FFI-rapport 2012/02009

Eksperimenter med trådløst sensornettverk for perimetersikring og akseovervåkning

Joakim Flathagen, Terje M. Mjelde, Reinert Korsnes, Vinh Pham og Jostein Sander

Forsvarets forskningsinstitutt (FFI)

24. januar 2013

FFI-rapport 2012/02009

1141

P: ISBN 978-82-464-2187-2
E: ISBN 978-82-464-2188-9

Emneord

Sensorer

Sensornettverk

Perimetersikring

Styrkebeskyttelse

Detektorer

Godkjent av

Torunn Øvreås	Prosjektleder
Anders Eggen	Avdelingssjef

Sammendrag

Hensikten med CD&E aktiviteten «EP1257 Trådløst sensornettverk» har vært å bidra til å kartlegge hvilken operativ nytteverdi et trådløst sensornettverk vil kunne gi på taktisk nivå. CDE-aktiviteten har overlappet med avslutningen på prosjekt 1141 «Situational Awareness Sensor System (SASS)» og har benyttet det trådløse sensorsystemet som ble utviklet i dette prosjektet. Det trådløse sensorsystemet bestod av 50 noder utstyrt med Passiv Infrarød Sensor (PIR), akustisk sensor og radar. I tillegg er det uttestet et kommersielt system, Flexnet, fra Exensor.

De trådløse sensorsystemene er uttestet i et scenario for perimetersikring og et scenario for akse-overvåkning. FFI vurderer aktiviteten som meget vellykket. SASS-systemet har vist seg både robust og stabilt innenfor de kravene som stilles til testutstyr av denne typen. Resultatene viser at et trådløst sensornettverk kan gi tidligere deteksjon av mulige inntrengere, hurtigere reaksjon-svevne og utvidet perimetersikring. Vi har erfart at utstyret er enkelt å deployere og har kort opplæringstid. Det er grunn til å anta at elektroniske sensorer vil kunne redusere personellbruk og belastningen et tradisjonelt vakthold medfører.

English summary

The purpose of the Concept, Development & Experimentation (CDE) project «EP1257 Trådløst sensornettverk (Wireless Sensor Network)» has been to study the operational effect of a Wireless Sensor Network in a tactical setting.

The activity has been conducted alongside with the project «1141 - Situational Awareness Sensor System (SASS)» and has taken advantage of the wireless sensing nodes developed in this project. The wireless sensor system used in the experiments consisted of 50 nodes equipped with Infrared sensor, an acoustic sensor and doppler radar. In addition to this system, a commercial system, Flexnet developed by Exensor, was used.

The wireless sensor systems were used in two scenarios: Perimeter surveillance and road surveillance. The results from the experiments show that the SASS-system was very robust and stable considering that the system is on a very early prototypical stage. The operational results show that a wireless sensor network can provide early detection of adversaries, improve the chain of reaction, and provide improved perimeter security. Our experiences conclude that the system is easy to deploy and simple to use. Further, it is reason to believe that electronic sensors can reduce the workload compared to using traditional observation soldiers.

Innhold

1 Innledning

1.1 Bakgrunn

I et overvåknings- og sikringsscenario er mennesket som kombinert sensor og beslutningstaker ikke optimal ved alle forhold. Anskaffelse av elektroniske hjelpemidler vil kunne gi tidligere deteksjon av en mulig inntrenger, hurtigere reaksjonsevne og utvidet perimetersikring. Elektronisk utstyr vil også kunne redusere personellbruk og belastningen et tradisjonelt vakthold medfører.

Å benytte trådløse sensorer for taktiske formål er en over femti år gammel ide som først ble realisert med «Air Delivered Seismic Intrusion Detector (ADSID)» av US Air Force under Vietnamkrigen på slutten av sekstitallet. Siden den tid har en rekke trådløse sensorsystemer blitt konstruert og uttestet av de fleste nasjoner. Parallelt med økt militær bruk har den sivile utviklingen innen mikroelektronikk og trådløs teknologi muliggjort stadig rimeligere og mer energieffektive sensorsystemer. Det er et markant skille mellom de første enkle systemene og dagens systemer. De tidlige systemene bestod av teknisk enkle sensornoder uten særlig prosesseringskapasitet. De var gjerne store og opererte uavhengig av hverandre og sendte ufiltrerte sensormålinger direkte inn til en basestasjon. Nye systemer er derimot basert på *multihopp nettverksteknologi* inspirert av pakkerutingen i Internett. Dette muliggjør stor redundans og automatisk feilkorrigering. Videre vil sensornodene kunne samarbeide under deteksjon slik at sannsynligheten for falske alarmer kan minimeres. Minimal størrelse på hver enkelt node og lave kostnader muliggjør systemer med et stort antall noder, men som likevel er enkle å deployere.

1.2 Motivasjon

Elektronisk overvåkning av en leirs perimeter er et effektivt hjelpemiddel for å oppdage og varsle om fiendtlig aktivitet i leirens nærområde. Ved bruk av ulike sensorer og detektorer ønsker man å oppnå raskere og sikrere varsling enn hva som er mulig ved bruk av vaktstyrker og observasjonsposter. Ved at mottiltak kan iverksettes i tide økes styrkebeskyttelsen.

Ulike sensorsystemer gir forskjellig grad av nøyaktighet i varsling og klassifikasjon. Valg av sensortyper vil typisk avhenge av en rekke forhold som for eksempel størrelse og varighet på leiren som skal beskyttes, forventet trussel, geografi og værforhold. Mastmonterte sensorer for eksempel, er mest egnet for langdistanse observasjon av store områder utenfor leir/posisjon, i prinsippet alt terreng innenfor fri sikt fra leiren. Gjerdemonterte perimetersensorer benyttes til overvåkning av et gjerde eller barriere. Både mast- og gjerdemonterte sensorer er tilpasset langvarige leiroperasjoner, og er lite hensiktsmessige i små hurtigforflyttende operasjoner. Til dette trengs et mer fleksibelt og lettere system. Innen denne kategorien finnes kommersielle produkter som markedsføres som «Unattended Ground Sensors (UGS)». Disse sensorpakkene består gjerne av et antall detektorer (noder) som plasseres slik at de dekker et større areal. Sensornodene kommuniserer trådløst inn til en basestasjon. Eksempler på nyere systemer er «Terrain Commander 2» fra Textron Systems (USA) og systemene «UMRA» og «Flexnet» fra Exensor Technology AB (Sverige)[3]. Disse

systemene er i dag forholdsvis kostbare, men en kraftig prisreduksjon kan forventes etter hvert som systemene blir mer utbredte og teknologien mer moden. For en utfyllende beskrivelse av ulike aktuelle sensorteknologier henvises til [2].

1.3 Oppdrag

Mandatet for det CD&E oppdraget som er beskrevet i denne rapporten har vært å studere muligheter med trådløs sensorteknologi for taktiske formål. Uttestingen og eksperimenteringen har hatt to hovedformål:

1. Å undersøke den operative effekten ved bruk av eksisterende trådløse sensorsystemer (state-of-the-art). Hva er mulig i dag?
2. Studere nye teknologier og derav finne mulighetsrommet for fremtidige trådløse sensorsystemer. Hva er mulig på sikt?

For å understøtte dette har vi under vår uttesting benyttet to ulike utstyrssett. Det ene er Flexnet fra Exensor, som vi betegner som det mest fremtidsrettede og komplette UGS systemet i dag. Det andre systemet består av 50 sensornoder som er utviklet og konstruert av FFI. Det FFI-konstruerte systemet gir helt andre muligheter for å studere spesifikke teknologier enn hva som er mulig i et lukket og ferdig kommersielt system, og har vært uvurderlig for å kunne fastslå både muligheter og problemområder, samt å skissere anbefalinger. CD&E forsøkene som beskrives i denne rapporten er basert på scenarier innen perimetersikring og akseovervåkning fra prosjektets scenarioarbeid [9].

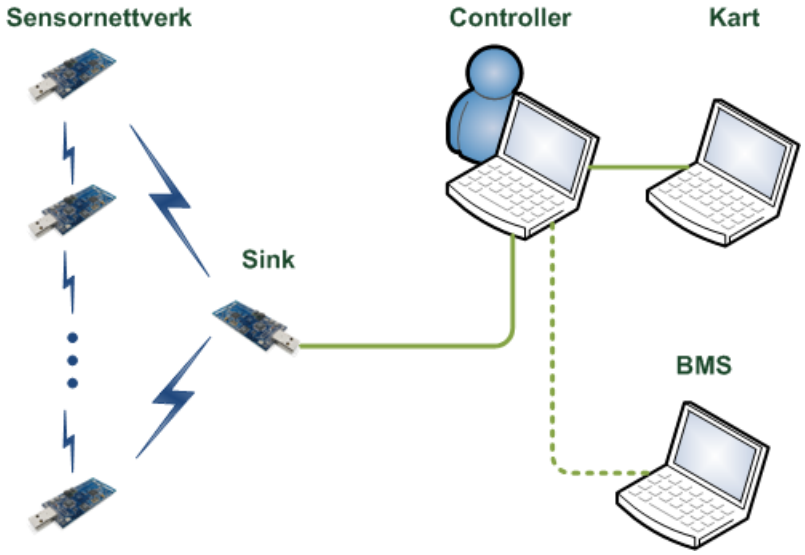
Før vi beskriver gjennomføringen av de to forsøkene beskrives det utstyret som ble brukt under uttestingen.

2 Sensorsystemer

2.1 Beskrivelse av SASS sensorsystem

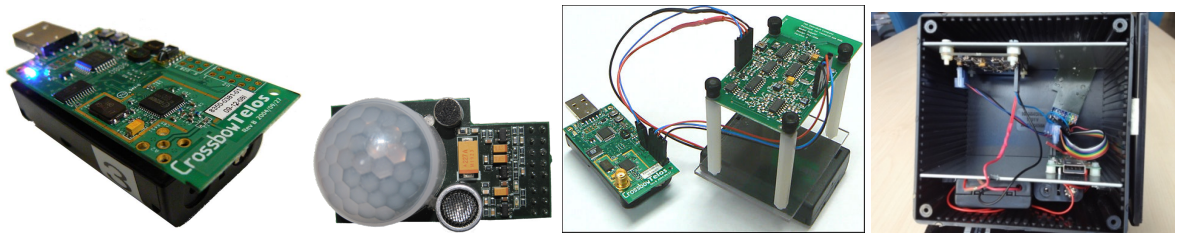
SASS («Situational Awareness Sensor System») er betegnelsen på det sensornettverkssystemet som ble utviklet i prosjekt 1141 og oppdrag 3836. SASS-systemet består av både programvare og elektronikk. De ulike modulene beskrives her kun kortfattet for å gi nødvendig introduksjon til de ulike konseptene som er utviklet og for å lettere kunne følge våre resultater og anbefalinger gitt i denne rapporten. For en utfyllende systembeskrivelse henvises til tekniske rapporter utgitt i prosjekt 1141 [7]. Arkitekturen til det komplette systemet vises i Figur 2.1.

Sensornettverk: Selve sensornoden (også kalt *mote* i litteraturen), er bygd opp rundt en kjerne bestående av standardkomponenter. Det sentrale kortet er en TelosB bestående av en mikrokontroller og en radiosender/mottaker (Figur 2.2a). TelosB er designet av University of California, Berkeley, men markedsføres av ulike produsenter, og er en meget populær prototypmodul benyttet av mange forskningsinstitusjoner og universiteter. Til denne har vi utviklet en egen sensormodul bestående



Figur 2.1 *SASS-systemet består av sensornoder som tilsammen danner et nettverk. Nettverket kommuniserer inn til en Controller via en sink.*

av en passiv IR detektor (PIR) og mikrofon (Figur 2.2b). PIR enheten har en Fresnellinse som gir ca 150 grader deteksjon og en teoretisk maksimal deteksjonsavstand på 10m. I tillegg benyttes en doppler radar fra Samraksh (Figur 2.2c). Både PIR og radar er velkjente detektortyper for å identifisere bevegelse. Elektronikken drives av standard AA batterier og er montert i en enkel boks (Figur 2.3). Det ble konstruert i alt 50 slike sensornoder for uttesting.

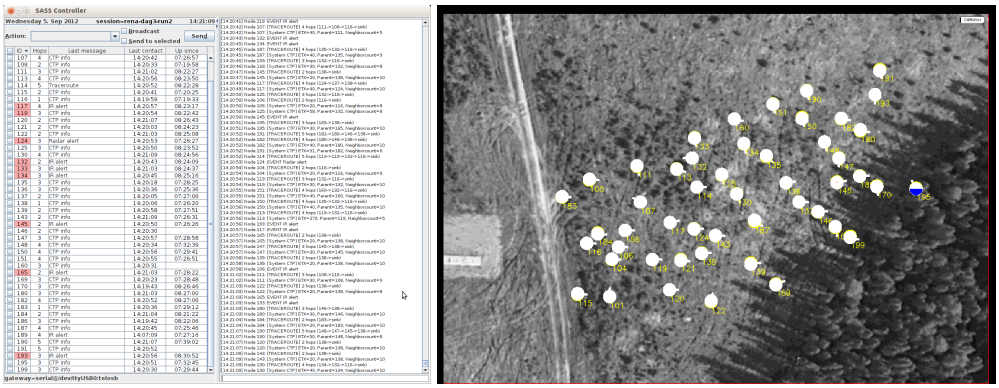


(a) Foto: OpenWSN (b) Foto: FFI (c) Foto: Samraksh (d) Foto: FFI

Figur 2.2 *SASS sensornoden består av (a) TelosB mote, (b) spesiallagd sensor-kort med PIR og mikrofon, (c) doppler radar-kort, og (d) innkapsling*

Sink: Alle målinger, alarmer og data som produseres av sensornodene sendes via en rutingprotokoll til en *sinknode*. Sinknoden er en tradisjonell TelosB som fungerer som en gateway mellom sensornettverket og en datamaskin. Denne datamaskinen er utstyrt med nødvendig programvare for å kommunisere med sensornettverket. Denne programvaren, «Controller», tjener to hensikter. For det første mottas og presenteres alle alarmer og målinger som foretas av sensornettverket her. Disse data blir også lagret for etterbehandling. Dernest benyttes «Controller» av operatøren for å konfigurere viktige parametre for sensorene (PIR, radar, akustisk) samt for nødvendig nettverkskonfigurering (se Figur 2.4).

Figur 2.3 Sensor-node utplassert i terreng



(a) Controller (b) Kart. Blått angir radar-alarm

Figur 2.4 «Controller»-programmet benyttes til å se rådata fra alle sensorene og til å konfigurere sensornettverkets oppførsel

Kartverktøy: «Controller» har kun et enkelt grensesnitt ment for utvikling og uttesting. I tillegg til dette er det utviklet et enkelt kartbasert verktøy som presenterer alarmer som genereres i nettverket på en lettfattelig måte. Dette verktøyet er ment å filtrere uønskede (falske) alarmer basert på ulike parametre samt å fusjonere data fra flere sensorer. Selv om noen sensorer vil kunne være plassert i et ugunstig miljø, og dermed vil kunne gi et uforholdsmessig stort antall falske alarmer, vil man ved datafusjon/aggregering kunne redusere andelen falske alarmer som presenteres til brukeren til et minimum.

BMS: Programvaren er ment å kunne kommunisere mot et BMS. For eksempel kan det være ønskelig at ulike filtrerte alarmer sendes direkte til et BMS i kjøretøy eller «NORMANS soldat-system» [4]. Denne funksjonaliteten ble ikke uttestet i forsøkene som beskrives i denne rapporten.

Sensorsystemet er ment for manuell deployering. Det vil si at nodene skal utplasseres enkeltvis av en soldat eller en operatør. Enkelte systemer nevnt i litteraturen bygges rundt et scenario der sensornodene for eksempel skytes ut eller slippes fra fly. Dette er derimot ikke relevant for et

perimetersikringsscenario. Ved manuell deployering er soldaten utstyrt med en bærbar datamaskin og GPS. Denne maskinen sender soldatens GPS posisjon til den sensornoden som utplasseres, slik at denne da får en noenlunde korrekt posisjonsangivelse. Et alternativ til vår løsning vil være å utstyre alle sensornodene med hver sin GPS-mottaker (slik som tilfellet er for Flexnet fra Exensor). Vår løsning sparer imidlertid både energi og utviklingskostnader siden det trengs kun én GPS.

2.2 Beskrivelse av Exensor Flexnet system

(a) (b) (c)

Figur 2.5 Exensor Flexnet består av (a) Seks UMRA mini seismisk detektorer, (b) et kamera (her kamuflert) , og (c) tre passive IR detektorer

I tillegg til FFIs egenutviklede system som beskrevet over ble det også uttestet et kommersielt system, Flexnet. Dette er det systemet vi kjenner til i dag som er tilgjengelig og som likner mest på våre konseptideer. Systemsettet FFI har består av seks seismiske detektorer (UMRA mini), tre passive IR sensorer, og et kamera. Alle disse ti sensorenhetene danner automatisk et mesh-nettverk (ikke ulikt hva som gjøres i SASS) slik at alarmer kan rutes automatisk via mellomliggende sensorenheter dersom avstanden mellom en perifer sensor og sentralen er lang. Hvilke valg produsenten har gjort av protokoller og liknende er ikke oppgitt.

Alle Flexnetenhetene er utstyrt med GPS slik at de selv finner egen posisjon som rapporteres inn til en sentral og presenteres der. Flexnet-systemet ufører ingen alarmfiltrering eller datafusjon, slik at en alarm generert av en enkelt sensor vil bli presentert som en faktisk alarm direkte til brukeren. En operatør kan eventuelt gjøre denne filtreringen manuelt. Umra mini sensorene (Figur 2.5a) kan gjøre enkel klassifisering av alarmer ved at den skiller mellom kjøretøy og personell.

3 Perimetersikring

3.1 Scenario

For å undersøke hvilken effekt trådløse sensorsystemer har i perimetersikringsøyemed, ble det utarbeidet et scenario for objektsikring. Utgangspunktet er deteksjon av personell til fots der området rundt objektet er av en karakter som vanskeliggjør full kontroll med tradisjonelt vakthold. Figur 3.1 viser området som ble valgt for uttesting. Området bestod av tett vegetasjon, fordypninger og grøfter, slik at en inntrenger ble gitt en mulighet å komme ubemerket inn til leiren,

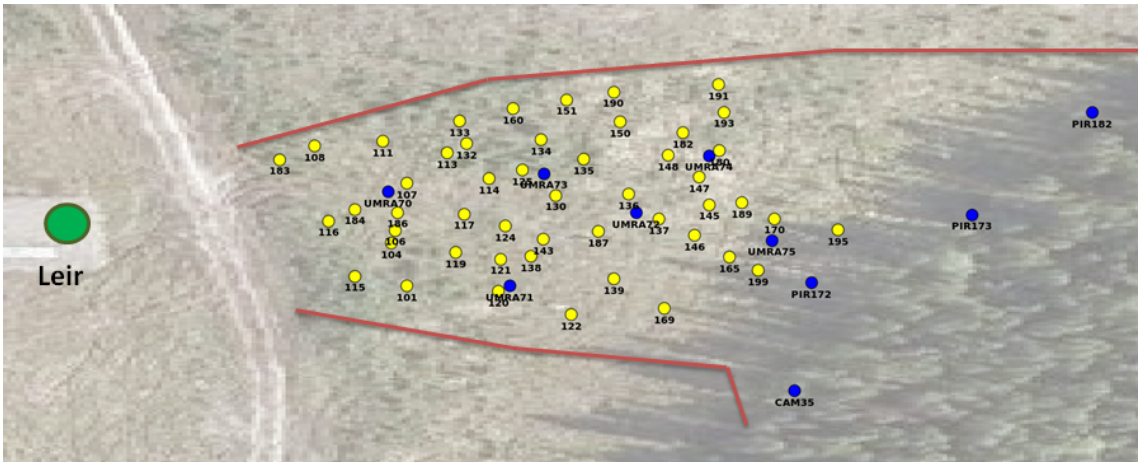
Figur 3.1 Området som ble overvåket. Bildet viser vaktpostens perspektiv.

eller i det minste så nært at de kunne utgjøre en fare i forhold til gitt trusselnivå. Oppgaven til sensorsystemene var i dette scenariet å gi rask og sikker varsling idet en eller flere inntrengere nærmet seg leiren.

3.2 Oppsett og gjennomføring av eksperiment

Det ble etablert en leir bestående av to telt som skulle sikres. Leiren ble etablert ved enden av en skinne for stridsvognssimulator på «BT-banen» på Rena. Leiren hadde åpen sikt i nord, vest og sydlig retning, mens det i østlig retning var begrenset sikt grunnet tett vegetasjon. Figur 3.1 viser utsikt fra leir i østlig retning. I dette østlige området ble det etablert en sektor på 100m bredde og 130m dybde som hadde spesiell interesse og som skulle overvåkes. I tillegg til sensorovervåkning ble leiren ble beskyttet med tradisjonelt vakthold.

I den sektoren som vaktpostene skulle observere plasserte vi ut våre 50 SASS-sensorenheter og de 10 Flexnet enhetene. Det store antallet SASS-noder gjorde det mulig å eksperimentere med mange ulike sensorplasseringer. Høyden over bakken varierte hovedsakelig mellom 0-40 cm, mens noen få sensornoder var plassert i trestammer i opptil 250 cm over bakken. Enkelte av sensornodene var skjult i vegetasjon eller kamuflert av mose, kvister etc., mens andre sensornoder hadde en mer åpen plassering. Videre varierte retningen sensorene pekte i. De fleste av sensorene pekte i østlig retning (dvs. bort fra leiren), men for noen sensorer var det naturlig med en annen innretting. Ut fra dette var det ikke noen garanti for at en sensor skulle gi utslag selv om en inntrenger passerte i sensornodens umiddelbare nærhet. Intensjonen var opprinnelig å muliggjøre multippel deteksjon av en inntrenger ved bruk av flere sensorer med overlappende deteksjonssektor. Den tette vegetasjonen gjorde det vanskelig å oppnå slik redundans i deteksjonen. De 50 sensornodene



Figur 3.2 Plassering av 50 SASS detektorer (gule) og 10 Excensor detektorer (blå) i forhold til leiren. Rødlinje markerer avgrensning av monitorert sektor.

ble spredt utover sektoren slik at området ble dekket best mulig. Plasseringen var grunnlagt i et ønske om å spore inntrengernes bevegelser i selve sektoren (se sensorplasseringen på Figur 3.2). Sensornodene ble tildels kamuflert (se Figur 3.3). Merk at forsøkene ikke hadde til hensikt å måle graden av kamuflasje[1]. Av denne grunn ble soldatene instruert om kun å rapportere om eventuelle sensorobservasjoner, ikke tilintetgjøre eller unngå dem, og ellers opptre så normalt som mulig.

(a) (b)

Figur 3.3 SASS sensornoder kamuflert

For Flexnet ble plasseringen av sensorene gitt av to forhold. For det første ønsket vi så tidlig varsling som mulig. Dermed ble de tre PIR-detektorene og et kamera (med PIR) plassert for sammen å dekke hele den ytre østlige grense av sektoren (se Figur 3.2). Dernest plasserte vi de seks UMRA-mini-sensorene spredt utover sektoren, slik at inntrengernes videre bevegelser kunne lokaliseres. UMRA-mini-sensorene ble samlokalisert med seks SASS-sensorer for å forenkle

[1]De fleste sensorene hadde meget begrenset kamuflasje for å forenkle innsamling av utstyret etter eksperimentets avslutning

gjenfunn etter eksperimentavslutningen.

Vaktstyrken bestod av tre soldater som hadde én nattkikkert samt én lysforsterkningsmonokkel for montering på HK416 tilgjengelig. I tillegg til vaktpostene var det en gruppe på tre soldater som spilte rollen som inntrengere. Med 12 soldater tilgjengelig tillot dette oss å gjøre fire gjennomkjøringer; to på dagtid og to på natten. Oppgaven til inntrengerne var å observere og rapportere om aktiviteten i leiren uten å bli oppdaget, mens oppgaven til vaktstyrken var å identifisere fiendtlig aktivitet i leirens perimeter så tidlig som mulig. Bortsett fra en observatør, som fulgte alle fire gruppene av inntrengere, var det ingen av soldatene som hadde rollen som inntrenger eller vaktstyrke mer enn en gang. De fire forsøkene ble gjennomført i henhold til Tabell 3.1.

Forsøk	Dag	Starttid	Forhold	Vaktstyrke	Inntrengere
A	05.09	10:00	Dag	Gruppe 1	Gruppe 2
B	05.09	14:00	Dag	Gruppe 2	Gruppe 1
C	05.09	22:00	Natt	Gruppe 3	Gruppe 4
D	06.09	01:00	Natt	Gruppe 4	Gruppe 3

Tabell 3.1 Forsøk. Det ble utført to forsøk på dagtid og to forsøk på natten

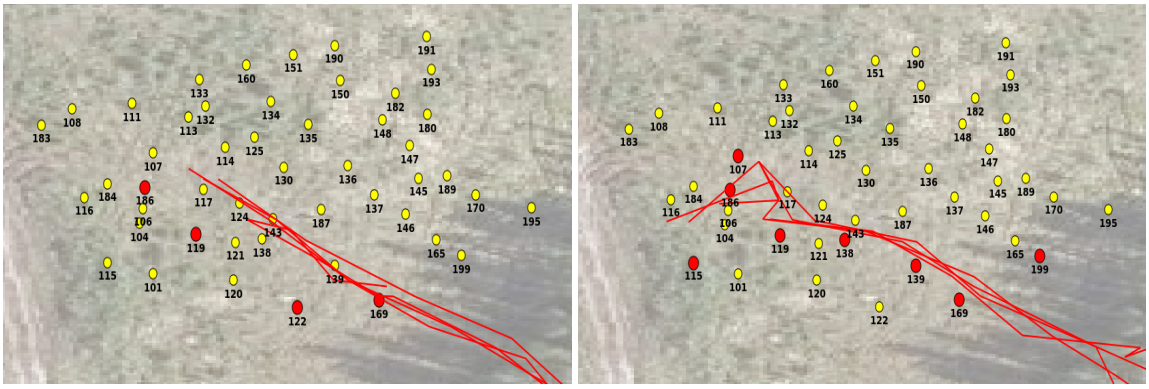
Soldatene som spilte rollen som inntrengere ble utstyrt med vester fra Hærens Taktiske Treningssenter. Deres posisjoner og tid kunne dermed logges og sammenliknes med alarmer generert fra sensorsystemene. Alarmer som ble generert uten at det var inntrengere i nærheten kunne med sikkerhet klassifiseres som falske. Inntrengerne hadde sin base ca 200m fra ytterkanten av monitorert sektor. Starttidspunktet er det tidspunktet da inntrengerne startet på vei mot leiren. I tiden mellom dette starttidspunktet og tidspunktet da inntrengerne kom inn i det monitorerte området, ble alle alarmer regnet som falske alarmer. Merk at ingen av de to systemene skiller mellom soldater og dyr/fugler. Slike deteksjoner vil også kunne føre til en viss andel falske alarmer.

3.3 Resultater

3.3.1 Resultater med SASS

For å filtrere bort feilmålinger ble SASS konfigurert slik at både PIR og radar måtte ha vært aktive på samme sensornode innenfor et tidsintervall på 5s for at det skulle registreres som reell alarm. Likevel ble det under forsøk A og B registrert så mange falske alarmer at sikker deteksjon av inntrengere ble ytterst vanskelig. De falske alarmene skyldes i all hovedsak vind. Under forsøk A og B ble det registrert en gjennomsnittsvind på hhv 3.3 og 8.1 m/s på målestasjonen på Rena flyplass. Vind i kastene var trolig en del høyere enn dette. Ved kraftig vind var det veldig mye vegetasjon i bevegelse innen sensorenes deteksjonssektor. Dette skapte problemer både for PIR og radar. Selv med fininnstilling av de sentrale parametre for både PIR og radar var resultatene fra forsøk B uentydige. Under forsøk A var det mulig for operatøren å bruke alarmene til å følge inntrengerne på et kart, men også her var andelen falske alarmer for høy til å gi entydige resultater. Det er verdt å merke seg at det ligger et stort potensial i forbedring av sensorytelsen.

Algoritmemessig kan det gjøres mye for å fjerne bakgrunnsstøy. Videre er selve sensorene vi har valgt meget rimelige og enkle. Det bør undersøkes hvorvidt andre sensorer av samme type, eventuelt andre typer sensorer, kan forbedre systemet uten å øke kostnaden nevneverdig. Spesielt ligger det et potensial innen PIR. Detektoren og linsen som ble benyttet er mest anvendelig innendørs, og langt bedre varianter finnes tilgjengelig for utendørsbruk.



(a) Forsøk C (b) Forsøk D

Figur 3.4 Resultat fra SASS. Figurene viser sensorenes plassering samt inntrengernes veivalg (fra høyre mot venstre) inn i området. Sensorer som har gitt alarm er merket med rødt.

For forsøk C og D ga SASS meget gode resultater. Figur 3.4 viser de sensorene som ga alarm relatert til inntrengernes bevegelser. Disse forsøkene ga et godt innblikk i potensialet til et slikt system. Det var mulig å følge inntrengernes bevegelser gjennom nettverket med høy nøyaktighet. Det var stor sikkerhet i målingene og minimalt med falske alarmer. For eksempel ga forsøk D kun én falsk alarm fra en enkelt sensornode. Denne alarmen var ukorrellert med nærliggende sensorer og slike alarmer kan derfor lett filtreres bort i programvare.

3.3.2 Tekniske resultater med SASS

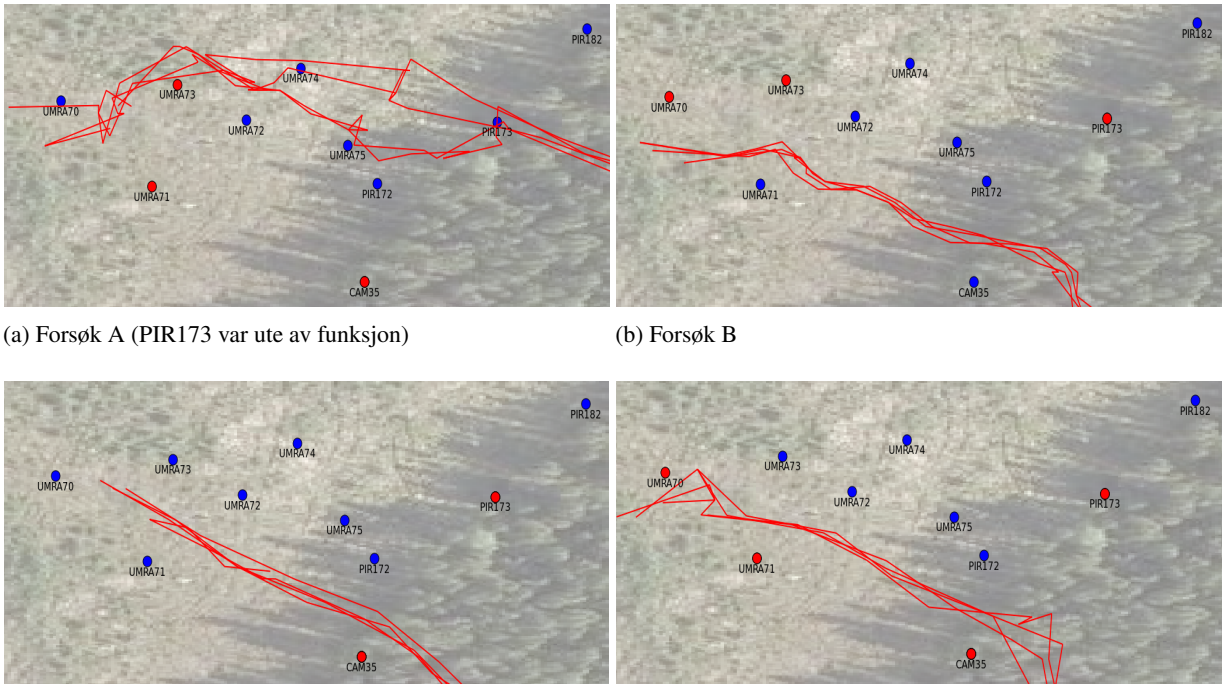
I tillegg til ren sensortrafikk ble det for alle forsøkene sendt kontrolltrafikk fra hver av sensornodene. Denne kontrolltrafikken gjorde det mulig å måle ytelsen til nettverket, slik som antall hopp fra en enkelt node til sink, hvilke stier trafikken tar gjennom nettverket, kvalitet på radiolinker, pakketap mv.

Forsøk	Pakketap	Meldinger/t
A	1.6%	6881
B	2.2%	8112
C	1.06%	6531
D	0.6%	6369

Tabell 3.2 Tekniske resultat fra forsøkene

Tabell 3.2 viser pakketap og totalt antall meldinger nettverket produserte per time. For alle fire forsøkene ble det målt noe pakketap. Pakketapet ligger innenfor det man vil kunne forvente av utstyr av denne typen. Resultatene viser at pakketapet påvirkes av mengden datatrafikk, noe som indikerer at pakketapet vil kunne reduseres med redusert trafikkpåtrykk. Trafikken består av to hovedelementer: kontolltrafikk og sensortrafikk. Kontrolltrafikken benyttes til å måle status i nettverket og er ikke nødvendig i en ferdig implementasjon. Sensortrafikken på den annen side, varierer med aktiviteten i monitorert sektor. I forsøk A og B var det vesentlig mer sensortrafikk enn i forsøk C og D. Denne sensortrafikken hadde i hovedsak sin årsak i at vind gjorde at sensorene ga (falsk) alarmmelding om bevegelse i deteksjonssektoren. Det er trolig at man ved å redusere trafikkpåtrykket (ved å sende mindre kontrolltrafikk) kan deployere vesentlig større nettverk enn vårt 50-noders nettverk uten at pakketapet blir en kritisk faktor.

3.3.3 Resultater med Flexnet



(a) Forsøk A (PIR173 var ute av funksjon)

(b) Forsøk B

(c) Forsøk C

(d) Forsøk D

Figur 3.5 Resultat fra Flexnet. Figurene viser sensorenes plassering og inntrengernes veivalg inn i området. Sensorer som har gitt alarm er merket med rødt.

Flexnet-systemet ga jevnt over gode resultater for alle fire forsøkene. Det ble registrert noen utfordringer med de seismiske UMRA-detektorene: Vi hadde kun seks detektorer tilgjengelig, noe som kan ha vært i minste laget for dette scenariet. I forsøk C klarte inntrengerne å komme seg forbi alle detektorene uten at noen av dem ga alarm (se Figur 3.5c). Mangelen på deteksjon skyldes sensorenes begrensede detektorrekkevidde. Terrenget bestod for det meste av fuktig og løst myrterreng, og deteksjon av personell var kun mulig innenfor en begrenset radius på anslagsvis 5-10m rundt sensoren. I noen tilfeller var inntrengerne fysisk i kontakt med sensoren (den

ga «tamper-alarm»[2]) uten at inntrengeren først ble detektert seismisk. Til tross for de overnevnte begrensninger i antall og deteksjonsradius, var sensorene meget pålitelige. Vi registrerte ingen falske alarmer under de fire forsøkene. Det var noe kjøretøytrafikk på en vei ca 150-200m fra sensorene. Disse kjøretøyene ble iblant detektert av sensorene, og korrekt klassifisert som kjøretøy. Alle alarmer som ble klassifisert som personell var korrekte.

Vi opplevde kablingsproblemer på de passive IR detektorene på Forsøk A. Dette ble rettet for de etterfølgende forsøkene, og PIR fungerte meget godt. Det ble observert kun en falsk alarm på PIR detektorene gjennom forsøksperioden.

Figur 3.6 En inntrenger kommer inn i området. Bilde tatt med Flexnet kamera (CAM 35) under Forsøk A.

Kameraet som ble benyttet er utstyrt med PIR-detektor og sender et bilde tilbake til kommandosentralen dersom PIR-detektoren gir utslag. Det er også mulig å konfigurere kameraet slik at det gir en alarm dersom det er vesentlige endringer i bildet. Denne innstillingen ga imidlertid en rekke falske alarmer. Selv om slike alarmbilder er enkle å eliminere av en operatør, må antallet slike alarmer minimeres for å øke brukbarheten til systemet. I beste bildeinnstilling var det ofte problemer med bildeoverføringen, noe som medførte at bildet ikke kom frem i sin helhet og ofte var ubrukelig. Ved å benytte innstilling for middels kvalitet fungerte systemet etter hensikten. Et eksempel på et godt alarmbilde er vist i Figur 3.6. Kameraet er ikke spesielt lysfølsomt og fungerer best i godt dagslys. Et nattkamera eller et termisk kamera hadde vært mer anvendelig. Exensor har nylig fått produkter i sin portefølje som har bedre spesifikasjoner og muligheter enn det kameraet som ble uttestet.

[2]UMRA-mini-er utstyrt med akselleromeetere og sender en alarmmelding dersom den løftes.

3.4 Oppsummering

Hovedresultatene er oppsummert i tabell 3.3. Tiden for inntrengning er tidspunktet da første soldat i inntrengergruppen kom inn i østlig perimeter. All den tid det var Flexnet-sensorer (PIR) plassert lengre øst enn der hvor SASS-nettverket hadde sin østlige grense, var det forventet en tidligere deteksjon med Flexnet enn med SASS. Resultatene er derfor ikke direkte sammenliknbare. SASS har bedre ytelse enn Flexnet dersom man ser isolert på UGS-delen i Flexnet. På dagtid ble det som tidligere nevnt usikre deteksjoner med SASS-systemet. For natt-testene fungerte SASS derimot like godt som Flexnet og, siden det var langt flere SASS-sensorer, med bedre presisjon (flere sensornoder ble aktivert).

Forsøk	Inntrenging	Flexnet deteksjon	SASS deteksjon	Vaktsoldaters deteksjon
A	10:21	10:22 (4)	10:22/usikker	10:31
B	14:12	14:12 (3)	usikker	14:25
C	22:05	22:10 (2)	22:22 (4)	ikke detektert
D	01:07	01:07 (4)	01:12 (8)	01:29

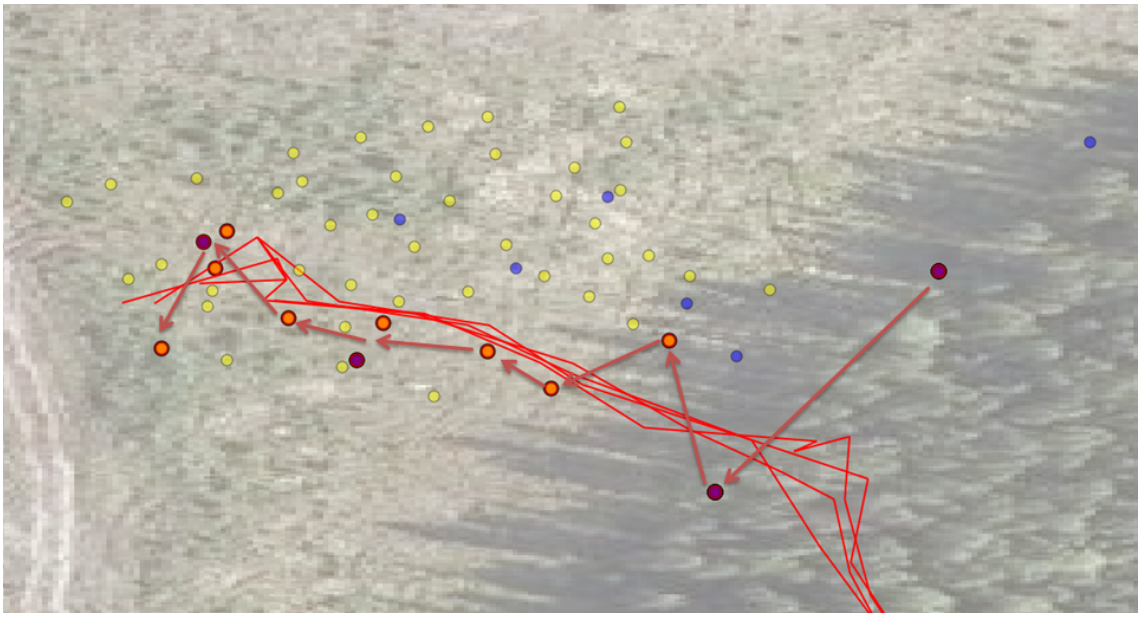
Tabell 3.3 Sammenlikning av deteksjonstidspunkt. Totalt antall alarmgivere som ble aktivert av inntrengere er gitt i parentes

I alle tilfeller ble inntrengerne detektert vesentlig raskere med sensorer enn hva vaktsoldatene klarte. Det er verdt å merke seg at eksperimentoppleggets natur gjorde at vaktsoldatene tildels var klar over tidspunktet inntrengerne ville ankomme området. Videre var vaktperiodene såpass korte at vaktsoldatene ikke ble slitne eller trette i noen særlig grad. Det er derfor naturlig å anta at forskjellene mellom vaktstyrken og sensorsystemene når det gjelder deteksjonspresisjon- og tid vil være langt større operativt.

3.5 Diskusjon

Kombinasjon av de to systemene ga tilsammen et meget bra situasjonsbilde. Figur 3.7 viser kombinerte deteksjoner for både SASS og Flexnet for forsøk D. Benyttelse av flere ulike sensorer (her: radar, ir og seismisk), gir sammen meget god deteksjonssannsynlighet. Samtidig er det mulig å utnytte disse for å redusere andelen falske alarmer. For eksempel må både PIR og radar aktiveres på samme sensornode innenfor et gitt intervall for at det skal registreres som alarm i SASS-systemet. Denne fremgangsmåten ga meget lav andel falske alarmer, og samtidig, en høy deteksjonssannsynlighet. Med bedre algoritmer og sensorer, vil det være mulig å benytte et mindre strengt detektorregime, og dermed oppnå enda større presisjon i deteksjonen uten å øke sannsynligheten for falske alarmer.

Det er opplagt at et hvert sensorsystem gir best resultater når hver sensor er omhyggelig plassert og kalibrert slik at det gir korrekte deteksjoner i gjeldende miljø. Vi erfarte at plasseringen av hver enkelt sensor er spesielt viktig når antallet sensorer er lavt (som for Flexnet). Med et høyt antall sensorer er gjerne ikke plasseringen like kritisk. Deployeringstiden til et system kan derfor ikke



Figur 3.7 Kombinasjon av Flexnet og SASS gir et veldig nøyaktig situasjonsbilde. Pilene viser inntrengernes bevegelser målt av sensorsystemene, mens røde linjer viser inntrengernes reelle bevegelser

sies kun å være avhengig av antallet sensorer. Et enkelt system med et høyt antall små sensorer kan gjerne deployeres på samme tid som et system med et langt færre antall sensorer.

4 Monitorering av veiakse

4.1 Introduksjon

Aksemonitorering kan være et av elementene i et perimetersikringssystem rundt en leir og således utvide konseptet presentert over. Men det kan også være et separat system for overvåkning av et område lengre fra leiren og som har spesiell interesse. Et sensorsystem som SASS kan benyttes til å overvåke slike akser ved at nodene utplasseres langs en vei eller trasé som motparten mest sannsynlig vil benytte. På denne måten dannes en overvåkningsgate med sensorer som kan dekke et stort område.

I et veiaksescenarie vil et stort antall sensornoder gi muligheter både til å overvåke lange akser og til å øke redundans og presisjon i deteksjonene. En stor tetthet på nodene vil kunne bidra til å angi retning og hastighet på kjøretøy, samt å kunne skille mistenkelige deteksjoner fra normalstatus basert på objektenes oppførsel. For eksempel kan det være ønskelig å gi alarm dersom et kjøretøy stanser en stund for så å kjøre videre. En slik oppførsel vil for eksempel kunne bety at noen har utplassert en IED, og at dette området må undersøkes nærmere med andre midler. Basert på innsamlede data fra sensorene langs aksen, kan slike hendelser spilles av og analyseres i ettertid.

4.2 Gjennomføring av eksperiment

Figur 4.1 Akseovervåkning av en 190m lang veiakse. 40 sensornoder med radar, IR og akustisk sensor utplassert.

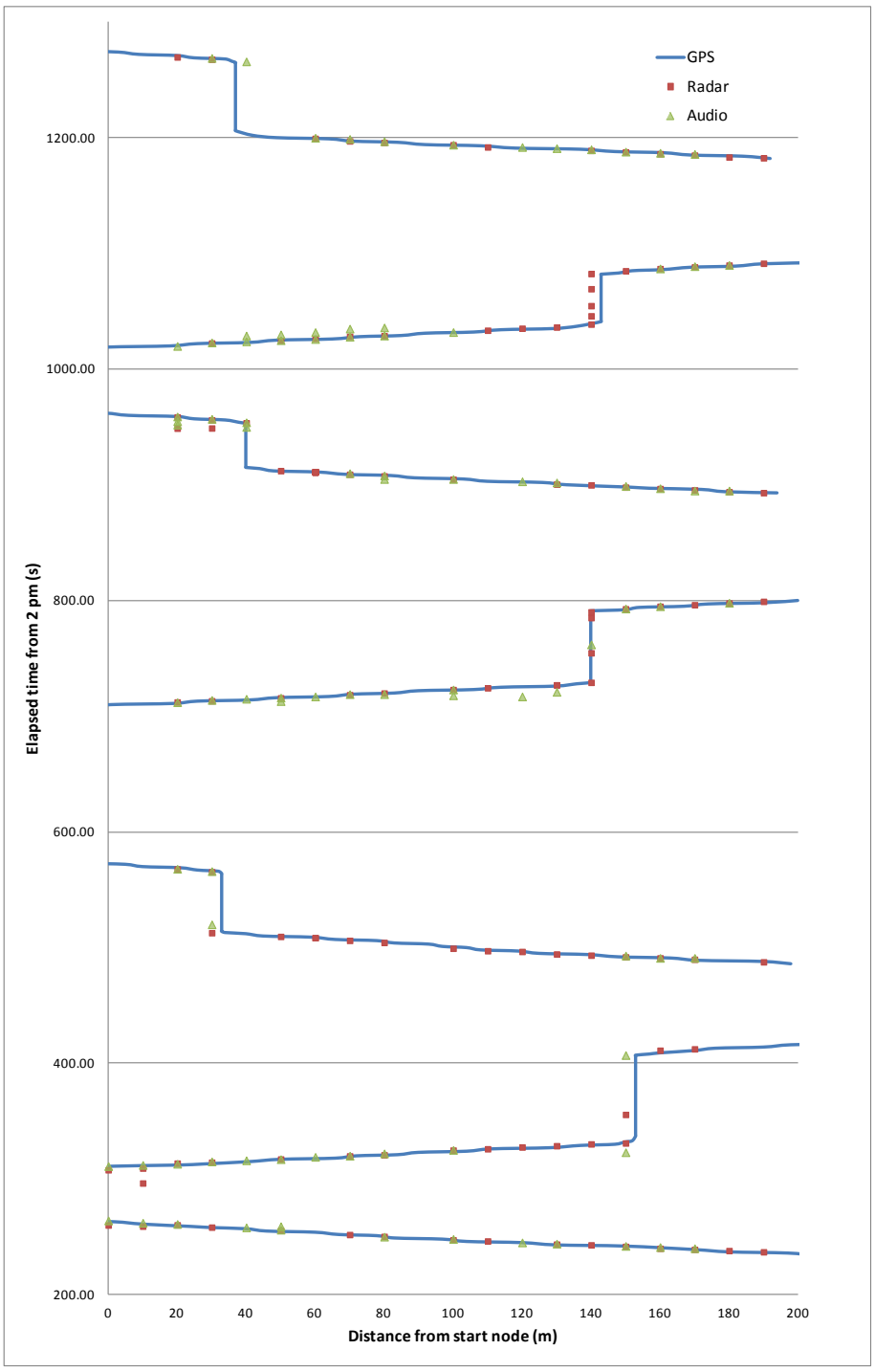
I dette eksperimentet ble det kun brukt FFIs egne SASS sensorer som beskrevet i kapittel 2.1. For tidligere resultater fra FFI-forsøk med veiaksemonitorering med andre sensorer, deriblant Flexnet, henvises til [1].

En veistrekning på 190m ble instrumentert med 40 SASS sensornoder, 20 på hver side av veien med en innbyrdes avstand på 10m (Figur 4.1). Sensorene på den ene side av veien ble aktivert med IR og Radar, mens de 20 sensorene på den andre siden ble aktivert med akustisk sensor (mikrofon). Det ble gjort en rekke forsøk med passering av kjøretøy både med og uten stopp.

Et viktig moment i dette eksperimentet er behovet for tidssynkronisering mellom noder i nettverket. Dette er avgjørende med tanke på korrekt gjengivelse av hendelsesforløpet og estimat av hastighet, spesielt når objektet som overvåkes har en høy hastighet. Av denne grunn har vi i dette eksperimentet brukt Flooding Time Synchronization Protocol (FTSP) som sørger for at klokken på nodene i nettverket er synkroniserte med hverandre. En mer detaljert beskrivelse av FTSP protokollen samt vår modifikasjon av protokollen er omtalt i en egen rapport [8].

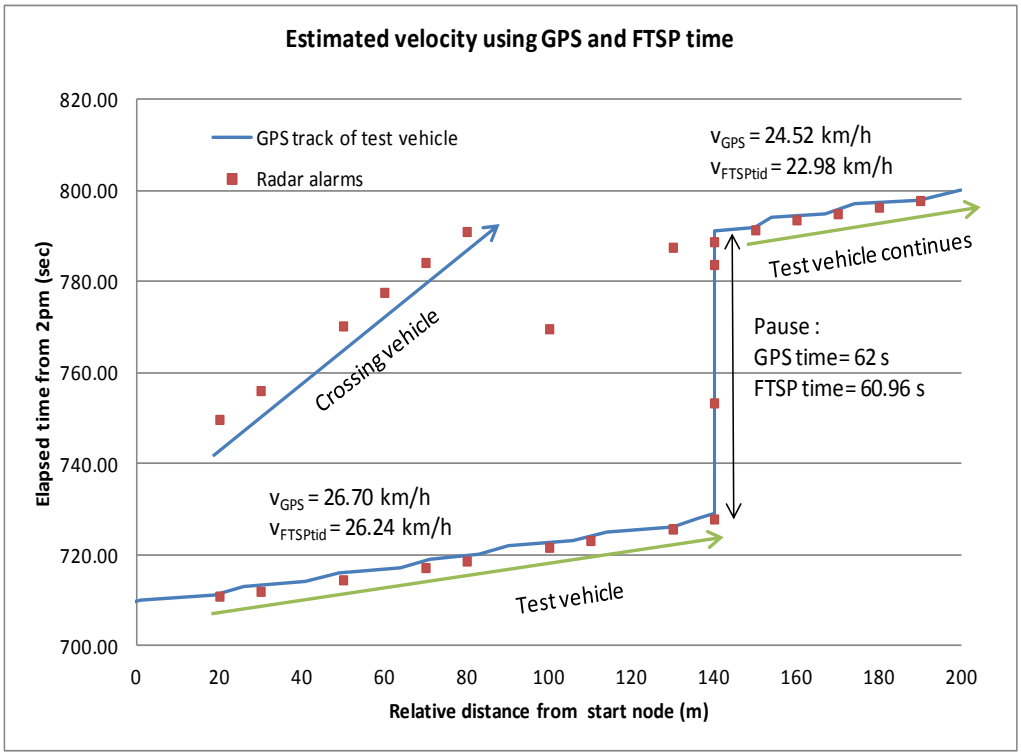
4.3 Resultater

Figur 4.2 viser målinger av testkjøretøyet som passerer gjennom nettverket. Figuren viser GPS-tracket til kjøretøyet, samt utslag med radar og akustiske sensorer langs x-aksen og tid på y-aksen. Det er mulig å spore et objekt gjennom nettverket med radar og i stor grad med mikrofon. Feilmålinger som ikke er korrelert med målinger fra andre sensornoder er enkle å filtrere bort. Spesielt for radar ga dette veldig gode resultater der falsk-alarmraten er liten. For mikrofon er andelen false alarmer noe høyere siden den er mer sensitiv for faktorer som for eksempel vind



Figur 4.2 Deteksjon av kjøretøy som passerer gjennom det monitorerte området.

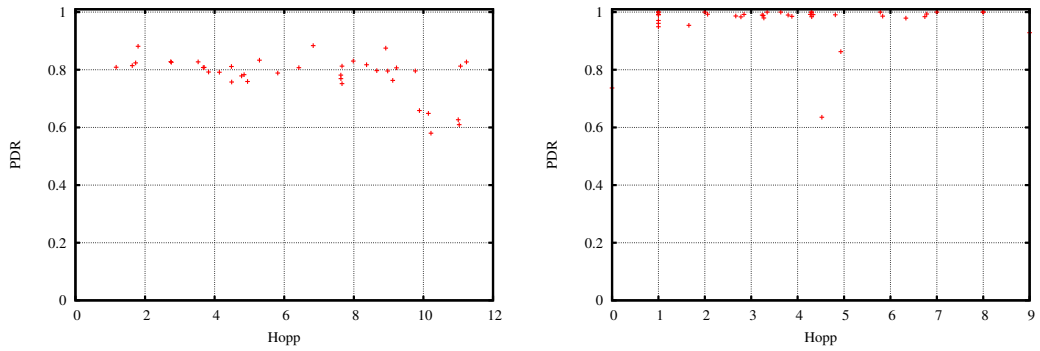
og andre støykilder. Passiv IR (ikke vist i figuren) fungerte også bra til kjøretøydeteksjon, men siden variasjoner i solforhold og skydekke påvirker sensoren, kan flere sensornoder gi falsk alarm samtidig. Slike tilfeller er vanskelige å filtrere bort.



Figur 4.3 Deteksjon av kjøretøy som kjører inn i området, gjør en stopp, og kjører videre. Sammenligning av estimert hastighet og varighet på opphold basert på tidssynkronisert sensordata og GPS-data

Figur 4.3 viser eksempel på kjøretøypassering med stopp. I dette forsøket kjørte vi inn i det monitorerte området og stanset etter 140m, før vi kjørte videre etter ett minutt. Selv om et annet kjøretøy var i området samtidig, er det mulig å skille ut denne hendelsen. Disse sensormålingene kan være inn-data til algoritmer for automatisk å skille ut abnormal og mistenkelig adferd fra normaltilstanden. For eksempel vil det kunne være mulig å gi et varsel dersom et kjøretøy stopper en viss tid på visse steder i veiaksen.

Figur 4.3 viser også at det mulig å estimere gjennomsnittshastigheten og varigheten på oppholdet med rimelig god nøyaktighet. Estimatene er basert på alarmenes tidsstempel (synkronisert tid) og ved bruk av lineær regresjon. Avviket mellom estimatene og kalkulert hastighet basert på GPS-data er relativt lite. Dette er en indirekte bekreftelse på at tidssynkronisering ved bruk av FTSP fungerer meget tilfredsstillende.



(a) Endeplassert sink (b) Midtplassert sink

Figur 4.4 Figuren viser hver av de 40 sensornodenes avstand til sink (i antall hopp) og pakkeleveringsraten (PDR).

4.4 Tekniske resultater

Det ble forsøkt to ulike sinkplasseringer. I forsøk A hadde sinken en plassering ved enden av nettverket, mens i forsøk B hadde sinken en plassering midt i nettverket. Figur 4.4 viser forholdet mellom avstanden sensornodene har til sink og pakkeleveringsraten. Med sink plassert på enden av nettverket, var den totale pakkeleveringsraten 78.38% (et pakketap på 21.5%). Det er også en tendens til at nodene lengst fra sink har høyest pakketap. Med en sinkplassering midt i nettverket økte pakkeleveringsraten til 96.8%. Vi ser at systemet er følsomt for antall hopp og nodetettheten. Rekkevidden på radionettverket (ett hopp) var typisk 30m i dette scenariet, men varierte mellom 10 og 60m. Forbedringer i antenneplassering, radiotype og frekvens vil gi et mer anvendelig system. Å bytte ut 2.4GHz radiokretsen til fordel for en som benytter frekvensområdet 868MHz vil kunne gi en anvendbar rekkevidde på rundt en kilometer. Dette vil gjøre det mulig å deployere et system som dekker en veistrekning på 2000-4000m med tilsvarende antall noder som ble benyttet i vårt eksperiment.

5 Oppsummering

5.1 Konklusjoner

SASS-systemet har vist seg både robust og stabilt innenfor de kravene som stilles til testutstyr av denne typen. Vi har sett at kombinasjon av sensortyper er veldig nyttig for å minimere andelen falske alarmer. Videre har forsøkene både for perimetersikring og akseovervåkning vist at et stort antall sensorer er meget nyttig for å kunne spore objekter i nettverket. Slik sporing kan benyttes til å gi et detaljert bilde av oppførselen til eventuelle inntrengere, og være et nyttig støtteverktøy for klassifisering. Flere sensorer i samme område vil kunne samarbeide om å øke deteksjonspresisjonen. Et stort antall sensorer er heller ikke nødvendigvis et hinder for enkel deployering og logistikk.

Anvendbarheten til sensornettverket avhenger av rekkevidden til radiosystemet som benyttes. Lengre rekkevidde går som oftest på bekostning av datakapasitet, men gir store fordeler som økt robusthet, enklere protokolldesign, og større spillerom ved deployering.

Bildegivende sensorer ses på som viktig for å verifisere alarmer. Likevel er det ikke gitt at kameraer i seg selv fører til et mer brukervennlig system. Det bør gjøres flere eksperimenter på hvilke kameratyper, plassering og antall som er formålstjenlig i perimeter- og aksescenarier.

5.2 Forslag til videre arbeid

Videre arbeid bør inkludere både videreutvikling, undersøkelse av eksisterende produkter og produsenter av sensorsystemer, og felttesting. Enkelte kapasiteter uttestes best ved at FFI fortsetter egenutvikling av sensornettverk. Vi har vist at slik utvikling er både gjennomførbar, rimelig og er kompetanseoppbyggende, samtidig som det gir en fleksibel plattform for uttesting av ulike sensorteknologier. Andre kapasiteter uttestes best ved at det kjøpes inn ferdige sensorsystemer. Det bør settes av ressurser til innkjøp av slikt utstyr, samt til å samarbeide med produsenter.

Et sensornettverk med marksensorer vil ikke operere alene, men må ses i sammenheng med andre sensorsystemer og aktuatorer. Totalsystemet må også kunne operere mot et kjent kartsystem og eventuelt et Battlefield Management System (BMS). FFI har gjort en initielt arbeid med slike grensesnitt [5]. Ved bruk av enkle og kjente grensesnitt det et stort potensial for å lage gode systemer som fungerer godt sammen. En type aktuell integrasjon er å knytte sensorsystemet opp mot en mobil overvåkningssensor, for eksempel et lite autonomt helikopter, Micro Unmanned Aerial Aystem (MUAS) [6], som kan nyttes for alarmverifikasjon. Dette kan være langt mer anvendelig enn å benytte stasjonære kameraer.

Systemene må være enkle å bruke samt raske å deployere. Et eksempel på et aktivt forskningsfelt er selvlærende autokonfigurerende sensorer. Slike sensorer vil selv kunne lære hva som er normaltilstand og hva som er alarmtilstand. Dette vil forenkle konfigureringen og bidra til sikrere deteksjoner. Det bør gjøres lengre tester med et større antall noder. Sensornodene må derfor konstrueres slik at de kan operere autonomt over lengre tid (måneder) og under røffe værforhold.

Appendiks A Akronymer og forkortelser

ADSID	Air Delivered Seismic Intrusion Detector
BMS	Battlefield Management System
CDE	Concept, Development & Experimentation
MUAS	Micro Unmanned Aerial Aystem
PIR	Passiv Infrarød Sensor
SASS	Situational Awareness Sensor System
UGS	Unattended Ground Sensors

Referanser

[1] I. Cook and H. Bouskell. Week 44 2010 Sensor demonstration report. Technical report, SDE-Report 1995/R/8813/19 (Restricted), 2011.

[2] I. Dyrdal. Anbefalinger for anskaffelsesprosjekt 5834 - sensormateriell. Technical report, FFI-Rapport-2012/00073, 2012.

[3] Exensor. The Flexnet system (http://www.exensor.com).

[4] J. Flathagen. Kommando, kontroll og informasjonssystemer på soldatnivå. Technical report, FFI-Rapport-2009/01059, 2009.

[5] J. Flathagen and F.T. Johnsen. Integrating Wireless Sensor Networks in the NATO Network Enabled Capability using Web services. In *IEEE Military Communications Conference, 2011-MILCOM 2011*, pages 828–833. IEEE, 2011.

[6] Hoelsæter, Ø., Bakstad, L., Gullbekk, H., Olafsen, H. NUAS - eksperimentrapport CD&E 2011. Technical report, FFI-Rapport-2012/00024, 2012.

[7] Pham, V., Flathagen, J.,Larsen, E., Mjelde, T., Korsnes, R., Sander, J. Sluttrapport for prosjekt 1141 Situational Awareness Sensor Systems (SASS). Technical report, FFI-Rapport-2012/02490, 2012.

[8] Pham, V., Larsen, E., Mjelde, T., Korsnes, R., Sander, J. FTSP tidssynkronisering for trådløst sensornettverk: Evaluering og tilpasning. Technical report, FFI-Rapport-2012/02078, 2012.

[9] Svinsås, E., Hanssen, L., Arneson, V., Larsen, E., Pham, V., Flathagen, J., Dalsjø, P., Gakkestad, J., Korsnes, R. Situational Awareness Sensor Systems (SASS) - grunnleggende scenarier og krav. Technical report, FFI-Notat-2009/01905, 2009.