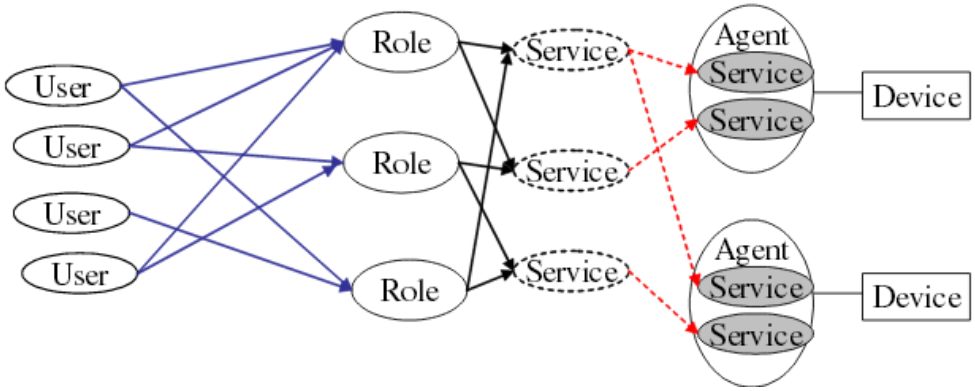
4.1 Säkerhet

När man börjar koppla apparater till nätverk som inte tidigare använts i sådana sammanhang uppstår det nya säkerhetsrisker. Apparater som t.ex. mikrovågsugnar och kylskåp kan vara väldigt lätta att manipulera och förorsaka skador om inte ett ordentligt säkerhetssystem existerar. Oönskade ändringar kan förekomma både internt och externt i ett nätverk, av antingen en verifierad användare, eller en utomstående individ. Därför är det viktigt att skapa ett säkerhetssystem som noggrant kan autentisera och auktorisera användaren [12].

4.1.1 Intern säkerhet

Intern säkerhet på ett smart kontor hanterar relationen mellan användarna och apparaterna, samt ändringar i omgivningen och gruppen av användare. Många problem uppstår inom ett smart kontor eftersom det måste vara både lätt tillgängligt att använda tjänsterna och samtidigt säkert. Autentisering är viktigt så att systemet vet vilken person som loggat in i nätverket. Systemet måste också vara öppet för gäster så att de får tillgång till en bestämd del apparater, men alla gäster som kopplas till nätverket är inte pålitliga. Miljön och användarna i systemet ändras regelbundet; användaren kan ta apparater som bärbara datorer med sig hem, eller så har företaget köpt nya surfplattor till de anställda. Detta kräver att nätverket måste fungera dynamiskt och anpassa sig till ändringar så snabbt som möjligt så att säkerhetsbrister inte uppstår.

Användarna kan inte kommunicera med apparaterna direkt, utan de måste gå genom agenter. Agenter fungerar som förmedlare mellan användare och apparater, så att det räknas som en tjänst från agenter när man använder sig av apparater. Med hjälp av agenter kan man dessutom kombinera flera tjänster så att användarna inte behöver göra alla begäranden separat. Till exempel om en användare skriver ut ett dokument kan agenten skicka pappret direkt till användaren via ett internt transportsystem, istället för att användaren själv måste begära transporten. Naturligtvis kräver detta kommunikation mellan alla agenter, så att varje agent måste ha information om alla andra agenter och vilka tjänster de erbjuder. I figur 4 har man en översikt över ett system och vilka steg användarna måste ta för att få tillgång till apparaterna.



Figur 4 - Visualisering över en rollbaserad tillgångskontroll [11].

Roller för användaren bestäms med hjälp av autentisering. Varje användare i omgivningen är given en roll, och varje roll har abstrakta tjänster. Det är dessa abstrakta tjänster som sedan bestämmer vilken agent som passar bäst till användarens begäran [12].

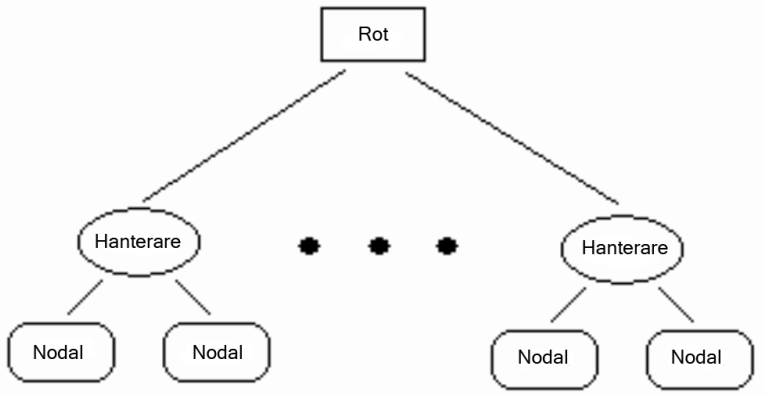
Ett rollbaserat tillgångskontrollsystem kan göra användningen av apparater krångligare för användare i omgivningen, men detta faktum gäller alla former av säkerhet. Säkerheten blir ännu mer komplicerad när man måste ta hänsyn till externa hot.

4.1.2 Extern säkerhet

Ubikvitära nätverk har många olika former av apparater kopplade till sig, och p.g.a. detta får man en väldigt heterogen omgivning. Eftersom systemet är så heterogent uppstår det nya utmaningar som kräver uppdaterade säkerhetsparadigmer [13].

Med vanliga datorer och nätverk har man fortfarande många säkerhetsbrister, och nu behövs det ett säkerhetssystem som kan opereras inom ett dynamiskt nätverk. Säkerhetssystemen för nätverk som används idag fungerar delvis på ubikvitära nätverk, men de kan bara skydda

systemet från enkla brytningar. Med hjälp av en detektor för nätverks-anomalier kan man identifiera ändringar över flera noder inom nätverket. Ifall det sker ändringar i noderna utan att detektorn är medveten om det, så flaggas det som ett möjligt anfall eller sabotageprogram.



Figur 5 - Nätverkstopologin för säkerhetssystemet [13].

Arkitekturen för extern säkerhet har liknande egenskaper som nämndes ovan i den interna säkerheten. I figur 5 ser man säkerhets-systemet som använder sig av tre olika agenter hierarkiskt: Nodal-, hanterings- och rotagenter. Nodalagenter är på den lägsta nivån av hierarkin, alltså de mest allmänna av agenterna. Varje nod i systemet är kopplad till en nodalagent. Nodalagentens huvudsakliga uppgift är att kontrollera den lokala säkerheten i nätverket, så att ingen manipulering sker på individuella noder. Ifall säkerheten bryts i en nod så anmäler nodalagenten det direkt till sin hanterare och försöker sedan motarbeta brytningen. Om mot-arbetningen misslyckas så måste nodalen avlägsna noden ur nätverket.

Hanteringsagentens uppgift är att kontrollera säkerheten av sina nodala agenter och de andra hanteringsagenter i nätverket. När en nodalagent anmäler sin hanteringsagent att en brytning har skett, så

kontrolleras det om andra hanteringsagenter fått liknande anmälningar. Detta görs för att verifiera att det inte är ett fördelat anfall. Ifall brytningen är enskild så kan hanteringsagenten hjälpa nodalagenten med att motarbeta brytningen, eller så kan hanteringsagenten omdirigera nätverkstrafiken för att minimera risken att brytningen sprider sig. Varje hanteringsagent måste rapportera till rotagenten.

Rotagentens huvudsakliga uppgift är att kontrollera alla andra agenter i nätverket, och vid behov tilldela uppgifter till agenterna. Rotagenten styrs oftast av en person, eftersom informationen den mottar från sina agenter kan vara nyttig för administratörn av systemet. Stark säkerhet är alltså väsentligt för rotagenten, och användingen av rotagenten kräver hård autentisering.

Med detta säkerhetssystem har man ett nätverk som fungerar på en abstrakt nivå, där det inte finns några statiska noder, med undantag av rotnoder. Detta är idealt för ett ubikvitärt system i vilket apparater läggs in och tas bort dagligen. Så länge apparaterna går genom säkerhets-analysen och uppdateras regelbundet har de tillstånd att använda nätverkets resurser. Följer man dessa säkerhetskontroller så garanteras det ett skyddat nätverk där inga brytningar utifrån förekommer [14].

4.1 Integritetsskydd

Inom de senaste åren har det varit mycket diskussion om olika staters informationsspårning runt omkring i världen. Människor har blivit mer medvetna om hur viktig deras personliga information är, och p.g.a. detta är det viktigt att ta hänsyn till människors ovilja att bli konstant spårade i en intelligent miljö.

Villigheten att dela information varierar mellan olika användargrupper; ålder, utbildning, kultur, m.m. spelar alla en roll för vad och hur mycket de vill dela med sig. Ifall man ska implementera ett *kontextmedvetet system* (eng. *context-aware system*) som är beroende av användarinformation, så måste användarna vara beredda på att spåras. Spårning i intelligenta miljöer skiljer sig från spårningen i dagens läge. När man sitter vid datorn på kontoret kan internetsökningar och programanvändning spåras, men direkt när man stiger upp och lämnar datorn så spåras man inte längre. I en intelligent omgivning så spåras man konstant, oberoende var man befinner sig eller vad man arbetar på. För att få det nya systemet använt till sin fulla potential måste man vara medveten om användarnas bekymmer över insamlingen av information. Därför ska det identifieras vilka typer av kontextinformation användarna är villiga att dela med sig, och hur mycket kontroll användarna vill ha över den information som samlas.

För att en kontextmedveten miljö ska fungera optimalt krävs det en viss mängd information av användarna. Identitetsinformation behövs för att kunna identifiera vem användaren faktiskt är. Platsinformation används för att identifiera var användaren befinner sig. Aktivitetsinformation kontrollerar användarens nuvarande och tidigare uppgifter, samt olika projekt användaren är en del av. Tillgänglighetsinformation kontrollerar ifall användaren är upptagen. Biometrisk information identifierar användarnas välmående, t.ex. deras humör eller stressnivåer. Personliga preferenser är informationen som sparats över användarens specifika preferenser i arbetsmiljön, t.ex. föredragen rumstemperatur och ljusstyrka. Agendainformation samlas från användarens kalender så att aktiviter och möten kan förberedas.

Medan det finns många olika former av information som samlas av användarna, så finns det enbart två olika sätt att samla dem. Att fånga information automatiskt är den vanliga formen av datafångst i en intelligent omgivning. Det betyder att information samlas kontinuerligt utanför användarens kontroll. Ifall användaren inte vill bli kontinuerligt spårad kan den använda individuell kontroll. Med hjälp av detta har användaren mer kontroll över vad som sparas i systemet, men det kräver sedan mera arbete att kontinuerligt bestämma vad som sparas och vad som inte sparas.

En undersökning har gjorts där man skickat ett frågeformulär åt olika företag i Tyskland och USA [15]. Man har listat olika informations-typer och låtit informanterna betygsätta hur bekväma de skulle vara med dessa spårningar. En skala från 0 till 10 valdes, där 0 betyder att man inte alls är villig att ge denna information, och 10 är att man ger informationen utan tvivel. Automatisk och manuell kontroll över data som samlas är delade i två olika delar i denna undersökning. I tabell 1 ser man direkt skillnaden mellan automatisk och manuell datafångst, och hur stor påverkan det har på användarnas villighet att ge ut sin information i alla kategorier. Att verifiera sin identitet för systemet är den mest acceptabla formen av spårning för användare, medan de inte vill ge information om deras fysiologiska tillstånd och nuvarande uppgift.

Resultaten varierade mycket mellan olika personer i undersökningen, och faktorer som nationalitet samt datorkunskap hade den största påverkan på villighet av datafångst. De personer som besvarade formulären i Tyskland var i medeltal mindre villiga att dela med sig information än de i USA. Detta kan bero på kulturella skillnader, och att tyskar var mera medvetna om hur farligt missbruk av personliga

data kan vara. Det visar sig också att de personer som säger sig vara kunniga med datorer är mera villiga att ge sin information i alla kategorier.

Informationstyp	**Automatiskt**	**Manuellt**
1. Identitetsinformation	4,86	7,59
2. Platsinformation	3,35	6,93
3. Aktivitetsinformation	2,73	6,32
4. Tillgänglighetsinformation	3,94	7,53
5. Biometrisk information	2,06	3,47
6. Personliga preferenser	3,85	6,02
7. Agendainformation	3,66	6,92
Genomsnitt	**3,49**	**6,40**

Tabell 1 - Användarnas villighet att dela information [14].

Innan man börjar standardisera intelligenta omgivningar i kontor så måste man ta hänsyn till de anställdas åsikter. Med hjälp av denna undersökning kan man komma till slutsatsen att automatiskt fångande av data utan användarnas samtycke är hänsynslöst. Det krävs att kontroll över data som fångas borde ges till användarna, inte till de som styr systemet.

5 Sammanfattning

Det finns ingen bestämd definition för vad ett smart kontor innefattar, men de olika tekniker som presenterades i denna avhandling ger en överblick av de instrument som kan användas för att skapa en kontext-medveten intelligent miljö. När man sedan kombinerat flera olika former av sensorer och skapat ett heterogent nätverk, så närmar man sig det ubikvitära systemet som Mark Weiser föreställde sig för 25 år sedan.

Det har experimenterats och forskats mycket i ubikvitär teknik inom olika omgivningar som hus, industrier och kontor, men fortfarande har man inte nått dess fulla potential. Tills alla persondatorer försvinner och datorerna blir osynliga i bakgrunden av våra liv, så finns det utrymme för innovation och förbättring av ubikvitär teknik.

Källförteckning

[1] Weiser, M. Sep 1991: *The Computer for the 21st Century*, www.ubiq.com/hypertext/weiser/SciAmDraft3.html [17.2.2016]

[2] Diane J Cook, Juan C Augusto, Vikramaditya R Jakkula 31.8.2009: *Ambient intelligence: Technologies, applications, and opportunities*. Pervasive and Mobile Computing, sidor 277-298, ISSN 1574-1192.

[3] Chen Chih-Wei, Aztiria Asier, Aghajan, Hamid, 20.6.2011: *Learning human behaviour patterns in work environments*. Computer Vision and Pattern Recognition Workshops 2011 IEEE Computer Society Conference, sidor 47-52, ISSN 2160-7508.

[4] Asier Aztiria, m.fl. Jan 2012: *Discovering frequent user-environment interactions in intelligent environments.* Personal and Ubiquitous Computing, sidor 91-103, ISSN 1617-4917

[5] Kiyoshi Kiyokawa, m.fl. 4.3.2012: *Owens Luis — A context-aware multi-modal smart office chair in an ambient environment*. Virtual Reality Short Papers and Posters 2012 IEEE, ISSN 1087-8270.

[6] Hironori Shigeta, m.fl. 4.3.2012: *Implementation of a smart office system in an ambient environment.* Virtual Reality Short Papers and Posters 2012 IEEE, ISSN 1087-8270.

[7] M. Poel, R. Poppe, A. Nijholt, 17.9.2008: *Meeting behavior detection in smart environments: Nonverbal cues that help to obtain natural interaction*. Automatic Face & Gesture Recognition, 2008.

[8] Hang Li, 16.9.2014: *A novel design for a comprehensive smart automation system for the office environment.* Emerging Technology and Factory Automation 2014, ISSN 1946-0740.

[9] Cristina Rottondi, m.fl. 9.3.2015: *An energy management system for a smart office environment*. International Conference and Workshops on Networked Systems, 2015.

[10] Ilche Georgievski, m.fl. 10.12.2012: *Optimizing Energy Costs for Offices Connected to the Smart Grid.* IEEE Transactions on Smart Grid (Volym: 3 Utsläpp: 4), sidor 2273-2285, ISSN 1949-3053.

[11] Jan Koch, m.fl. 17.9.2007: *Indoor Localisation of Humans, Objects, and mobile Robots with RFID Infrastructure*. Seventh International Conference on Hybrid Intelligent Systems, 2007, sidor 271-276, ISBN 978-0-7695-2946-2.

[12] Wataru Yamazaki, Fumio Mizoguchi, 25.6.2003: *Design and Implementation of Access Control System for Smart Office Environment.* Software Security — Theories and Systems (Volym 2609), sidor 249-262, ISSN 0302-9743.

[13] Jun Wang, m.fl. 2005: *Secure Smart Environments: Security Requirements, Challenges and Experiences in Pervasive Computing.* Center for Computing Science University of Illinois at Urbana-Champaign.

[14] C. V. Dyke, C. K. Koc, 27.1.2003: *On ubiquitous network security and anomaly detection.* Applications and the Internet Workshops, 2003, sidor 374-378, ISBN 0-7695-1873-7.

[15] Carsten Röcker, 23.3.2010: *Information Privacy in Smart Office Environments: A Cross-Cultural Study Analyzing the Willingness of Users to Share Context Information.* Computational Science and Its Applications – ICCSA 2010, sidor 93-106, ISSN 0302-9743.