



Soldatens WBAN

Förstudie

JOUNI RANTAKOKKO, GUNNAR ERIKSSON, ANDERS HANSSON,
DANIEL EIDENSKOG, DAVID LINDAHL, STEVEN SAVAGE

Jouni Rantakokko, Gunnar Eriksson, Anders
Hansson, Daniel Eidenskog, David Lindahl,
Steven Savage

Soldatens WBAN

Förstudie

Titel	Soldatens WBAN - Förstudie
Title	Soldier WBAN – a feasibility study
Rapportnr/Report no	FOI-R--4237--SE
Månad/Month	Mars
Utgivningsår/Year	2016
Antal sidor/Pages	50 p
ISSN	1650-1942
Kund/Customer	FMV
Forskningsområde	4. Informationssäkerhet och kommunikation
FoT-område	Ledning och MSI
Projektnr/Project no	E324536 / E324832
Godkänd av/Approved by	Per Johannesson
Ansvarig avdelning	Ledningssystem

Detta verk är skyddat enligt lagen (1960:729) om upphovsrätt till litterära och konstnärliga verk, vilket bl.a. innebär att citering är tillåten i enlighet med vad som anges i 22 § i nämnd lag. För att använda verket på ett sätt som inte medges direkt av svensk lag krävs särskild överenskommelse.

This work is protected by the Swedish Act on Copyright in Literary and Artistic Works (1960:729). Citation is permitted in accordance with article 22 in said act. Any form of use that goes beyond what is permitted by Swedish copyright law, requires the written permission of FOI.

Sammanfattning

Syftet med denna förstudie var att genomföra en initial analys av de möjligheter och svårigheter som kan förväntas uppkomma vid ett framtida införande av trådlösa korthållsradionet (*WBAN – Wireless Body Area Network*) på soldaten. WBAN-systemet är primärt avsett för överföring av information från soldatburna sensorer till en processorenhet (dator) och/eller användargränssnitt. Den huvudsakliga motiveringen för att införa WBAN-system på soldaten är att reducera vikt och storlek för soldatens utrustning genom att ersätta kablar och kontaktdon med små, lätta och strömsnåla WBAN-enheter.

Utmaningarna vid införandet av ett generellt WBAN-system för soldaten är flera, exempelvis risken för upptäckt eller avlyssning av informationen, robusthet mot störning och interferenser samt att informationen i vissa fall kan vara av kritisk natur vilket kräver hög tillgänglighet.

I rapporten ges beskrivningar av utvecklingen av möjliga framtida soldatburna sensorer på kort och lång sikt och de användarbehov som i dagsläget förutses. Initiala analyser har genomförts av robusthet och smygegenskaper för alternativa tekniker, som efterliknar de som anges i standarden IEEE 802.15.6. Generella säkerhetsaspekter för WBAN-system och designrekommendationer för framtida WBAN-system beskrivs även. Slutligen föreslås en roadmap för det fortsatta arbetet som bedöms vara nödvändigt för att möjliggöra ett framtida införande av WBAN i soldattillämpningar.

Nyckelord:

Soldat, WBAN, WPAN, kabelersättare, robusthet, smygegenskaper, säkerhet, UWB, HBC

Summary

The purpose of the conducted study was to perform an initial analysis of expected possibilities and difficulties when implementing a wireless body area network (WBAN) for soldier applications. The WBAN system is primarily designed to transfer data from soldier-worn sensors to a processing unit and various user interfaces. The main motivation for introducing a soldier WBAN is to reduce weight and size of the soldier equipment by replacing cables and bulky connectors with small, lightweight and energy efficient WBAN-transceivers.

The challenges that are expected to arise when considering the implementation of a general soldier WBAN are multiple, including the risk that the enemy can detect the presence of our soldier's or eaves-drop on the information, robustness towards jamming and inter- and intra-system interference sources, and that the information can be of critical nature for the soldier leading to a requirement for high availability.

Future soldier-worn sensors are described, both in the short and long terms, together with the user needs that are anticipated today. Initial analysis of the anti-jamming and covert capabilities have been performed for alternative technologies, which resemble those described in the IEEE 802.15.6 standard. General security aspects for WBAN's and design recommendations for future systems are also described. Finally, a roadmap is proposed for the work that is deemed needed for paving the way for a future implementation of a soldier WBAN system.

Keywords:

Soldier, WBAN, WPAN, cable replacement, robustness, stealth, security, UWB, HBC

Innehållsförteckning

1	Inledning	7
1.1	Bakgrund	7
1.2	Syfte och mål	8
1.3	Studiens upplägg	8
1.3.1	Avgränsningar	9
1.3.2	Rapportens disposition	9
2	Sensorer för soldattillämpningar	11
2.1	Soldatsystemets utveckling och inriktning	11
2.2	Möjliga soldatburna sensorer i närtid	12
2.3	Möjliga soldatburna sensorer på längre sikt	14
2.3.1	Future Soldier 2030 Initiative	14
2.3.2	Övervakning av soldaten och dess omgivning	15
2.3.3	Diskussion.....	15
3	Analys av användarbehov	17
3.1	Generell kravdiskussion	17
3.2	Exempel på krav som kan påverka WBAN	17
3.3	Robusthets- och smygaspekter	19
3.3.1	Exempel på hotbild	19
3.3.2	Robusthetsaspekter	19
3.3.3	Smygegenskaper	20
3.4	Informationssäkerhet	20
3.5	Hälsorisker	20
3.5.1	Diskussion.....	21
4	Tekniköversikt	23
4.1	Trådlösa korthållsradionät (WBAN/WPAN)	23
4.1.1	Civila system	23
4.1.2	Militärspecifika system	24
4.2	Trådbunden kommunikation (BAN).....	25
4.2.1	Utvecklingstrender i närtid	25
4.2.2	Utvecklingstrender bortom 2020	27
4.3	Alternativa trådlösa tekniker.....	27
4.3.1	Kommunikation med kroppen som överföringsmedium	28
4.3.2	Ultraljud	28
4.3.3	Molekylär kommunikation	29
5	Analys av robusthet och smygegenskaper	31
5.1	Robusthet.....	31
5.2	Smygegenskaper	32

5.3	Utvärdering	32
5.3.1	Slutsatser och diskussion	34
6	Analys av säkerhetsaspekter	37
6.1	Informationens skyddsvärde.....	37
6.2	Signalskydd	37
6.3	Nätverkstopologi	39
6.3.1	Addition av otillåtna enheter till nätverk.....	39
6.4	Självskydd.....	39
6.4.1	Hotbeskrivning	39
6.5	Diskussion och slutsatser	40
6.5.1	Nyckelhantering	41
6.5.2	Autentisering.....	41
6.5.3	Öppet kontra hemligt WBAN	41
7	Rekommenderade designprinciper	43
7.1	Samexistensaspekter och systemförslag	43
7.2	Designrekommendationer	43
8	Slutsatser och rekommendationer	45
8.1	Sammanfattande gapanalys.....	45
8.1.1	Robusthet och smygegenskaper.....	45
8.1.2	Säkerhetsaspekter.....	45
8.2	Rekommendationer	45
	Referenser	47
	Appendix A – Robusthetsanalys	49

1 Inledning

Syftet med förstudien var att genomföra en initial analys av möjligheter och svårigheter med att införa trådlösa korthållsradionät på soldaten. Radionätets primära uppgift är överföring av information från soldatburna sensorer till en processorenhet (dator) och/eller användargränssnitt.

Rapporten utgör slutrapportering av förstudien *Soldatens WBAN*¹ som finansierats inom ramen för FMV FoT-verksamhet inom delområdet Samband och Telekom.

1.1 Bakgrund

Soldatens stridsförmåga och operativa effekt kan förbättras väsentligt genom användandet av soldatburna sensorer. Erfarenheter från tidigare MARKUS-studier (se [1]) och efterföljande arbeten inom Försvarmakten har visat på de vinster som kan uppnås med ny teknik. Erfarenheterna baseras främst på införandet av satellitnavigeringshjälpmedel och digitalt kartstöd, radiosamband inom gruppen samt mörkermateriel för soldaten (såsom bildförstärkare, mörkerriktmedel, termiska IR-kameror). En utmaning är dock att soldatens utrustning redan idag väger för mycket. Införandet av nya förmågor förutsätter därför att dessa inte belastar soldaten ytterligare utan snarare kan leda till reduceringar i utrustningens vikt. Det förutsätter sannolikt i sin tur att det framtida soldatmaterielsystemet utvecklas till ett integrerat (och modulärt) system.

Den civila marknaden inom konsumentelektronik driver utvecklingen framåt när det gäller att uppnå en förbättrad prestanda för små, lätta och strömsnåla personburna sensorer. En modern smartphone innehåller ett stort antal sensorer med prestanda som få kunde ana för ens tio år sedan. Utvecklingen har dock varit mest dramatisk när det gäller reduktionerna i sensorernas vikt, storlek, energieffektivitet och kostnad (*Size, Weight, Power and Cost, SWaP-C*). Utvecklingen av ruggade sensorer anpassade för soldattillämpningar går däremot långsammare. Det har bland annat lett till att militären i USA har börjat använda konsumentelektronik i en större omfattning där ett exempel är mobiltelefoner som görs mer stryktåliga med olika skal.

Den snabba sensorutvecklingen har gjort att soldaternas mycket hårda krav på *SWaP-C* i många fall kan vara möjliga att uppfylla. De kablar och kontaktdon som behövs för att överföra informationen från sensorerna (som i en del situationer inte kan vara samlokaliserade med dator och visualiseringsenhet) utgör dock en betydande integrationsutmaning på soldaten. Det gäller exempelvis mellan sensorer och beräknings- eller visualiseringsenhet såsom GPS- eller GNSS-mottagare³ och display för ett navigeringsstöd eller *Blue-Force-Tracking (BFT)* system, CBRN⁴-sensorer, hälsomonitoreringssensorer, eller från ett headset till radio (eller Buret Krypto).

Idag kan soldaterna använda en trådlös PTT-knapp (*Push-to-talk*) på vapnet som medger att soldaten kan sända med gruppradion utan att släppa vapnet med händerna. Systemet har en hög robusthet mot störning på så sätt att soldaten kan använda själva radions PTT-knapp istället om den elektromagnetiska miljön förhindrar den trådlösa PTT-funktionaliteten.

Utmaningarna vid införandet av ett generellt WBAN-system för soldaten är flera, bland annat risken för upptäckt eller avlyssning av informationen, robusthet mot störning och interferenser. Informationen är i vissa fall av kritisk natur vilket kräver en hög tillgänglighet. Det finns ett flertal tekniska utmaningar, varav en gäller valet av frekvenser. Dessa

¹ WBAN – Wireless Body Area Network.

³ Satellitnavigeringshjälpmedel, GPS – Global Positioning System alternativt GNSS – Global Navigation Satellite System.

⁴ CBRN – Chemical, Biological, Radiological and Nuclear.

måste vara tillåtna globalt, i alla framtida operationsområden, och ge möjlighet att använda en stor bandbredd som kan medge höga datakter och samtidigt ge en hög robusthet.

1.2 Syfte och mål

Den huvudsakliga motiveringen för att införa WBAN-system på soldaten är att reducera vikt och storlek på soldatens utrustning, genom att ersätta kablar och kontaktdon med små, lätta och strömsnåla radiosystem. En förutsättning är då att ett WBAN inte väsentligt minskar tillgängligheten (robustheten) eller säkerheten i systemet.

Ett annat viktigt motiv är att det öppnar upp för bättre placering av vissa sensorer, där behovet av kabel tidigare har omöjliggjort bland annat placering på hjälmen, vapnet eller kängor. Sådana placeringar kan ge en förbättrad förmåga, exempelvis i form av högre noggrannhet vid akustisk lokalisering av prickskytt eller navigeringsförmåga i GNSS-störda miljöer.

De huvudsakliga målen med arbetet har varit att:

- höja kunskapsnivån rörande förutsättningarna för att införa WBAN-system i militära applikationer,
- beskriva användarnas behov av WBAN-system,
- identifiera kvarstående frågeställningar som är kritiska för ett eventuellt införande, främst när det gäller säkerhet, robusthet och smygegenskaper,
- samt ge rekommendationer för fortsatt arbete.

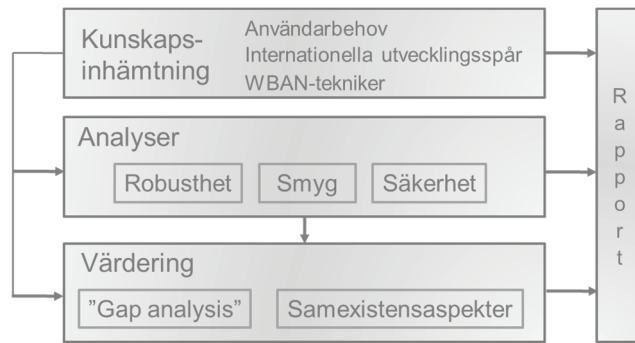
1.3 Studiens upplägg

Projektet har genomförts i form av en bred förstudie där målet bland annat har varit att ge en inblick i teknikutvecklingen inom området, beskriva möjliga användningsområden och de olika applikationernas specifika förutsättningar och krav på exempelvis dataakt och informationssäkerhet. Initiala analyser av utvalda civila WBAN-system med avseende på de beskrivna användarbehoven genomförs även och en gapanalys lägger därefter grunden för de rekommendationer som ges i slutet av rapporten.

En stor mängd korthållsradiosystem finns beskrivna i litteraturen och i olika standarder (främst inom IEEE 802-serierna) och många system har utvecklats till produkter det senaste årtiondet. Det är dock troligt att dessa inte kommer att uppfylla soldaternas krav på robusthet, smygegenskaper och säkerhet då de har utvecklats med delvis andra mål och för andra tillämpningar. Därför ges även rekommendationer angående möjliga alternativa, eventuellt militärspecifika, tekniker som kan vara intressanta för framtida WBAN-system för soldaten.

Förstudien har genomförts i ett flertal olika arbetspaket, som beskrivs i figur 1.1. Arbetspaketen inkluderar (i) kunskapsinhämtning av användarbehov, internationella utvecklingsspår och olika WBAN-tekniker, (ii) initiala analyser av robusthet, smygegenskaper och säkerhet (generellt), samt (iii) värdering av brister hos befintliga tekniker matchat mot behoven och (iv) även initiala diskussioner kring samexistensaspekter rörande kommande soldatsystem. Översikten av tekniklösningar inkluderar även en kort genomgång av alternativ till traditionella radiobaserade lösningar.

Varje delområde har endast studerats översiktligt och syftet har främst varit att identifiera och beskriva de svårigheter som behöver adresseras innan WBAN-system kan införas i framtida soldatmaterielsystem.



Figur 1.1: Skiss av ingående arbetspaket.

1.3.1 Avgränsningar

I arbetet har befintliga och framtida möjliga soldatburna sensorer identifierats, men vissa intressanta framtida möjligheter har definierats som varande utanför fokus i denna studie. Det gäller bland annat små radiostyrda UAV:er (*Unmanned Aerial Vehicle*) med kameror som styrs av en soldat och skickas in i byggnad och sänder realtidsvideo tillbaka till soldaten (eng. *cargo-pocket ISR*). Sådana mikro-UAV:er används redan idag av militär i USA och Norge.

Inte heller kommunikation mellan soldaterna ingår i denna studie, även om vissa korthållsradiotekniker även kan användas för att skicka stora mängder data (exempelvis realtidsvideo) mellan soldater som befinner sig nära varandra.

1.3.2 Rapportens disposition

I kapitel 2 ges en beskrivning av utvecklingen av möjliga framtida soldatburna sensorer på kort och lång sikt. En beskrivning av de användarbehov som förutses, samt exempel på generella krav på ett WBAN som har identifierats i studien, ges i kapitel 3. En översikt av alternativa tekniker för informationsöverföring som kan vara av intresse för militära WBAN beskrivs därefter i kapitel 4. Initiala analyser av robusthet och smygegenskaper för olika tekniker, som efterliknar de som anges i standarden IEEE 802.15.6, ges i kapitel 5. Analysen baseras på de i kapitel 3 uppskattade kraven på robusthet mot störning och önskade smygegenskaper. I kapitel 6 diskuteras generella säkerhetsaspekter för WBAN-system. Slutligen, i kapitel 7 och 8, genomförs en sammanfattande gapanalys och rekommendationer för designprinciper och fortsatta studier som kan bana väg för ett eventuellt införande av ett militärt WBAN-system ges.

2 Sensorer för soldattillämpningar

Utvecklingen av soldatburna sensorer på kort och lång sikt beskrivs i detta kapitel. Försvarmakten har tidigare genomfört ett omfattande studiearbete riktat mot utvecklingen av ett modernt soldatsystem. Diskussionerna i denna rapport som berör sensorer och förmågor som är önskvärda i ett framtida soldatsystem inkluderar dessa arbeten.

När det gäller vilka soldatburna sensorer som är aktuella både på kort sikt och i ett perspektiv bortom 2025 så har vi även hämtat inspiration från den civila utvecklingen. Dessutom har de arbeten som genomförs av US Army RDECOM och deras Natick Soldier Systems Center studerats (se exempelvis följande presentationer och rapporter: [2]-[4]).

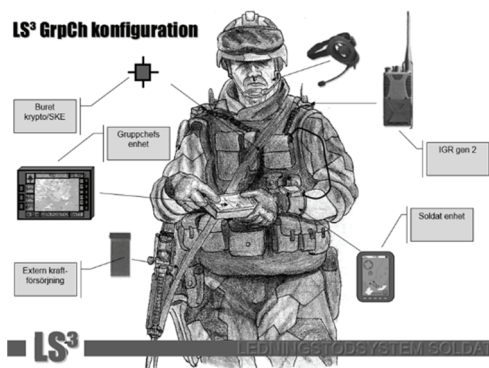
2.1 Soldatsystemets utveckling och inriktning

De olika MARKUS-studierna som genomförts resulterade i ett antal handfasta och konkreta rekommendationer beträffande den önskade utvecklingen, på kort och medellång sikt, av det svenska soldatsystemet.

I [1] gavs rekommendationen att som ett första steg fokusera på soldatens förmåga genom att införa: (i) radiokommunikation inom grupp, (ii) förmåga till mörkerstrid, samt (iii) grafiskt stöd för positionering. Därefter rekommenderades att gruppens förmåga utvecklas genom: (i) dataöverföring, (ii) dygnet runt förmåga med gruppens vapen och (iii) målnmätning för invisning och precisionsbekämpning. Som steg tre föreslogs sedan att fullfölja utvecklingen inom de prioriterade områdena IK-system, nytt eldhandvapensystem, vapen med verkansmöjlighet bakom skydd samt videoöverföring nära realtid.

Flera av dessa rekommendationer har redan införts och resterande åtgärder ger en tydlig och logisk inriktning av hur arbetet bör fortsätta i takt med att ekonomin tillåter. Överföring av rörliga bilder har troligen nedprioriterats men i övrigt verkar dessa rekommendationer vara fortsatt aktuella.

Ett ledningsstödsystem för soldaten ses fortsatt som en önskvärd framtida komponent i den fortsatta utvecklingen, se skiss i figur 2.1. Det medger dels införandet av utpekade prioriterade förmågor såsom lägesuppfattning och snabb delning av mål. Det möjliggör även en fortsatt utveckling av soldatburna automatiserade sensorer där exempelvis prickskytte-lokalisering, CBRN-detektion och fysiologiska sensorer kan anslutas och presenteras för soldaten samt automatiskt och snabbt förmedlas vidare. Det utgör därmed en möjliggörare för utvecklingen mot ett mer integrerat soldatmaterielsystem. Däremot är bedömningen i nuläget att det är tillräckligt att i ett första steg tillse att gruppchefer och ställföreträdande gruppchefer får denna förmåga.



Figur 2.1: Skiss av ingående komponenter i den gruppchefsconfiguration som föreslogs i PTTEM Ledningsstödsystem soldat (LS³). Illustration: Fredrik Herrlitz.

Av naturliga skäl ger dock ovanstående arbeten lite information om den önskade utvecklingen på längre sikt.

2.2 Möjliga soldatburna sensorer i närtid

I [2] och [5] beskrivs översiktligt de sensorer som är aktuella redan i det korta perspektivet, inkluderande

- Headset med mikrofon och hörlurar,
- användargränssnitt såsom display (*End-user device – EUD*), mörkersikten och musplattor,
- positionerings- och navigeringssensorer,
- datorer,
- vapensikten,
- trådlös PTT,
- fysiologisk monitorering och
- målinmätning.

Utvecklingen av bärbara sensorer ger redan idag möjligheten till kontinuerlig fysiologisk övervakning av ett flertal vitala faktorer. I [6] ges en översikt av utvecklingen av bärbara sensorteknologier (s.k. wearables) som kan vara lämpliga för framtida monitorering av främst soldaternas hälsa och status.

I tabell 2.1 ges en kort sammanfattande beskrivning av nya eller förbättrade förmågor som kan möjliggöras med soldatburna sensorer, de sensorer som behövs för att uppfylla de olika förmågorna, samt en beskrivning av kontext och behov av WBAN för dessa sensorer. Kravet på datatakt varierar kraftigt för olika sensortyper, från under 1 kbps för sensorer som ger positions- eller varningsmeddelanden, i storleksordningen 5 till 10 kbps för tal och över 10 Mbps för bildalstrande sensorer.

Tabell 2.1: Sammanställning av förmågor och sensorer, samt presentationshjälpmedel, som redan används eller kan vara möjliga att realisera inom 10 år. Datatakt: Låg: <1 kbps, Medel: 1-1000 kbps och Hög: >1 Mbps.

Förmåga	Sensorer	Beskrivning	Trafikmodell	Data-takt
Befintliga, alternativt tekniken mogen för användning 2020				
Gruppkommunikation (IGR)	Mikrofon och hörlurar	Eventuellt hjälmintegrerade i framtiden. Digitaliserat tal mellan headset och sammankopplingsenhet, radio eller buret krypto.	Kontinuerlig (under pågående talsession)	Medel
	PTT-transceiver	PTT-radiosändare på vapnet medger tal via radio utan att släppa vapnet. Ingen data skickas, förutom för autentiseringsändamål. Olika frekvenser anger vilken PTT-knapp (talgrupp) som valts.	Kontinuerlig (under pågående talsession)	N/A
Navigeringsstöd	GNSS-mottagare och digital karta	Fri sikt mot satelliterna önskvärd. Antennen typiskt integrerad i mottagaren (GPS08). Digital karta och GPS/GNSS-mottagare kan bli separerade fysiskt. GNSS-mottagare genererar positionsmeddelanden (enligt NMEA eller militär ICD-standard) 1 till 10 ggr per sekund.	Kontinuerlig, uppdatering på sekundbasis	Låg
	Bildförstärkare			Hög

Mörkerhjälp-medel	IR-värme-kamera	Hjälmmonterad eller buren. Internationellt används och/eller demonstreras vapenmonterade sensorer.	Kontinuerlig, under användning	
Skjuta runt hörn	Siktesmonterad kamera samt hjälmmonterad display	Vapenmonterad kamera och hjälmmonterad display, strömma realtidsvideo med inlagt "rödpointssikte".	Kontinuerligt, vid användning (hårda krav på låg fördröjning)	Hög
Lokalisering av prickskytt	Mikrofonarray	Riktning och (grovt) avstånd fås från varje separat sensorenhet. Hjälmmontering önskvärd, montering på axel vanligast idag.	Sporadiskt, vid detektion	Låg
Snabb målan-givelse	Vektorkikare eller motsvarande	Mäter avstånd och riktning till mål och överför dessa automatiskt till lednings(stöd)system. Handhållen utrustning	Sporadiskt, vid målinmätning	Låg
Fysiologisk monitorering	Pulsmätare	Mätning av medelpuls, pulsintervall, andningsfrekvens	Kontinuerlig alternativt varning vid detektion av avvikelser	Låg
	Andningstakt			
NBC-detektion	Radiometer	Varningsmeddelande och detektionsinformation Skydd mot strålning, smitta och gift	Sporadiskt, vid detektion	Låg
Tekniken mogen för användning 2025				
Autentisering	Biometrisk sensorer	Automatisk autentisering som ger möjlighet stoppa användning av personlig utrustning såsom radio, displayer som visar lägesbild, eller vapen för icke-auktoriserade personer. Exempelvis handledsburna sensorer (klockarmband).	Sporadiskt, vid detektion av godkänd autentisering	Låg
Navigering och positionering, i alla miljöer och vid GNSS-bortfall	GNSS-mottagare	Fri sikt mot satelliterna önskvärd och hjälm- eller axelmontering ger högre noggrannhet gentemot en inbyggd antenn. Extern antenn tros även bli vanlig i integrerade positioneringssystem.	Kontinuerlig, uppdateringstakt 1-10 Hz	Låg
	Tröghets-sensorer	Eventuellt samlokalisering med GNSS-mottagare, men fotmontering ger ökad noggrannhet. Rekommenderat att beräkna förflyttning (riktning och avstånd) sensornära och endast skicka dessa. Överföring av rådata till processor kan ge viss ökad noggrannhet men det ställer mycket höga krav på datatakt och robusthet.	Kontinuerlig, förflyttning (riktning och avstånd) på sekundbasis (alt. rådata från tröghetssensorer)	Låg (Hög)
	Bildalstrande sensorer	Möjliggör uppbyggnad av karta i realtid. Relativt hög strömförbrukning vilket ev. medför att sensorer, processor och batteri samlokaliseras.	Positionsmeddelanden på sekundbasis. (Eventuellt skickas byggnadsritning mellan noder på soldaten.)	Låg (Medel)
Användar-gränssnitt (inmatning)	Musplatta	Vapenmonterad ersättare till datormus. Experiment pågår i USA.	Kontinuerligt, vid användning	Medel
	Ögonföljande kamerasensor	<i>Eye-tracker</i> monterad i glasögon eller HMD (<i>Head-mounted-display</i>). Civil forskning driver området, ersättare till datormus.	Kontinuerligt, vid användning	Medel

Användar-gränssnitt (presentation)	Visuell display	Monterad i bröstficka, på underarm eller hjälm (HMD). Positioner och tillhörande attribut, och eventuellt karta, strömmas från processor/dator till display.	Kontinuerligt	Medel / Hög
	Hörlurar (3D-ljud)	Intuitiv förståelse av hotriktning eller riktning till egna enheter. Förutsätter att huvudets eller kroppens orientering kan estimeras. Stöd för lägesuppfattning, hörbarhet, hotriktning. Tal samt sporadisk information för navigeringsstöd (korridorsnavigering) eller endast lägesuppfattning.	Kontinuerligt (under pågående talsession)	Medel / Låg
	Taktil (haptisk)	Vibrationer uppmärksammar varningsmeddelanden eller som navigeringsstöd (typ navigering i mörker längs en förvald korridor). Integrerad exempelvis i bälte eller kläder.	Troligen sporadiskt, med 10-tals sekunder mellan event	Låg
Lokalisering av prickskytt	Mikrofon på varje soldat	Förutsätter samverkan (informationsutbyte) mellan flera soldater med mikrofon, möjliggör noggrannare lokalisering av skytt än individuella enheter. Hjälmmontage önskvärd, annan montering kan kräva multipla mikrofoner (typ mage/rygg).	Sporadiskt, vid detektion	Medel
Fysiologisk monitorering	Syresättning och blodsockerhalt	Olika sensoralternativ, exempelvis icke-invasivt med nära infrarött ljus (<i>fNIR – functional near-infrared spectroscopy</i>).	Kontinuerligt eller varning (vid behov)	Låg
	Temperatur	Kärntemperatur, eventuellt kroppintern (svald) sensor för mätning av inre temperatur (kärntemperatur).	Kontinuerligt eller varning	Låg

2.3 Möjliga soldatburna sensorer på längre sikt

I [4] presenteras en visionär bild av förmågor som kan vara möjliga att realisera på längre sikt. Delar av beskrivningarna kommer att vara svåra att realisera före 2030, speciellt då de behöver integreras till *ett* system. Det uttalade syftet med studien var dock att stimulera diskussioner om, och prioriteringar av, hur den framtida soldaten bör utrustas. Prioriteringar av önskade förmågor är kritiska då utvecklingen av dessa inte förväntas ske automatiskt av industrin utan kräver fokuserade forskningsinsatser.

2.3.1 Future Soldier 2030 Initiative

I [4] definieras sju områden där soldatens förmågor och system kan utvecklas:

- Soldatens prestanda och träning
- Soldatens skydd
- Verkan
- Mobilitet och logistik
- Soldatens nätverk
- Soldatens sensorer
- Soldatens strömförsörjning

I rapporten beskrivs exempelvis olika sätt att monitorera soldatens mentala och fysiska status med fysiologiska och beteendesensorer. En utveckling av det kulturella stödet är önskvärd, i form av automatisk översättning (både lyssna och prata), gestigenkänning och bedömning av möjliga hot och personers intentioner baserat på icke-verbal information.

Tredje generationens människa-maskin-gränssnitt beskrivs även, med handskar och dräkter för gestbaserad interaktion med exempelvis robotar, eller med talbaserad interaktion. Virtuella gränssnitt är av intresse, med korrekt positionsinformation och känslbaserad återkoppling. Automatiska moder (och modbyten) som ger användaren den information som behövs för den uppgift som ska lösas är en nyckel för att minska soldatens kognitiva belastning. Liknande tekniker utvecklades och utvärderades även i MUMSIS-projektet [7],[8]. Biometrisk ansiktsigenkänning är ytterligare en önskad förmåga, exempelvis i vägspärrar och vid måligenkänning.

Soldatens hälsostatus monitoreras kontinuerligt med små fysiologiska sensorer inbäddade i uniformen, vätskesystemet, kängor och hjälmen. De förväntas ge information om energistatus, arbetsbelastning, stressnivåer, sömn osv. Sår och skador kommer att upptäckas automatiskt och sår ska kunna självrengöras och förseglas medan inplanterade autoinjektorer ska kunna medicinera soldaten automatiskt, även mot kemiska och biologiska hot.

Alla soldater ska kunna mäta in mål och begära eldunderstöd genom direkt och indirekt eld. Elektrooptiska hyperspektrala hjälmmonterade sensorer/sikten med hög upplösning och förmåga att observera och följa mål/hot 360-grader runt soldaten ger möjlighet att följa och bekämpa multipla mål snabbt och effektivt under alla siktförhållanden. Soldaten ska även kunna få realtidsvideo från sensorer, UAV:er och satelliter för ökad lägesuppfattning.

Dessa förmågor förutsätter införandet av ett antal olika sensorer kombinerat med processorer och massiv signalbehandling. En utmaning är givetvis att ge soldaten rätt information utan att öka den mentala belastningen hos soldaten.

2.3.2 Övervakning av soldaten och dess omgivning

Ett stort antal forsknings- och utvecklingsprojekt sammanfattas i [6]. Den civila utvecklingen är extremt snabb och driver utvecklingen. Teknikerna delas grovt in i tre kategorier av bärbara sensorer: (i) medicinska sensorer (såsom klockor och armband), (ii) ”smarta tatueringar” och (iii) sensorer för monitorering av omgivning/miljö.

Medicinska sensorer innefattar bland annat Googles kontaktlinser för mätning av blodsockernivåer direkt från tårvätskan, olika sportarmband som mäter puls och fysisk aktivitet, samt medicinska armband⁵ som mäter puls, andning och syresättning. Dessutom utvecklas produkter riktade mot hälsomonitorering med textilintegrerade biometrisk sensorer såsom t-shirts och bröstband⁶ [9]. Smarta tatueringar, eller tunna, flexibla hudsensorer som appliceras likt tillfälliga tatueringar, ska i framtiden kunna mäta temperatur, puls, syresättning och andra vitala parametrar. Även sensorer inbäddade i plåster eller bandage utvecklas⁷. Genom analyser av personens svett kommer även elektrolytbalans, vätskeförlust, risken för värmeslag och annat kunna detekteras och predikteras. Här finns även exempel på vibrerande magnetiska tatueringar. Små portabla sensorer för monitorering av miljö och omgivning som ska kunna ge tidiga varningar för biologisk, kemisk eller radiologisk kontaminering är även under utveckling [6].

2.3.3 Diskussion

Ofta beskrivs i litteraturen koncept där det i framtiden finns två, eller flera, centraler på soldaten där det sitter sensorer och energiförråd. De vanligaste placeringsalternativen för dessa centraler är vapnet (t.ex. kamera, IR-sikte, ficklampa, avståndsmätare och rödpunktsikte), hjälmen (inkluderande kameror, hörlurar, radio, mikrofon, HMD och

⁵ Se exempelvis www.oxitone.com eller www.biovation.com

⁶ T.ex. Zephyr bioharness (www.zephyranywhere.com).

⁷ www.gentag.com

mörkerseende) och ett centralt energiförråd (batterier där man skulle kunna ansluta en CPU för datalagring/databearbetning och övervakning av energinivån).

Denna indelning är aktuell primärt för de sensorer som drar mycket energi. Enklare sensorer kan istället strömförsörjas av små knappcellsliknande batterier under veckor i sträck och de kan därmed placeras mer fritt på soldaten.

3 Analys av användarbehov

I detta kapitel ges en beskrivning av de användarbehov och exempel på generella krav på ett WBAN som har identifierats i denna initiala studie. Användarbehoven har främst identifierats genom inläsning av krav- och inriktningsdokument, bland annat [1],[10],[11], och genom interna diskussioner där möjliga framtida sensorer har identifierats och analyserats. Ett antal generella behov och krav som enligt vår bedömning även kan vara relevanta för framtida militära WBAN har även extraherats utifrån litteraturstudier av bland annat WBAN i medicinska och andra civila tillämpningar. Dessa berör främst robusthet mot störning och interferenser, smygegenskaper och säkerhetsaspekter.

Notera att de ”krav” som beskrivs nedan endast utgör av författarna beskrivna exempel som skulle kunna vara relevanta för framtida WBAN-system. Syftet med att beskriva dessa är främst att öka förståelsen för vilka egenskaper som vi tror att ett framtida WBAN bör ha och på så sätt möjliggöra en första gapanalys av befintliga tekniker.

3.1 Generell kravdiskussion

De viktigaste allmänna kraven på ett WBAN för soldattillämpningar diskuteras härnäst.

Systemet behöver vara självorganiserande då radiokanalen kan förändras mycket snabbt. Kanaldämpningen (*path loss*) kan variera kraftigt när delar av utrustningen eller kroppen kommer emellan sändaren och mottagaren. Ett annat exempel är om soldaten kastar sig i skydd på ett lerigt underlag, där delar av WBAN-noderna under denna tid skulle kunna utsättas för en mycket hög kanaldämpning.

Noder ska kunna tillkomma eller falla bort, exempelvis för att möjliggöra ett modulärt system som anpassas (konfigureras) inför operationen. Systemet behöver automatiskt kunna hantera detta på ett säkert sätt.

Systemet måste kunna hantera heterogena sensornoder med kraftigt varierande krav på datatakt, fördröjning, trafikmönster osv. Datatakterna kan variera från enstaka paket (50 till 100 bytes) vid oregelbundna intervall till realtidsöverföring av tal eller video (flertal Mbps). Vissa noder förväntas endast sända ett fåtal paket data vid enstaka tillfällen, såsom sensorer för skottlokalisering eller NBC-detektionssensorer, medan andra typer av noder förväntas sända information kontinuerligt. Den senare typen innefattar bland annat position och orientering för egennavigering och trådlös överföring av lägesbild till display.

Låg energiförbrukning är ett viktigt krav då det kraftigt påverkar vikt och storlek (batteri), men även soldatintegrationsaspekterna. Det är sannolikt svårt att få soldaterna att byta sensorer och/eller batterier regelbundet. En första ansats är att detta kan göras som mest en gång i veckan.

Tiden för att få soldaten redo för strid, där all utrustning ska tas på och aktiveras, kommer att vara begränsad. Detta medför att manuell uppstart av sensorer, autentisering mellan sensorer och centralenhet och eventuell laddning av kryptonycklar inte bör genomföras vid dessa tillfällen.

3.2 Exempel på krav som kan påverka WBAN

Följande krav är extraherade från kravdokument som är kopplade till utvecklingen av soldatsystemet, främst remissversionen av Systemmålsättning Soldatmaterielsystem [11]. MARKUS-studierna diskuterade kraven utifrån önskade förmågor hos soldaten i ett antal framtagna scenarion, såsom ledning, information & underrättelser, verkan, rörlighet, uthållighet och skydd. De föreslagna kraven i [11] baseras till viss del på tidigare genomförda MARKUS-studier (se [1],[10]). I tabell 3.1 ges en delmängd av kraven och en kortfattad analys av deras påverkan på WBAN-systemet.

Tabell 3.1: Delmängd av föreslagna krav på Soldatmaterielsystemet [11] och möjlig påverkan på ett WBAN.

Ref.	Formulering	Påverkan på WBAN
SMS-512	Soldatmaterielsystemet skall vara modulärt uppbyggt	Noder ska kunna tillkomma eller falla bort för att möjliggöra ett modulärt system som anpassas (konfigureras) inför operationen. Systemet behöver kunna automatiskt hantera detta på ett säkert sätt (med bland annat autentisering av noder).
SMS-970	Soldatmaterielsystemet skall kunna anpassas i förhållande till hot, miljö, uppgift och befattningar	
SMS-1234	Soldatmaterielsystemet skall vara konfigurerbart för olika typer av uppdrag och uppdragslängd upp till 72h med autonomt uppträdande.	Påverkar kraven på energiförsörjning där eventuellt batteriförsörjda sensorer och WBAN-noder måste kunna fungera utan byte av batterier, men även driftsprofiler i samband med analyser av eventuellt hälsofarliga strålningsnivåer från WBAN.
SMS-458	Kablar och kontakter i soldatens burna utrustning bör funktionellt och ergonomiskt integreras i uniforms-, skydds-, och/eller bärsystem.	Smarta textilier och kabelband bör användas i framtida trådbundna BAN.
SMS-795	Huvudmonterad utrustning utöver hjälm skall inte väga mer än 1 kg.	Inkl. WBAN vilket medför en kraftig begränsning i vikt på detta.
SMS-1224	Soldatmaterielsystemet skall ha full funktionalitet omedelbart efter avstigning ur farkost.	Innebär att systemet även behöver fungera inuti fordonet för att undvika uppstartsförfarande och -tider.
SMS-798	Personligt eldhandvapen bör kunna konfigureras för att kunna sikta och verka över murar eller runt husknutar utan att vitala delar av soldatens kropp är blottade för eventuella motståndare (t.ex. med periskop, kamera eller liknande).	Kan innebära kamera på vapnet med trådlös överföring av realtidsvideo till display (exempelvis på hjälmen).
SMS-238	Personlig observationsutrustning skall möjliggöra att soldaten kan lägesbestämma terräng, objekt och mål genom riktning och avstånd och/eller koordinater.	Förutsätter sensorer för mätning av avstånd och riktning.
SMS-259	Soldatmaterielsystemet skall ha stöd för att identifiera egna.	Olika alternativ finns, förutsätter sannolikt kombination av "markörer" och "sensorer" (t.ex. när-IR markör och mörkerhjälpmedel eller radiodaserad fråga/svar funktion)
SMS-258	Personlig observationsutrustning bör ha stöd för att kunna riktningsbestämma inkommande direktriktad eld nära realtid.	Kan lösas med sensorer för akustisk skottlokalisering.
SMS-261	Soldatmaterielsystemet bör möjliggöra upptäckt av nedgrävda och maskerade minor (t.ex. minsökare).	Sensorer för automatisk upptäckt är önskvärda, dock oklart om detta kan lösas med sensorer som är del av soldatens personliga utrustning.
SMS-866	Kommunikation ska kunna ske utan att eldberedskap med personligt vapen sänks.	Förutsätter användning av trådlös PTT (<i>push-to-talk</i>).
SMS-962	Ledningsstödssystemet skall kunna ange egen position (t.ex. med GPS).	Positioneringssensorer såsom GNSS-mottagare.
SMS-568	Soldatmaterielsystemet bör ha en funktion för varning mot aktiv belysning.	Sensorer för detektion av aktiv belysning förutsätts.
SMS-220	Soldatmaterielsystemet skall ha funktion för indikering av förekomst av CBRN-ämnen.	

SMS-1411	Soldatmaterielsystemet skall automatiskt indikera och i nära realtid varna för förekomst av CBRN-ämnen.	Sensorer för detektion förutsätts. Intensimeter/dosimeter. Gruppformåga. Idag med ljudsignal.
SMS-214	Soldatmaterielsystemet bör kunna hantera information med säkerhetsklass upp till nivå Hemlig/Secret enligt gällande FIB, lagar och förordningar.	Den övre gränsen som ett Buret krypto är kravsatt för att kunna hantera är Hemlig/Restricted och högre krav än så är inte aktuellt att anta för ett WBAN-system.
SMS-284	Dokumenterade stridsförlopp skall vara skyddade mot otillbörlig åtkomst.	Informationssäkerhet, kryptering.

3.3 Robusthets- och smygaspekter

I detta delkapitel diskuteras exempel på möjliga framtida hot, samt robusthets- och smygaspekter för framtida WBAN.

3.3.1 Exempel på hotbild

I de analyser av robusthet och smygegenskaper som genomförs i kapitel 5 har vi valt att genomföra analysen baserat på en hotbild bestående av relativt små störsändare och signalspaningsutrustning, som har enkla antennsystem och begränsade uteffekter.

Det första exemplet på den typen av hotbild utgörs av soldatburna system eller små radiosändtagare som placeras ut på exempelvis hustak. Den typen av system har sannolikt mycket begränsad riktverkan och antas i denna rapport ha uteffekter omkring 1 W.

Ett annat framtida hot avseende en tekniskt avancerad motståndares möjlighet att utföra signalspaning eller störning riktat direkt mot soldaternas WBAN rör en mini-UAV med en enklare gruppantenn som cirklar ovanför en stad på någon eller några hundra meters höjd. UAV:n kan då antas befinna sig under frisiktsförhållanden (*LOS - line-of-sight*) till soldaterna åtminstone delar av tiden. Analyser av robusthet och smygegenskaper bör därför baseras på antagandet om fri sikt mellan dessa.

3.3.2 Robusthetsaspekter

Systemet måste kunna hantera svåra interferensmiljöer, både avseende interferenser från elektronisk utrustning och egna radiosändare som kan vara placerade på soldaten eller i fordonet. Ett möjligt exempel på intersysteminterferens kan vara interferenser från Interngruppradion (IGR) som används för kommunikation inom gruppen. Vissa grupp-radiosystem använder frekvenser på 2.4 GHz som även används av olika WBAN-standarder. I många situationer befinner sig dessutom soldaterna inom en grupp mycket nära varandra, exempelvis uppsatt i stridsfordon eller vid rensning av byggnad.

Sammanfattning av möjliga krav rörande systemets robusthet mot interferenser:

- Systemet skall kunna användas avsatt och inuti stridsfordon.
- Systemet skall kunna fungera tillfredställande med all soldatens elektroniska utrustning igång.
- Systemet skall möjliggöra kommunikation mellan (minst) 10 enheter inom ett WBAN.
- Systemet skall ha full funktionalitet då (minst) 8 separata WBAN befinner sig inom en radie på 2 m.

Systemet skall även kunna hantera avsiktlig störning. Det är dock inte möjligt att designa ett WBAN som är omöjligt att störa ut, men det är viktigt att designa det så att realistiska

störscenarion rörande avstånd, kanalparametrar och störarens sändareffekt och antennsystem ändå kan hanteras. Robusthet mot avsiktlig störning kan erhållas bland annat genom bandspridningsmetoder (exempelvis i form av frekvenshopp eller direktsekvenskodning), adaptiv uteffekt och avancerade antensystem. Adaptiv uteffekt ger möjlighet att vid behov öka robustheten till priset av ett ökat upptäcktsavstånd.

Exempel på möjligt krav rörande systemets robusthet mot avsiktlig störning:

- Systemet skall fungera under störning med motsvarande en handhållen störsändare, eller från en sändare monterad på en mini-UAV, på ett avstånd över 200 meter.

3.3.3 Smygegenskaper

Sammanfattning av troliga krav rörande systemets smygegenskaper:

- Systemet skall inte kunna upptäckas på avstånd över 200 meter med motsvarande en handhållen mottagare eller en mottagare monterad på en mini-UAV.
- Systemet bör kunna övergå i en ”smygmod” där alla för operationen icke-kritiska informationsvägar stängs av helt och där kritiska länkar endast använder lägsta uteffekt och största tillgängliga bandspridning. I smygmod bör systemet inte kunna upptäckas på ett avstånd större än 50 meter med motsvarande en handhållen mottagare eller en mottagare monterad på en mini-UAV.

För att kunna uppnå goda smygegenskaper och samtidigt ett system som har en hög robusthet krävs sannolikt att systemet är adaptivt avseende exempelvis uteffekt och bandbredd.

3.4 Informationssäkerhet

Det är sannolikt att informationssäkerhetsklassen för informationen som ska överföras från de olika sensorerna eller till presentationsgränssnitten kommer att variera. För en display som ska visa till exempel lägesbilden innehållande mål och egna enheters (soldater och fordon) positioner så kommer den information sannolikt bli klassificerad som Hemlig / Restricted.

I USA utreds exempelvis möjligheten att överföra all information till displayen via ett WBAN istället för kabel till deras användargränssnitt i NettWarrior-konceptet. Det innebär att ett säkerhetsgodkänt WBAN behöver tas fram och användas om liknande information ska skickas i ett svenskt system. Ett NSA-godkänt (*National Security Agency*) militär-specifikt WBAN, benämnt ISW⁸ (*Intra-Soldier Wireless*), utvecklas i USA, lett av US Army CERDEC och Natick Soldier Systems Center [4]. ISW beskrivs närmare i delkapitel 4.1.2.1.

Viss sensorinformation kan bedömas vara öppen men ändå vara av känslig natur på grund av personliga integritetsskäl, såsom hälsomonitoreringssensorer. Det finns även sensorinformation som sannolikt inte är av känslig natur, exempelvis rådata från tröghetssensorer eller PTT-funktionalitet till radion som inte innehåller någon information.

Det är därmed troligt att ett framtida WBAN för soldaten behöver hantera olika nivåer av informationssäkerhet.

3.5 Hälsorisker

Systemet får inte vara hälsofarligt att använda under typiska driftprofiler. Här avses i huvudsak den mängd energi som kroppen absorberar (och omvandlar till värme) från

⁸ <http://www.govcb.com/A-THIS-IS-A-REQUEST-FOR-INFORMATION-ADP13975914630000298.htm>

radiovågor och mäts för varje sekund per kilogram. Måttet benämns SAR (*Specific Absorption Rate*) och gränsvärdet är satt till en nivå som bedöms vara långt under de nivåer där det finns säkerställda hälsorisker.

Gränsvärdet för hur mycket kroppen maximalt får absorbera från radiosändare i frekvensbandet 100kHz till 10 GHz är i EU satt till 2 W/kg kroppsvävnad lokalt i huvud och överkropp mätt i tio gram vävnad (i USA är gränsvärdet istället 1.6 W/kg i ett gram). Detta motsvarar maximala sändningseffekter på 20 mW i EU (1.6 mW i USA) [12]. I medel för hela kroppen är ett maximalt värde på 80 mW/kg angivet. Som jämförelse kan nämnas att gränsvärdet för SAR för mobiltelefoner är satt till 2 W/kg⁹.

Som typiska driftsprofiler för analyser av ackumulerade nivåer används lämpligen de driftsprofiler som anges i Systemmålsättning Soldatmaterielsystem, där exempelvis soldatmaterielsystemet under insats används 140 timmar under en medelvecka. I [11] anges att *“Soldatmaterielsystemet skall vara konfigurerbart för olika typer av uppdrag och uppdragslängd upp till 72h med autonomt uppträdande”* (SMS-1234).

3.5.1 Diskussion

Noggrannare analyser av eventuella negativa hälsoaspekter bör genomföras innan ett WBAN implementeras. Analysen bör baseras på de arbetsmiljökrav som gäller inom Försvarsmakten.

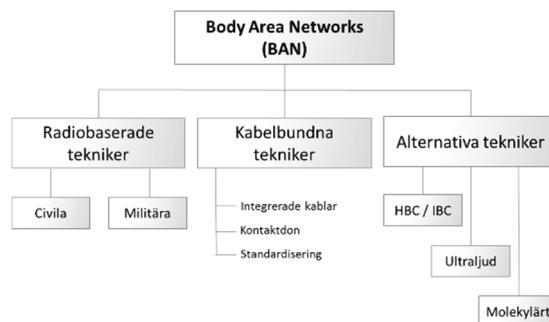
De civila WBAN-systemen är designade för användning på licensfria band där uteffekter (normalt mindre än 0.1 W) och s.k. *duty-cycle* är kraftigt begränsade. De har även hårda krav på låg energiförbrukning. De utsända effekterna är betydligt lägre än för mobiltelefoner som i perioder kan sända med 1-2 W. Däremot kan ett större antal WBAN-noder komma att användas och adaptiv uteffekt kan komma att användas för ökad robusthet, vilket bör inkluderas i analyserna.

Olika designval påverkar SAR-nivåerna, bland annat när det gäller antenn där både antenntyp och dess direktivitet. Magnetiska antenner (exempelvis loopantenner) genererar E-fält som mestadels är riktade längs med kroppen och tros därmed orsaka mindre uppvärmning än elektriska antenner [12].

⁹ www.stralsakerhetsmyndigheten.se

4 Tekniköversikt

I detta kapitel ges en översikt av olika alternativa tekniker för informationsöverföring. En översikt av indelningen i olika tekniker som diskuteras ges i figur 4.1. Där beskrivs militära och civila radiobaserade och kabelbaserade tekniker och andra alternativ såsom HBC (*Human Body Communications*), ultraljud och molekylär kommunikation. En bra översikt av WBAN-området ges i [13].



Figur 4.1: Översiktlig indelning av kommunikationstekniker (inspirerad av [21]).

4.1 Trådlösa korthållsradiönät (WBAN/WPAN)

I rapporten används normalt benämningen WBAN men i litteraturen används även uttrycket WPAN (*Wireless Personal Area Network*) för radiosystem som ofta har en lite längre räckvidd men som även kan användas i vissa WBAN-applikationer. I civila system har uttrycket WBAN de senaste åren främst kommit att beteckna system som följer standarden IEEE 802.15.6. Standarden är utvecklad för kommunikation till/från sensorer inuti, på och till viss del även runt kroppen och den är främst avsedd för medicinska tillämpningar.

4.1.1 Civila system

Det finns ett mycket stort antal trådlösa korthållsradiosystem som har föreslagits i forskningsartiklar, utvecklats till standarder och som implementerats i färdiga produkter (se [12]–[14] och referenserna där). Vi har i denna studie velat täcka flera alternativa frekvensområden och även poängtera soldaternas krav på låg vikt, lågt pris och energieffektivitet. Därför fokuseras analyserna på frekvenser och andra parametrar som liknar de som anges i den nya standarden IEEE802.15.6 [15]. Standarden möjliggör användning av ett flertal olika frekvensband, datatakter och en rad andra parametrar och egenskaper. Även kommunikation på låga frekvenser med hjälp av HBC-tekniker beskrivs i standarden, så den innefattar även ett stort antal möjliga tekniklösningar.

Olika WPAN-alternativ såsom BLE (*Bluetooth low energy*), ZigBee (som baseras på standarden IEEE802.15.4), Z-Wave (framtagen för hemautomationstillämpningar) och andra system har normalt en betydligt högre energiförbrukning i jämförelse. Som exempel kan nämnas att den enkla jämförelse av energiförbrukningen för ZigBee, UWB-system (*Ultra Wideband*) och HBC som beskrivs i [16] visade på strömförbrukningar på 106 nJ per översänd bit (vid 250 kbps), 2.5 nJ per bit (vid 16.7 Mbps) och 0.24 nJ per bit (upp till 10 Mbps) för dessa tre alternativ. Även om dessa beräkningar baseras delvis på forskningsprototyper och inte innefattar alla förbrukningskällor så ger de fortfarande en indikation av teknikernas potentiella strömförbrukning. Både UWB och HBC har potential att kraftigt reducera strömförbrukningen i jämförelse med tidigare framtagna WPAN-tekniker.

4.1.1.1 IEEE802.15.6

I standarden IEEE 802.15.6 anges olika tekniker (de s.k. fysiska och accesslagren beskrivs) för kommunikation, såsom (i) smalbandig kommunikation (NB) på olika frekvensband vid 400, 800 och 900 MHz samt vid 2.4 GHz, (ii) bredbandig kommunikation med UWB-tekniker mellan 3.1 och 10.6 GHz, samt (iii) E-fältskommunikation (HBC) som använder sig av frekvenser mellan 5 och 50 MHz [17]. Kommunikationsavstånden är designade för att klara upp till två meter. Strömförbrukningen bedöms ligga runt 1 till 10 mW men den påverkas av en mängd faktorer, exempelvis dataakten.

De respektive systemens olika fysiska lager kan kort beskrivas som (baserat på [18]):

- *NB*: Informationsdataakter kan konfigureras mellan 50 och 500 kbps. Modulationsformerna DPSK (*Differential Phase Shift Keying*) används förutom vid 400 MHz där GMSK (*Gaussian Minimum Shift Keying*) används. NB använder öppna frekvensband vilket kan resultera i kraftiga intersysteminterferenser.
- *HBC*: E-fältskommunikation, centrerad runt 21 MHz med en maximal dataakt på ungefär 1.3 Mbps. (Tekniken beskrivs i delkapitel 4.3.1.)
- *UWB*: Avsedd för att uppnå höga dataakter med en låg komplexitet och låg energiförbrukning. UWB stödjer 11 olika kanaler med bandbredd på 499.2 MHz. Både impulsradio (IR) med av/på- eller fasskiftsmodulation och en bredbandig frekvensmodulerad signal stöds av standarden. Dataakter mellan 0.5 och 10 Mbps kan användas. Uppfyller MICS-bandets (*Medical Implant Communications Service*) hårda krav på utsänd effekt som bedöms vara säker för människan.

Utöver ovanstående palett av alternativ för det fysiska lagret anger standarden även flera olika alternativa accesstekniker. Det medför att det enbart inom denna standard finns ett stort antal alternativ att beakta. Mer information om dessa tekniker finns bland annat i [15],[17],[18].

4.1.2 Militärspecifika system

I den genomförda litteraturstudien har inte information om färdigutvecklade säkra militärspecifika WBAN eller WPAN hittats. I USA har forskning och utveckling rörande olika tekniker för trådlös överföring av sensorinformation bedrivits sedan BBN Technologies utvecklade BodyLAN i mitten av 1990-talet och det är ett av de tidigaste exemplen på ett WBAN/WPAN [19]. Ett annat exempel på forskningsprojekt är överföringen av realtidsvideo från vapensikten till en HMD (Natick Soldier Systems Center) bedrivits i SPINE-projektet (*Soldier Planning Interfaces and Networked Electronics*) (se [2],[3],[20] och figur 4.2).

Utvecklingen i USA går mot att utveckla ett eget militärspecifikt WBAN/WPAN som även ska kunna överföra hemlig information [3].

4.1.2.1 Intra-Soldier Wireless (ISW)

Huvudsyftet med ISW anges vara att minska integrationsproblemen och vikt/storlek för soldaten, vilket ska avlasta soldaten och därmed medge en ökad mobilitet, rörelsefrihet och uthållighet. Arbetet drivs av US Army Communications Electronics Research & Development Engineering Center (CERDEC) Space & Terrestrial Communications Directorate (S&TCD) och Natick Soldier Systems Center. Under 2014 efterfrågade de information från industri inom detta område (ett s.k. *sources-sought*¹⁰), med bland annat följande beskrivningar:

¹⁰ <http://www.govcb.com/A-THIS-IS-A-REQUEST-FOR-INFORMATION-ADP13975914630000298.htm>



Figur 4.2: Exempel på utveckling av prototyp för hur realtidsvideo kan överföras från vapnets sikten till en HUD, i detta exempel från FWS-I (*Family of Weapon Sights Individual*) till ENVG-III (*Enhanced Night Vision Goggle*) [2].

“CERDEC S&TCD will initiate a technology development program “Intra-Soldier Wireless” ISW. The ISW program will focus on adapting the Ultra-WideBand (UWB) commercial wireless technology to meeting current Army requirements to wirelessly link ancillary devices worn or used within a dismounted soldier. In its final form ISW will provide an embeddable miniaturized Application Specific Integrated Circuit (ASIC) secure tactical WPAN for the dismounted soldier. This will allow for the wireless communication and data transfer of the various devices and peripheral equipment on the soldier. An example is to wirelessly link the weapons sight to the head mounted display. Metrics for success include; unburdening the soldier, increasing freedom of maneuver, improving soldier situational awareness, and increasing soldier mobility.”

ISW ska kunna trådlöst koppla ihop soldatburna komponenter såsom användargränssnitt (t.ex. *NettWarrior End User Device, EUD*), hjälmmonterad display, radio, headset, vapenmonterad mus, PTT-omkopplare, olika kroppsburna biosensorer (främst för hälsostatusövervakning) och andra sensorer som kan vara placerade på olika ställen på soldaten. Fokus är på att utveckla ett system som är robust, har goda smygegenskaper och hög robusthet mot störning. Det måste även kunna hantera hemlig information (*“Secret and Below”*). ISW ska även uppfylla soldaternas hårda krav på storlek, vikt och energieffektivitet, samt säkerställa att strålningsnivåerna är under gränsvärdena vid användning mer än 24 timmar i sträck.

Fokus gällande teknikval är att anpassa kommersiell trådlös UWB-teknologi för att möta kraven avseende exempelvis robusthet och smygegenskaper. ISW ska kunna skicka både tal och data, där sensordata, bilder och video är aktuellt. Ambitionen är även att hantera både punkt-till-punkt och punkt-till-multipunkt dataöverföring [2].

4.2 Trådbunden kommunikation (BAN)

Det finns givetvis flera fördelar med att även fortsättningsvis använda kablar för kommunikationen till och från sensorer, processorer och användargränssnitt. Möjligheten att samtidigt hantera strömförsörjningen av sensorerna via samma (alternativt en parallell) kabel, smygegenskaperna kombinerat med den höga informationssäkerheten, är några av de absolut viktigaste. Flera forsknings- och utvecklingsprojekt har genomförts internationellt det senaste årtiondet, främst i USA, med syftet att försöka reducera vikt och robusthet (exempelvis lösa kablar som fastnar och går sönder) för dessa BAN.

4.2.1 Utvecklingstrender i närtid

Det är i trådbundna BAN-sammanhang vanligt att diskutera begreppen data- och energiöverföring tillsammans. Eftersom alla sensorer kräver någon form av energiförsörjning är det praktiskt att sensorn strömförsörjs med samma kablage som informationen från sensorn sänds igenom.

Det finns huvudsakligen två inriktningar inom forskning och utveckling. Den ena berör själva hårdvaran, dvs. sensorer, kablar, kontakter och strömförsörjning och den andra fokuserar på mjukvaran som behövs för att få sensorerna att kommunicera med varandra och omvärlden på ett säkert, tillförlitlig och energisnålt sätt. Då det krävs olika kompetenser verkar utvecklingen inom områdena bedrivas delvis oberoende av varandra.

4.2.1.1 Möjliga systemkoncept

Ofta beskrivs i litteraturen om trådbundna BAN koncept där det i framtiden finns två, eller eventuellt tre, centraler på soldaten där större och tyngre sensorer är samplacerade. Enklare sensorer som kan strömförsörjas av små knappcellsliknande batterier under veckor i sträck kan dock placeras mer fritt på soldaten.

Det är inte klart var på kroppen huvudbatteriet bör placeras, men utvecklingsprojekt i USA använder sig av konforma batterier, med något böjda batterier som bättre passar kroppens form, som placeras i sidfickor i stridsvästen. Systemet kallas för SWIPES (*Soldier Worn Integrated Power Equipment System*) och har utvecklats av Arotech tillsammans med US Army. En uppdaterad version benämnd SWIPES II PD^{11,12} har även kablage för dataöverföring integrerat i västen. Tekniken finns tillgänglig men det hanterar endast dataöverföring på soldatens överkropp, inte information från hjälm- eller vapenmonterade sensorer.

Vapnet kan utrustas med ett batteri som försörjer påkopplade enheter med energi genom exempelvis en strömförande s.k. *Picatinny* räls. Ett robust alternativ för dataöverföringen mellan vapnet och soldaten saknas dock ännu. NATICK Soldier Center har arbetat med att utveckla ett trådlöst WBAN för överföring av realtidsvideo och siktesmarkering (mot-svarande rödpunktssikte) från vapnets olika kameranikten till soldatens HMD (*Helmet-mounted-display*). En sådan lösning ställer höga krav på datatakt och låg fördröjning, vilket kan göra det svårt att uppfylla krav på smygegenskaper och eventuell kryptering. Skulle handskar med insydda kablageband eller textilremmar kunna utvecklas till ett alternativ?

4.2.1.2 Kablar

Det har rapporterats [21] att införandet av integrerade kablar och valfritt placerade kontakter kan medföra mycket kortare kablar och därmed sänker soldatens burna last med upp till ett kilogram. Genom s.k. *wire-integrated textile cabling* skyddas kablarna mot nötning och mekaniska skador vilket innebär att isoleringen kan reduceras med bibehållen prestanda.

Ett exempel på existerande textilliknande kablar för kombinerad energi- och dataöverföring, med möjlighet till datatakt upp till ca 10 Mbps, är Textro-Interconnects¹³. De är platta, flexibla i formen och sy- och tvättbara, vilket kan göra det möjligt att integrera dessa på en uniform eller stridsväst.

4.2.1.3 Kontakter

Kontakterna utgör en viktig del av ett BAN-system. I samarbete med NATICK Soldier Center har företaget Physical Optics Corp. tillverkat och testat två typer av lågprofilkontakter. Den s.k. SNAPNET-kontakten¹⁴ finns i två varianter, för (i) energi och dataöverföring enligt USB2.0 standarden (upp till 480 Mbit/s) och för (ii) RF signaler upp till 6 GHz (RG188 koaxialkabel). Kontakten är liten och smidig (ca 15 mm x 4.5 mm) och den har testats enligt MIL-STD 810G och 461F. Kontakten kan placeras var som helst på ett klädesplagg som innehåller integrerade kablar och kan kopplas in/ur med bara en hand.

¹¹ <http://www.efbpower.com/SWIPES/SWIPES2PD/>

¹² <http://www.sdle.co.il/AllSites/810/Assets/jeff%20jubin%20-%20electric%20fuel.pdf>

¹³ <http://www.textronicsinc.com/products/textro-interconnects>

¹⁴ http://www.poc.com/media/23737/snapnet_datasheet_fnl_10.16.13.pdf

Fungerande prototyper för militärt bruk har tillverkats men det är oklart om detta ännu är en mogen (tillräcklig fysisk robusthet) teknik.

4.2.2 Utvecklingstrender bortom 2020

Redan idag utvecklas prototypsystem med platta kablar som integreras i band eller textilremmar som sys in i kläder och uniformer, samt stickade textilier med ledande trådar som sys ihop till ett klädesplagg. Det senare alternativet påstås vara mycket robust och kunna tåla stor fysisk åverkan med bibehållen funktionalitet så länge det finns mer än 10 % av textilen kvar. Denna utveckling bedöms vara intressant för framtida soldattillämpningar. En utmaning som kvarstår att lösa är standardisering av dataprotokoll och kontakter mellan sensorer och uniform.

Winterhalter et al [22] rapporterade 2005 om deras arbete som genomförts inom US Army FFW (*Future Force Warrior*) konceptet riktat mot dataöverföring genom integrerade kablar och optisk fiber. Praktiska försök gjordes för att tillverka bland annat en åtsittande T-tröja innehållande en spiral databuss för användning tillsammans med kroppsnära hälsosensorer. De utvecklade kablarna utvärderades enligt gällande industristandarder för (i) risker avseende *RF hazard and safety* och (ii) prestanda för USB2.0 dataöverföring. Även tester av robusthet (nötning och mekanisk belastning) gjordes med tillfredställande resultat. Det är möjligt att dessa, eller liknande, kablar kan komma att användas tillsammans med SWIPES systemet. De trådar och optiska fibrer som användes är kommersiellt tillgängliga produkter.

I ovanstående exempel är sannolikt TRL-nivån (*Technology Readiness Level*) omkring 6.

4.2.2.1 Diskussion

I situationer då soldaten behöver skicka information från vapenmonterade sensorer så håller denne sannolikt i vapnet. Detta skulle kunna möjliggöra överföring av data från vapnet till soldaten med hjälp av insydda kabelband och smarta textilier (handskar och uniform). Om soldaten alltid bär handskar är dock oklart, men trenden pekar mot mer användande av heltäckande skydd pga. risk för kemiska hot samtidigt som utvecklingen inom materialteknikområdet pekar mot ”lättare, tunnare och mer flexibla” textilier med bättre taktiska egenskaper. Redan idag finns handskar som är kompatibla med pekskärmar och sådana handskar kan framöver behövas även för soldaten. Den stora utmaningen i denna approach är dock överföring av data mellan handsken till uniformsjackan om kablar inte kan accepteras mellan dessa.

Genom att införa ett standardiserat kommunikationsprotokoll och förintegrerade kontakt-don på exempelvis stridsväst, uniformsjacka- och byxor och handskar skulle det kunna vara möjligt att designa ett säkert BAN som kan uppfylla de flesta av användarkraven. Sensorerna bör då kunna kopplas in enkelt via ett *plug-and-play* koncept. Detta förutsätter dock att kontakterna kan göras små och enkla men ändå robusta mot fysisk åverkan. Vid diskussioner med personal på Markstridsskolan framhålls att kablage till/från exempelvis hjälm och vapen inte är önskvärt vilket medför att trådlös dataöverföring sannolikt kommer att behövas som ett komplement även i framtiden.

4.3 Alternativa trådlösa tekniker

Tre alternativa trådlösa tekniker beskrivs i detta delkapitel. De är sannolikt inte intressanta i närtid men speciellt E-fältskommunikation i närfältet med kapacitivt kopplade HBC skulle kunna utvecklas till ett intressant alternativ på längre sikt. Ultraljud och molekylär kommunikation verkar främst vara lämpligt för kommunikation med sensorer inuti kroppen, alternativt för hudmonterade eller hudintegrerade sensorer liknande de smarta tatueringar som beskrevs tidigare.

4.3.1 Kommunikation med kroppen som överföringsmedium

Kroppen består till stor del av vätska och kan därmed användas för att överföra elektriska signaler. Forskning pågår inom flera olika alternativa sätt för att överföra information genom att använda kroppen som överföringsmedium. En introduktion till området ges i [16] medan [23] beskriver de inblandade utbredningsmekanismerma, elmiljöaspekter och även ger en bild av systemaspekterna på ett bra sätt. Där används samlingsnamnet *Intra-Body Communications* (IBC), varav HBC som ingår i IEEE 802.15.6-standarderna ingår. De flesta IBC-tekniker baseras på kapacitiv eller galvanisk koppling. En jämförelse av egenskaperna för dessa två tekniker ges i tabell 4.1.

Båda alternativen har goda smygegenskaper. Ett galvaniskt kopplat system är sannolikt mycket svårt att avlyssna eller detektera då det förutsätter direktkontakt med personen. E-fältskommunikation med låga sändningseffekter har sannolikt även det mycket goda smygegenskaper då E-fältet avtar betydligt snabbare med avståndet än andra RF-tekniker. Kapacitivt kopplade system är sannolikt att föredra då det inte förutsätter direktkontakt med huden utan eventuellt även kan fungera för noder på uniform osv.

Tekniken är intressant då den ger möjlighet till utmärkta smygegenskaper men det i dagsläget oklart när tekniken kan vara tillräckligt robust för ett militärt WBAN.

Tabell 4.1: Jämförelse mellan egenskaper vid kapacitiv och galvaniskt koppling [16].

Egenskap	Kapacitiv koppling	Galvanisk koppling
Kommunikationsprincip	E-fältskommunikation (elektriska fält)	Vägledare
Beskrivning	Signalen genereras mellan två sändtagare (elektroder) genom att generera strömloop genom en extern jordpunkt. Den inducerade elektriska signalen kontrolleras av en elektrisk potential och kroppen agerar som en ledare med jorden som returväg.	En elektrisk signal (växelström) mellan två elektroder i sändaren. Signalen propagerar huvudsakligen mellan elektroderna men en dämpad signal kan även tas emot med två mottagarelektroder. Den svaga strömmen resulterar i en signal som är olika i de två mottagarelektroderna.
Signalstyrning	Elektrisk potential (statiskt laddad elektrod)	Växelström över minst två elektroder
Dominerande signalväg	Omgivningen	Kroppen
Omgivningspåverkan	Ja, både brus och interferenser	Nej (endast kroppen)
Förutsätter hudkontakt	Nej, elektrod i närheten är tillräckligt	Ja

4.3.2 Ultraljud

WBAN som använder ultraljud (på icke-hörbara frekvenser) som kommunikationsmetod, främst avsett för kommunikation med sensorer inuti kroppen, beskrivs i [24],[25]. En av fördelarna är att mindre värme absorberas i kroppen. Kroppen består normalt av runt 2/3-delar vatten och det är ett medium där radiosignaler dämpas snabbt men där ultraljud fungerar betydligt bättre. Ultraljud används bland annat i undervattenskommunikations-tillämpningar.

Ultraljudsignaler som sänds genom kroppen utsätts för flervägsutbredning orsakat av reflektioner i skelettdelar och spridning av signalen. Kroppens densitet varierar och så gör även signalens hastighet. I [25] föreslås därför ett bredbandigt ultraljudskommunikations-system baserat på sändning av korta pulser, liknande impulsradio UWB, där pulserna är så korta så att de kan lösa upp flervägsutbredningskomponenterna enkelt.

Ultraljud skulle eventuellt kunna utgöra ett alternativ för kommunikation med sensorer inuti kroppen, men det är sannolikt inte ett alternativ för sensorer som placeras på kroppen i en militär applikation.

4.3.3 Molekylär kommunikation

Nanotekniken har banat vägen för ett nytt forskningsområde med inriktning mot medicinska WBAN, s.k. *Nano Communication Networks (NCN)*. Molekylär kommunikation möjliggör koordinerade aktioner för bio-nanomaskiner i vätskefyllda miljöer såsom inuti kroppen. Biologiska molekyler används för att bära informationen samtidigt som de även kan utgöra själva informationen. Exempel på applikationer som nämns i forskningen berör främst det biomedicinska området, såsom implanterbara system för tillförsel av medicin (riktad mot exempelvis tumörer), biohybridimplantat och liknande [13]. Dessa system är främst avsedda för (långsam) kommunikation med mycket små nanoroboter där biokompatibilitet är centralt.

TRL-nivåerna (*Technology Readiness Level*) är dock fortfarande på en låg nivå för detta område och det är oklart om det kan komma att utgöra ett reellt alternativ för militära WBAN annat än i ovan beskrivna applikationer.

5 Analys av robusthet och smygegenskaper

En initial analys av olika WBAN-alternativs robusthet och smygegenskaper har genomförts. Vi har valt att analysera olika frekvensområden med parametrar som efterliknar de som anges i IEEE 802.15.6-standard. I analysen jämför vi gränser för sändareffekt för tänkta kommunikationssystem baserade på standarden som beskrivs i kapitel 4. Effektgränserna beräknas utgående från tre tänkta krav på systemets robusthet och dess smygegenskaper.

För att utvärdera möjliga WBAN-systems robusthet så antar vi först följande krav (baserat på kapitel 2):

- **R200:** Systemet ska fungera under störning på 200 meters avstånd från en liten UAV.

För att utvärdera smygegenskaperna definierar vi även följande två krav:

- **S200:** Systemet ska inte kunna upptäckas på 200 meters avstånd från en liten UAV.
- **S50:** I smygmod ska systemet inte kunna upptäckas på 50 meters avstånd från en liten UAV.

Baserat på de olika frekvensbanden i specifikationen analyserar vi tänkta smalbandiga system med centerfrekvenserna 400 MHz, 870 MHz och 2.4 GHz samt ett UWB-system centrerat runt 7 GHz. De systemparametrar som valts för dessa system är även relevanta för soldatburna störare eller signalspaningsmottagare.

Robusthetskravet leder till en undre gräns för utsänd effekt medan de två smygkraven leder till övre gränser för utsänd effekt. Vi jämför dessa värden med den undre gräns för utsänd sändareffekt som krävs för att kommunikation ska vara möjlig utan störning.

5.1 Robusthet

Vi antar i denna förenklade analys att signal-brus-förhållandet (SNR) i mottagaren måste vara över en tröskelnivå γ_r för att kommunikation över länken ska vara möjlig. Den lägsta sändareffekt som möjliggör kommunikation ges av (se Appendix A för en härledning):

$$P_t > \gamma_r N_0 L_1 R \quad (1)$$

där L_1 motsvarar den totala länkdämpningen över radiokanalen (inklusive kroppens eller utrustningens påverkan), R utgör informationsdatatakten och N_0 är mottagarbrusets spektraltäthet.

Motsvarande krav på utsänd effekt som krävs för att klara av att kommunicera under störning (där en fullbandsstörare som har en bandbredd som är större än eller lika med signaleringsbandbredden antas):

$$P_t > \gamma_r P_j \cdot \frac{G_j G'_r L_1}{L_j} \cdot \left(\frac{W_j}{R} \right)^{-1}, \quad (2)$$

där P_j , G_j , L_j och W_j är störarens uteffekt, antennvinst, transmissionsförlust (vid fri sikt) respektive bandbredd. Vi antar att mottagarens antennvinst G'_r i störarens riktning är 0 dB.

5.2 Smygegenskaper

I utvärderingen av WBAN-systemens smygegenskaper så antar vi i denna förenklade analys att signalspanarens SNR-tröskel γ_i för detektion är i samma storleksordning som brusnivån i dess mottagare, dvs $\gamma_i = 0$ dB med en brusfaktor F_i som är 10 dB. SNR-tröskeln påverkas av hur snabbt signalspanaren måste detektera signalen och vid långa detektionstider bör en lägre tröskel ansättas.

Om vi vill att spanaren ska misslyckas att detektera en signal från en WBAN-sändare, bör kommunikationssystemets uteffekt då begränsas enligt följande:

$$\begin{cases} \frac{P_t G_t' G_i}{L_i W_i k T_0 F_i} < \gamma_i, \text{ för } W_i \geq W_t, \\ \frac{P_t G_t' G_i}{L_i W_t k T_0 F_i} < \gamma_i, \text{ för } W_i < W_t, \end{cases} \quad (3)$$

där G_i är signalspanarens antennvinst i riktning mot sändaren, L_i länkdämpningen mellan sändaren och signalspanaren, W_i signalspanarens mottagarbandbredd och W_t den utsända signalens bandbredd. Vi antar att sändarens antennvinst G_t' i riktning mot signalspanaren är 0 dB och att det är fri sikt till signalspanaren. Länkdämpningen är avståndsberoende så olika övre gränser på utsänd effekt erhålls för de två smygkraven för upptäckt på 50 respektive 200 meter.

5.3 Utvärdering

Länkdämpningen är en central parameter i de genomförda länkbudgetanalyserna. Det är svårt att hitta entydiga skattningar på den totala länkdämpningen L_1 baserat på modeller och genomförda mätningar i situationer där kroppen eller utrustning dämpar signalen, se till exempel [26]-[30]. Vi har därför valt att genomföra analyserna utifrån två värden för L_1 när det inte är fri sikt mellan sändare och mottagare:

- 50 dB respektive 70 dB för de smalbandiga systemen
- 70 dB respektive 90 dB för UWB-systemet (runt 7 GHz).

De lägre värdena är för optimistiska i situationer där någon kroppsdel dämpar signalen men de kan ses som övre nivåer som kan förväntas vid LOS. De högre värdena är troligen mer vanligt förekommande vid non-LOS (NLOS) förhållanden. De länkdämpningar som kan förväntas vid LOS på ett avstånd av 2 m är 31 dB (400 MHz), 37 dB (870 MHz), 46 dB (2.4 GHz) och 55 dB (7 GHz). Motsvarande värden på 0.2 m avstånd är 20 dB lägre.

Tre informationsdataakter utvärderas: 100 kbit/s, 500 kbit/s och 5 Mbit/s. Kanalen delas dock mellan flera användare vilket sänker de reella dataakterna för varje länk. De parametervärden som används beskrivs i tabell 5.1.

Parametrar för störare och signalspanare baseras på kraven **R200**, **S50** och **S200** som gavs i inledningen till kapitlet. Där är det tänkt att en liten UAV används för störning respektive signalspaning. En sådan UAV skulle kunna ha antennvinsten $G_i = 5$ dB för spaning eller störning och vi antar att den kan störa med effekten $P_j = 1$ W. Det finns stora osäkerheter när det gäller ett verkligt framtida systems parametrar så i denna analys är syftet främst att exemplifiera de möjligheter och svårigheter som olika tekniker förväntas stöta på när det gäller att uppfylla framtida krav på robusthet och smygegenskaper.

Tabell 5.1: Valda parametrar för utvärderingen.

Konstanter	
Ljushastigheten	$c = 3 \cdot 10^8$ m/s
Boltzmanns konstant × referenstemperatur	$kT_0 = -174$ dBm/Hz
Kommunikation	
Kommunikationssystemets antennvinster	$G_t = G_r = 0$ dB
Mottagarens brusfaktor	$F_r = 10$ dB
Kommunikationssystemets länkdämpning	$L_i = \{50, 70\}$ dB
SNR-tröskel för kommunikation (E_b/N_0)	$\gamma_r = 10$ dB
Störare	
Störarens antennvinst	$G_j = 5$ dB
Störarens effekt	$P_j = 1$ W
Signalspanare	
Signalspanarens antennvinst	$G_i = 5$ dB
Mottagarens brusfaktor	$F_i = 10$ dB
SNR-tröskel för detektion	$\gamma_i = 0$ dB

Tabell 5.2: Effektkrav för smalbandiga vågformer i IEEE 802.15.6. Spektraleffektiviteten η antas vara 1 bit/s/Hz i samtliga fall ($W_j = R/\eta$).

IEEE 802.15.6 NB		Gränser för sändareffekt P_t [dBm]			
Center-frekvens	Datatakt [kbps]	Lägst effekt, utan störning $L_1 = \begin{cases} 50 \text{ dB} \\ 70 \text{ dB} \end{cases}$	Lägst effekt, vid störning (R200) $L_1 = \begin{cases} 50 \text{ dB} \\ 70 \text{ dB} \end{cases}$	Högsta tillåten effekt, vid signalspaning (S50)	Högsta tillåten effekt, vid signalspaning (S200)
400 MHz	100	-54	24	-61	-48
		-34	44		
	500	-47	24	-54	-42
		-27	44		
870 MHz	100	-54	18	-54	-42
		-34	38		
	500	-47	18	-47	-35
		-27	38		
2,4 GHz	100	-54	9	-45	-33
		-34	29		
	500	-47	9	-38	-26
		-27	29		

Tabell 5.3: Effektkrav för UWB-vågformer i IEEE 802.15.6. Bandbredden antas vara 2.5 GHz.

IEEE 802.15.6 UWB		Gränser för sändareffekt P_t [dBm]			
Frekvens	Datatakt [kbps]	Lägsta effekt, utan störning $L_1 = \begin{cases} 70 \text{ dB} \\ 90 \text{ dB} \end{cases}$	Lägsta effekt, vid störning (R200) $L_1 = \begin{cases} 70 \text{ dB} \\ 90 \text{ dB} \end{cases}$	Högsta tillåten effekt, vid signalspaning (S50)	Högsta tillåten effekt, vid signalspaning (S200)
7 GHz	100	-34	-24	8	20
		-14	-4		
	500	-27	-17		
		-7	3		
	5000	-17	-7		
		3	13		

Robusthetskravet **R200** leder till en undre gräns för utsänd sändareffekt medan de två smygkraven **S50** och **S200** leder till övre gränser för utsänd sändareffekt. Vi jämför dessa värden med den undre gräns för utsänd sändareffekt som krävs för att kommunikation ska vara möjlig utan störning. Dessa fyra beräknade effektkrav ges i tabell 5.2 för de smalbandiga WBAN-systemen, samt i tabell 5.3 för WBAN-system baserade på UWB.

När det gäller de smalbandiga systemen, så kan vi konstatera att det är svårt att klara störkravet (**R200**) utan att sändningseffekten blir orimligt hög; detta gäller särskilt för länkdämpningen 70 dB, där sändningseffekterna ligger över 20 dBm i samtliga utvärderade fall (fjärde kolumnen i tabell 5.2). För sändareffekter över 10 till 20 dBm är det tveksamt om det finns batterier med tillräckligt bra kapacitet, annat än för tillfällig användning. Alla rutor med sändareffekt över 20 dBm är markerade med rött i tabellen.

En övre gräns för sändareffekten givet att smygkraven (**S50** och **S200**) ska vara uppfyllda ges i kolumn fem och sex. Lägsta möjliga effekt för kommunikation (kolumn tre) måste ligga under dessa värden för att smygkraven ska kunna uppfyllas; så är fallet för länkdämpningen 50 dB i samtliga fall utom för centerfrekvensen 400 MHz, där **S200** uppfylls men inte **S50**. För länkdämpningen 70 dB kan inget av smygkraven uppfyllas utom för centerfrekvensen 2,4 GHz, där **S200** uppfylls men inte **S50**.

För WBAN-system baserat på UWB-teknik, se tabell 5.3, kan vi se att alla tre kraven kan uppfyllas, utom för den högsta datatakten vid länkdämpningen 90 dB då robusthetskravet och smygkravet **S50** är oförenliga. Att de kombinerade stör- och smygkraven i de flesta fall skulle kunna vara möjliga att uppfylla beror på den stora bandspridningen där signalbandbredden (efter bandspridningen) är 2.5 GHz. Denna analys av smygegenskaperna motsvarar ett direktsekvensbandspritt system och med Gaussiskt brus. För impulsradio UWB bör en fördjupad analys av smygegenskaperna genomföras med beaktande av mottagare som är specifikt anpassade för att upptäcka den typen av sändare.

5.3.1 Slutsatser och diskussion

I litteraturen finns en stor spridning vad gäller modeller och mätresultat för den resulterande länkdämpningen på och när signalen passerar genom kroppen. En normal länkdämpning kan ha värden kring 70 dB men länkdämpningar på uppemot 90 dB har rapporterats. Vi har i analysen för de smalbandiga alternativen räknat på två värden: 50 dB och 70 dB. Noterbart är att om systemet måste kunna hantera dessa höga länkdämpningar som uppstår då signalen passerar kroppen eller soldatens utrustning innebär det att signalspaningsavstånden (under fri siktsantagande) riskerar att bli stora. Vi har analyserat

kommunikationssystem med centerfrekvenserna 400 MHz, 870 MHz och 2.4 GHz och 7 GHz. Under LOS-förhållanden motsvarar de två länkdämpningarna räckviddsändringar på 19 m, 9 m, 3 m och 1 m (för 50 dB) samt 189 m, 87 m, 31 m respektive 11 m (för 70 dB).

Smalbandiga system har svårt att klara kraven på smyg och robusthet om man ställer kravet att systemet ska vara robust nog att hantera även situationer där signalen dämpas av kroppen. Frekvenshoppning skulle kunna förbättra förutsättningarna, åtminstone vid 2.4 GHz. Dock har den genomförda analysen inte beaktat interferenser från andra radiosystem och i dessa öppna frekvensband kan ett större antal sändare vara aktiva. Inte heller egeninterferenser, från andra WBAN-system i närheten, har beaktats. Slutsatsen är därmed att smalbandiga system med liknande parametrar som de som analyserats här förväntas ha mycket svårt att klara de krav på robusthet och smygegenskaper som sannolikt kommer att ställas på ett framtida militärt WBAN-system.

UWB-tekniken indikerar i dessa analyser en hög robusthet och goda smygegenskaper, samtidigt som höga datatakt kan uppnås. Säkerheten i kommersiella system behöver dock eventuellt förbättras för att de ska kunna användas i militära sammanhang. Impulsradio UWB ger möjlighet att applicera textskydd men det är oklart om detta även kan göras för FM-UWB systemet som beskrivs i IEEE 802.15.6. Interferenser från andra WBAN utgör ett mindre problem för WBAN-system.

6 Analys av säkerhetsaspekter

Detta kapitel utgör en tentativ analys av ett framtida system för soldatens interna kommunikationsbehov ur ett IT-säkerhetsperspektiv. Denna initiala analys är genomförd på en övergripande, diskussionsmässig nivå då det ännu inte finns ett konkret system att utgå ifrån. Syftet är att belysa säkerhetsaspekter som behöver analyseras och omhändertas inför ett eventuellt införande av WBAN för soldattillämpningar.

Utöver i radiosammanhang traditionella informationssäkerhetshot som behandlar exempelvis skyddsvärd information, autentisering och risker vid nyckelhantering tillkommer även riskerna för avsiktlig manipulering av mjukvara i WBAN- eller sensornoder. Detta hot är möjligen inte främst en attackåtgärd som en motståndare kan använda sig av taktiskt inför eller under en strid, men den kan vara aktuell som en form av bestraffning eller påtryckningsmedel av både nationer och terrororganisationer. Cyberattacker kan ses som relativt enkla¹⁶, lågriskoperationer och denna hotbild bör införlivas i analyser av framtida WBAN-system.

6.1 Informationens skyddsvärde

Skyddsvärdet för informationen som kan tänkas transporteras i ett framtida WBAN är inte känd idag utan den förväntas variera beroende på vilka sensorer som är aktuella och eventuell sensornära signalbehandling som utförs. Den kan grovt indelas i de tre aspekterna sekretess, riktighet och tillgänglighet.

Sekretess innebär att obehöriga inte ska kunna ta del av informationen och den vanligaste skyddsmekanismen för att säkerställa detta vid trådlös transmission är kryptering. Styrkan som krävs för sekretesskyddet beror på den information som överförs, exempelvis kan en soldats absoluta position omfattas av sekretess medan information från en skomonterad sensor om en relativ förflyttning (steglängd och riktning) kan vara öppen. Den mest känsliga informationen i nätverket blir normalt sett dimensionerande för skyddsnivån.

Riktighet avser både att informationen måste komma från en betrodd källa och att den inte ska ha kunnat förvanskas under överföringen, det vill säga att den både ska vara autentisk och korrekt. Skyddsvärdet bestäms utifrån hur viktigt det är att ha korrekt information av respektive typ. Ofta finns ett antal olika nivåer av känslighet där viss information endast är ”kul-att-ha”, till exempel nästa veckas väderprognos för en enskild soldat, medan riktigheten hos annan information kan vara mycket kritisk som till exempel ordergivning eller positioner för att undvika vådabekämpning.

Tillgänglighet avser att information ska finnas åtkomlig hos rätt entitet vid rätt tidpunkt. I WBAN:et blir detta i princip förmågan att tillse att kommunikationen fungerar med tillräckligt stor sannolikhet i alla relevanta situationer för att kunna säkerställa att informationen kan överföras mellan olika noder när detta behövs. En stor del av tillgänglighetskraven hamnar rimligtvis på radiodelen där exempelvis förmågan att motstå såväl oavsiktliga som avsiktliga störningar är en aspekt. Att fastställa kravnivån på tillgänglighet är ofta svårt och det krävs en noggrann analys av skyddsvärdet. För låga skydds krav kan ge dålig tillförlitlighet i kritiska situationer och då potentiellt innebära fara för soldaterna. För höga krav kan å andra sidan ge problem med komplexitet, vikt, energiförbrukning, smygegenskaper och så vidare.

6.2 Signalskydd

Hotbilden för WBAN:et är komplex och beror till stor del av vilken information som skickas i systemet. Figur 6.1 visar de huvudsakliga attackvektorer för WBAN:et, baserat

¹⁶ Se exempelvis www.defcon.org för djupare hotbildsanalys.

på definitionen av signalskydd som ges i [31]. I ett radiobaserat system kan signalskyddet delas upp i krav på både radiodelar och IT-delar där gränsen mellan dessa delar är flytande och vissa hot kommer behöva hanteras av båda. De attackvektorer som är satta inom parentes i figuren är inte direkt relevanta i IT-säkerhetsperspektivet utan hanteras primärt av radiosystemet, medan övriga attackvektorer kan vara relevanta både för radiosystemet och ur IT-säkerhetsperspektiv. Notera att ”signalering” i detta sammanhang inte ska ses enbart ur perspektivet radiosändning utan även ska tolkas som transmission av data som tolkas av enheterna. Exempelvis kan en falsksignalering vara en radiosändning som tas emot och avkodas till tolkningsbar data för att sedan störa funktionen eller introducera felaktig information i enheterna.

Om sekretessklassificerad information skickas är *avlyssning* ett givet hot, där en extern aktör exempelvis kan tänkas fånga upp signalering som innehåller en hemlig positionsangivelse. Sekretessskyddet implementeras i form av ett textskydd där kryptering av informationen normalt sett utgör lösningen.

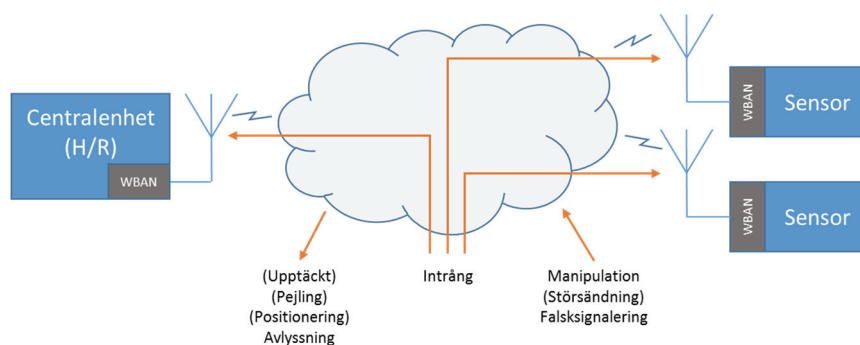
Definitionen av falsksignalering i [31] är ”[f]örsätlig inblandning i signalering för att t ex skapa förvirring, blockera kommunikationen eller inhämta underrättelser”. Falsksignalering kan alltså vara sändningar där huvuduppgiften är att störa systemets kommunikation eller för att injicera skadlig trafik i nätet. Termen falsksignalering används sällan i IT-säkerhetssammanhang men det finns många exempel på attacker som passar in i definitionen.

Falsksignalering kan också vara inriktad på informationen för att påverka användarfunktionen i systemet, till exempel i form av ett fabricerat paket med en felaktig position för att vilseleda användaren.

Falsksignalering ligger nära *manipulation* där legitima paket ändras för att lura mottagaren att avsändaren skickat annan information än som faktiskt skickats. Ett klassiskt exempel på detta är en fiktiv bankapplikation där en part skickar ett paket med betydelse ”överför 100 kr till konto X” och en attackerare manipulerar paket till att betyda ”överför 100 kr till konto Y” för att på så sätt tillskansa sig pengarna.

Falsksignalering och manipulation motverkas ofta genom autentisering av avsändande part, till exempel genom asymmetriska krypton med tillhörande certifikatkedjor eller genom symmetriska kryptometoder med förladdade gemensamma kryptonycklar.

Det sista hotet är *intrång* där en yttre aktör använder kommunikationssystemet som väg in på insidan av en eller flera noder. Ett intrång kan ge en direkt skada, till exempel när attackeraren kan hämta ut sekretessklassad information. Intrånget kan även användas som medel för att skapa en indirekt skada, ofta genom att manipulera den attackerade enheten genom att införa skadlig kod. Den skadliga koden kan sedan ligga aktiv eller latent för att vid lämpligt tillfälle slå ut enheten, alternativt läcka eller manipulera informationen.



Figur 6.1: Översiktlig hotbild för WBAN.

Intrångsskydd är komplext och består ofta av många olika delar där strikt kontroll av indata med flera lager av skyddsmekanismer som ska hindra utnyttjande av brister i mjukvaran används så att en angripare inte ska kunna utnyttja eventuella svagheter. Vilka skyddsmekanismer som ska användas i ett framtida WBAN är beroende av bland annat säkerhetskrav och systemets arkitektur vilket innebär att dessa måste bestämmas i samband med att systemet krävställs och designas.

6.3 Nätverkstopologi

Hur nätverkets topologi planeras kommer naturligtvis att påverka säkerhetsfrågorna. Om det finns en central router som all kommunikation passerar blir det lättare att ställa in delsystemen att inte kommunicera med främmande enheter men å andra sidan har man då skapat en *single-point-of-failure* som måste vara mycket säker. Multihopptopologier har dock andra säkerhetsproblem. En analys av hur nätverksdesignen påverkar säkerhetsmodellen måste finnas med i utvecklingen av ett militärt WBAN. En stjärntopologi med en central nod är dock i dagsläget det troligaste alternativet, eventuellt med möjlighet till reläfunktionalitet i noderna för att öka robustheten.

6.3.1 Addition av otillåtna enheter till nätverk

En av de stora fördelarna med att ha trådlösa nätverk är möjligheten att dynamiskt kunna addera eller ta bort enheter ur nätverket. Om denna process kan missbrukas är det möjligt att en angripare kan (i) lägga till enheter som inte ska finnas i nätverket, (ii) få enheter avstängda från nätverket, eller (iii) utge sig för att vara en befintlig enhet och ta över kommunikationen mellan denna och nätverket.

Det finns metoder som att använda stark kryptering eller frekvenshopp som försvårar en angriparens uppgift men exakt vilka metoder som fungerar för en viss implementation måste utredas i en framtida utveckling.

6.4 Självskydd

Som tidigare nämnts är skydd mot intrång en del som krävs i systemet. Intrångsskydd är en del i det som kallas självskydd där även ett antal andra hot ska hanteras.

Grundprincipen för självskyddet är att en enhet i princip inte får förlita sig på något annat än sig själv för sitt skydd. I realiteten är det omöjligt att bygga en enhet som inte till någon grad måste förlita sig på sin miljö för att minska den upplevda hotbilden. Denna avvägning bör göras utifrån enhetens specifika hotbild.

Kraven på självskyddet ökar normalt sett för produkter med kvalificerade motståndare där det även kan krävas ett signifikant skydd mot exempelvis fysisk manipulation.

Alla datorer har vissa saker gemensamt, exempelvis en processor och någon form av minne. Detta kommer med största sannolikhet att vara fallet även för de olika WBAN-enheter. Varje enhet måste ha en processor för att kunna bearbeta data och styra radion, ett minne för att lagra data och en radioenhet för att kunna kommunicera med de andra enheterna i nätverket. Någon form av strömförsörjning är också nödvändig. Denna antas vara i form av ett lokalt batteri och har utelämnats ur modellen.

Förutom dessa komponenter kommer en del enheter att ha sensorer av olika slag, vilka i sin tur kan vara enkla dumma mätapparater eller fullständiga komponenter med egna processorer. En sensorenhet förväntas inkludera WBAN-nod, sensorhårdvara samt eventuellt minne och processor för sensornära signalbehandling.

6.4.1 Hotbeskrivning

I trådlösa nätverk finns det tre huvudsakliga intrångsvektorer för att kringgå självskyddet:

- a) Fysisk modifiering av tillåtna enheter
- b) Modifiering av tillåtna enheters mjukvara genom otillåten radiokommunikation
- c) Modifiering av tillåtna enheters mjukvara genom att maskera angreppet som en tillåten uppdatering av mjukvara

Dessa tre utgör en gemensam bas sett från det trådlösa nätverket men det kan även tillkomma ytterligare intrångsvektorer beroende på andra anslutningsmöjligheter på enheterna. Exempelvis kan en enhet ha en USB-port för att kunna genomföra inställningar och uppdateringar, varpå denna port tillkommer som potentiell intrångsväg till enheten.

6.4.1.1 Fysisk modifiering av tillåtna enheter

Attacker i form av fysisk modifiering innebär att angripare på något sätt lyckas ändra på de fysiska komponenterna som sitter i en enhet, antingen genom att lägga till, byta ut eller ta bort komponenter i enheten. Det kan även göras genom att placera ny hårdvara i kontakter på enheten, som USB-enheter och liknande. Möjligheterna för denna typ av angrepp är naturligtvis direkt beroende på hur hårdvaran ser ut och om angriparen kan få tillgång till enheten för att utföra modifieringen.

Ett specialfall av fysisk modifiering är om en angripare kan påverka tillverkningen av enheterna så att de anländer från tillverkaren med dold funktionalitet som angriparen kan utnyttja. Denna funktionalitet kan var allt från passiva, till exempel ändringar i krypteringsalgoritmer för att introducera säkerhetshål, till dolda radiokomponenter som fungerar som bakdörrar in i systemet, hela vägen till rena sabotagekretsar som kan orsaka permanent förstörelse av enheten om de aktiveras. Det måste därför finnas någon metod för att upprätthålla tilltron till enheterna, till exempel genom att granska hårdvarukomponenter innan de kopplas in i systemet.

6.4.1.2 Modifiering av tillåtna enheters mjukvara

De flesta kommersiella system byggs för att fungera med ständiga uppdateringar. I många fall förekommer även parametrar eller kryptonycklar som måste kunna uppdateras med jämna intervall. Under denna process, eller genom att initiera en sådan process, är det möjligt att en angripare kan introducera skadlig kod i systemet genom brister i processen eller genom sårbarheter i enheten. Det kan potentiellt ske genom radiosändningar eller genom att på något sätt manipulera programvaran som uppdaterar systemet.

Genom en sådan uppdatering kan enhetens beteende potentiellt ändras. Exakt vad som kan uppnås genom angreppet är i hög grad beroende av hur enheten är uppbyggd. En bra design och implementation kan göra det mycket svårt för en angripare att ta sig in via denna vektor. Även i de fall som en angripare kan ta sig in, kan olika metoder förhindra vidare spridning i nätverket och i hög grad underlätta rensning av systemet till ursprunglig status. Dessa metoder inkluderar kryptering, säkerhetskopiering med flera.

Processen för uppdatering måste ha en hög säkerhetsnivå. Det finns olika säkerhetsmetoder som kan användas, som certifikat från legitima programvaruleverantörer, testning av uppdateringar på simulerade system för analys, och så vidare. Men dessa måste testas och införas i organisationen som ska använda systemet. Det är viktigt att policyer och metoder för en säker uppdatering finns som stöd för den personal som ska utföra handgreppen. Uppdateringar bör endast tillåtas under kontrollerade former.

6.5 Diskussion och slutsatser

Det finns många olika problemområden som måste hanteras för att upprätthålla IT-säkerheten i WBAN:et. Detta avsnitt tar upp ett par specifika områden som potentiellt kan vara svårhanterliga ur regelverks- och hanteringsperspektiv.

6.5.1 Nyckelhantering

Kryptografiska metoder används ofta för att lösa säkerhetsproblem inom sekretess, riktighet och autentisering men kryptering kräver normalt sett att någon form av kryptonycklar finns i systemet. Dessa kan antingen vara externt skapade och inladdade i enheterna eller lokalt genererade. Om nycklarna skapas externt måste det finnas en hantering av dessa med tekniskt stöd och rutiner för distribution och inläsning av nycklarna. Någon form av hopkopplingsförfarande för att överföra nycklar mellan enheterna behövs istället om de genereras i enheterna. En ytterligare komplexitet är att enheterna kan omfattas av sekretess då kryptonycklar är inlästa. Det kan ge stora praktiska problem i soldaternas vardag, till exempel att det skulle kunna bli restriktioner på att ta av sig vissa plagg då detta skulle innebära en risk att en enhet glöms kvar, tappas bort eller stjäls.

6.5.2 Autentisering

Ömsesidig autentisering av enheter för att säkerställa att endast betrodda enheter kan anslutas till nätverket kan hanteras på olika sätt. Enheternas identiteter kan matas in via ett användargränssnitt, laddas på via en konfigurationsport eller genom att enheter paras ihop genom ett specifikt förfarande. Hur detta ska göras för att vara säkert samtidigt som det är lätt för soldaten att hantera utrustningen är ett område som kräver ett gediget arbete. Att exempelvis kräva inläsning av nya kryptonycklar med jämna och potentiellt ganska korta intervaller i ett större antal enheter per soldat lär vara hindrande i praktiken och kan dessutom innebära att riskerna i systemet ökar.

6.5.3 Öppet kontra hemligt WBAN

Om WBAN-systemet ska kunna överföra hemlig information så kan de civila system som analyserades i kapitel 5 inte användas. Ett säkerhetsgodkänt WBAN behöver då utvecklas. UWB-tekniken är ett intressant alternativ och i USA pågår utveckling av ett liknande system där ambitionen är att det ska bli godkänt av NSA (*National Security Agency*).

Om WBAN:et inte designas för att hantera hemlig information så utgör WBAN:ets koppling till centralenheten en uppenbar problematik då denna kan tänkas innehålla hemlig information. Kopplingen ger en potentiell källa för läckage där hemlig information kan komma ut via WBAN:ets radiogränssnitt, antingen i form av direkt signalering eller genom röjande signaler. Såväl direkt utsändning som röjande signaler kan uppstå på grund av en attack mot systemet eller en brist i centralenhetens mjukvara eller hårdvara. Om WBAN:et konstrueras för att kunna hantera hemlig information, exempelvis för att överföra lägesbilder eller positioner, så ställs höga krav på sekretesskyddet i WBAN:et. Å andra sidan förenklas centralenhetens separation av hemlig information från WBAN-gränssnittet. Även sensorerna löper dock risken för att manipuleras så att de riskerar att sprida skadlig kod i nätverket. Det är troligt att kommersiella sensorer kommer användas i hög grad för att reducera kostnad, vikt och storlek och det kan vara svårt att uppnå motsvarande säkerhetsnivå för dessa.

7 Rekommenderade designprinciper

Integrationsaspekter gentemot soldatens övriga utrustning är ytterst viktiga vid införandet av ett WBAN. En viktig motivering för ett WBAN är att förenkla denna integration. Samexistensaspekter med främst ett framtida Buret Krypto (*Soldier Node*) är viktiga och diskuteras härnäst.

7.1 Samexistensaspekter och systemförslag

Figur 7.1 visar en schematisk bild över en möjlig framtida realisering av ett WBAN för soldaten. I vänster av bilden återfinns de radioapparater som används för kommunikation med andra soldater. Kommunikationen mellan soldaterna kan skyddas med en kryptoapparat, till exempel Buret Krypto eller annan liknande utrustning, för att ge möjlighet att utbyta hemlig information (upp till nivån Hemlig / Restricted). Taltrafiken, som i framtiden sannolikt kommer utgöras av tal som skickas som IP-paket, s.k. *VoIP*, skickas efter att talet har avkodats direkt till soldatens headset. Datatrafik till/från radion hanteras av en centralenhet av något slag. Förutom den krypterade kommunikationen över radion så kan centralenheten även kommunicera lokalt, med exempelvis soldatens sensorer och presentationshjälpmedel, via WBAN:et.

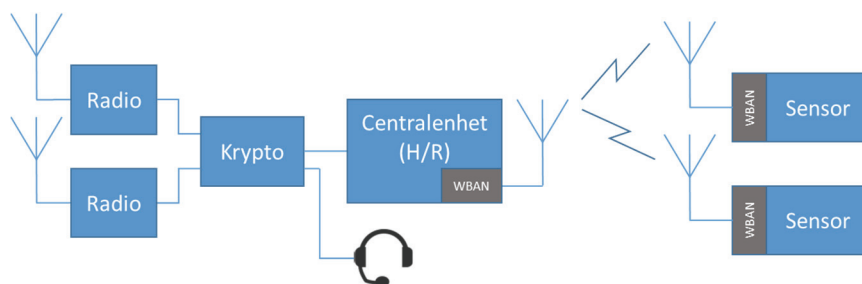
Ett systemförslag enligt figur 7.1 bör kunna realiseras och integreras med ett Buret Krypto om WBAN-noderna kan designas så att de kan hantera hemlig information. En utmaning är dock att lösa detta på kort sikt då WBAN-noderna inte bedöms ha denna möjlighet.

7.2 Designrekommendationer

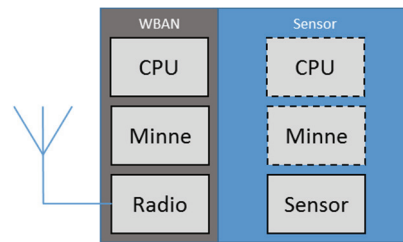
En sensorenhet bör inkludera WBAN-nod, sensorhårdvara samt eventuellt minne och processor för sensornära signalbehandling, se figur 7.2. För att uppnå ett kostnadseffektivt system är det sannolikt att WBAN-noden bör vara likadan i alla sensorer, samt att den har ett standardiserat gränssnitt för att kunna kopplas ihop med heterogena sensorer.

För att minimera kraven på datatakt i ett WBAN är ett bra alternativ att bygga in beräknings- och analyskapacitet i ändnoderna (sensornära) så att en mindre mängd bearbetad sensorinformation behöver överföras istället för rå sensordata som kan kräva höga datatakt.

En möjlig framtida lösning, sannolikt bortom år 2025, skulle kunna vara att kombinera uniformsintegrerad kabelbunden dataöverföring med en trådlös överföring av information. Den trådlösa överföringen behöver då genomföras på mycket kort avstånd mellan hjälmen och exempelvis uniformskragen och mellan vapnet och uniformsärmen. Denna radiolänk skulle då endast ersätta kablarna till/från hjälm och vapen. I ett sådant system är det kritiskt att en LOS-kanal kan garanteras där varken kroppen eller utrustning väsentligt dämpar signalen.



Figur 7.1: Systembild för tänkbart soldatsystem med WBAN och soldatens gruppradio.



Figur 7.2: Troliga ingående komponenter i enskilda sensornoder.

Detta bör kunna vara möjligt på dessa korta avstånd genom att även använda multipla antenner på exempelvis hjälm/vapen, uniformskrage och uniformsärm. Eftersom kanalens dämpning på radiosignalen då sannolikt skulle vara låg ökar möjligheterna dramatiskt att designa ett robust WBAN med goda smygegenskaper.

8 Slutsatser och rekommendationer

En sammanfattande gapanalys som baseras på de användarbehov som diskuteras i kapitel 3 och de tekniklösningar som beskrivs i kapitel 4 och analyseras i kapitel 5 ges härnäst. En enkel roadmap för det fortsatta arbetet presenteras slutligen.

8.1 Sammanfattande gapanalys

Slutsatserna ges i form av en gapanalys av alternativa WBAN-teknikers robusthet och smygegenskaper och en generell diskussion om viktiga säkerhetsaspekter.

8.1.1 Robusthet och smygegenskaper

De smalbandiga system som har ingått i analysen, vars parameterintervall inspirerats av standarden IEEE 802.15.4, har svårt att samtidigt uppnå en tillräcklig robusthet och goda smygegenskaper. Även om dessa system inte direkt har inkluderats i analyserna, så kan troligen samma bedömning göras för WPAN-system såsom BLE, ZigBee och andra liknande system.

UWB-tekniken har potential för att kunna uppnå en hög robusthet och goda smygegenskaper, även vid relativt höga datatakt. Impulsradio UWB ger möjlighet att applicera kryptologisk bandspridning av signalen. Påverkan från interferenser från andra WBAN behöver dock analyseras och mer detaljerade analyser av robusthet och smygegenskaper bör genomföras.

HBC har i denna studie inte studerats i tillräcklig grad för att möjliggöra en bedömning av teknikens mognadsgrad. Bedömningen är dock att den har ett flertal intressanta egenskaper som kan göra det till ett intressant alternativ för ett framtida militärt WBAN.

8.1.2 Säkerhetsaspekter

Det finns idag inga möjligheter att sända hemlig information över existerande WBAN. Det innebär bland annat att headset och en eventuell display som visar en lägesbild fortsatt måste använda trådbunden överföring. För sensorer som inte genererar skyddsvärd information kan civila WBAN eventuellt ge ett tillräckligt skydd avseende autentisering för att utgöra ett alternativ. De ger eventuellt även möjlighet till länkkryptering som kan möjliggöra att personlig information, som av integritetsskäl inte bör spridas, kan få en godtagbar nivå av kryptering. Ett problem som i så fall kommer behöva lösas uppstår i situationer då WBAN:et ska kopplas till en dator som innehåller skyddsvärd information.

På längre sikt är det önskvärt att även kunna skicka hemlig information över WBAN:et, men endast upp till den nivå som specificeras i buret krypto (Hemlig / Restricted).

De viktigaste säkerhetsrelaterade frågeställningarna som behöver adresseras är länkkryptering, nyckelhantering och autentisering. Säkerhetslösningen kan bli kostnadsdrivande och det är *kritiskt att en för soldaten lätthanterlig lösning kan uppnås där noderna även uppfyller kraven på låg vikt, litet och energisnålt*. Kan dessa krav inte uppnås finns inte längre något större incitament för att ersätta kablar med ett WBAN.

8.2 Rekommendationer

Bedömningen i nuläget är att behovet av ett WBAN inte är akut utan snarare kommer att uppstå om ett antal år vid ett eventuellt införande av ett ledningsstödsystem för soldaten eller liknande utrustning med processor och användargränssnitt.

Utifrån resultaten i denna studie så rekommenderar vi att följande åtgärder initieras:

- Genomför en workshop, med deltagare från Försvarmakten, i syfte att prioritera användarbehoven, bedöma sekretessnivåer för framtida sensorer, samt uppnå samsyn om den framtida soldatutvecklingen och tidplaner för denna.
- Följ utvecklingen av ISW i USA och bedöm om det eventuellt kan utvecklas till ett intressant system även för Försvarmaktens behov.
- Genomför fördjupade studier av UWB-teknikens robusthet mot interferenser och dess smygegenskaper gentemot mottagare som specifikt riktar sig mot den typen av sändning. Tekniken förväntas i närtid kunna ge en hög robusthet, goda smygegenskaper och låg effektförbrukning och kan utgöra ett alternativ på kort sikt för sensorinformation som inte är hemlig.
- Följ utvecklingen inom området HBC, främst när det gäller kapacitivt kopplade tekniker, och bedöm dess mognadsgrad.
- En fördjupad analys av säkerhetsaspekterna bör genomföras av UWB-tekniken. Generellt så bör en sådan analys genomföras i ett tidigt skede, för att redan i en designfas kunna påverka utformningen, men tidsaspekten avgörs även av om ett införande förväntas basera sig på (delvis) egenutvecklad teknik (exempelvis gällande säkerhetslösningar) eller upphandling av befintliga system. Även potentiella medicinska aspekter bör analyseras i ett tidigt skede.
- Påbörja/påverka utvecklingen av ett standardiserat gränssnitt för att kunna koppla ihop en WBAN-nod med heterogena sensoralternativ. Ett standardiserat gränssnitt behöver sannolikt utvecklas för att uppnå ett kostnadseffektivt system samtidigt som det förenklar uppbyggnaden av ett modulärt system och framtida uppgraderingar av sensorerna.

Referenser

- [1] Studieförsök 01094: *SF Markstridsutrustad soldat (MARKUS) – SLUTRAPPORT*, MSS 2007.
- [2] W. E. Cole, "Military "Humionics" – Integrating Electronic Systems on the Soldier," *AFCEA Brief*, mars 2015.
http://www.afceaboston.com/documents/events/nh15/AFCEA_Brief_3_March_2015_v4-4.pdf
- [3] P. Varney, "NSRDEC Overview," februari 2012.
- [4] *Future Soldier 2030 Initiative*, RDECOM, US ARMY NATICK SOLDIER RD&E CENTER, 2009.
- [5] "Body area networks in defence applications," *Presentation at the BodyNet Workshop*, Oslo, Norge, september 2012.
- [6] D.L. Hirschberg, K. Betts, P. Emanuel, and M Caples, *Assessment of wearable sensor technologies for biosurveillance*, Edgewood Chemical Biological Center, US Army RDECOM, ECBC-TR-1275, november 2014.
- [7] Per-Anders Oskarsson, Pär-Anders Albinsson, Charlotte Hellgren, Jonathan Svensson, Jouni Rantakokko, Britta Levin, Jari Laarni, Juhani Heinilä, Antti Vääänen, Johan Tofte, Jari Matikainen, Petri Virtanen, Erik Lundström, *WP2: Multimodal functionality and UI design*, EDA Report, B-1143-RT-GP (Multimodal Soldier Interface System – MUMSIS), mars 2015.
- [8] J. Laarni, B. Levin, I. Aaltonen, J. Heinilä, A. Vääänen, J. Svensson, J. Matikainen, P. Gustaffson, E. Lundström och P. Virtanen, *WP4: Demonstrator system evaluation and final system requirements*, EDA Report, B-1143-RT-GP (Multimodal Soldier Interface System – MUMSIS), december 2015.
- [9] M. Batalin, E. Yuen, B. Dolezal, D. Smith, C. Cooper och J. Mapar, "PHASER: Physiological health assessment system for emergency responders," *Proc. of IEEE International Conference on Body Sensor Networks*, Cambridge, MA, maj 2013.
- [10] ÖSM soldatsystem MARKUS (FM 21 900:60493).
- [11] Remiss Systemmålsättning (TTEM) soldatsystem (FM 2015-396:2).
- [12] S. Movassaghi, M. Abolhasan, J. Lipman, D. Smith och A. Jamalipour, "Wireless body area networks: a survey," *Transactions on IEEE Communications Surveys & Tutorials*, 2014.
- [13] R. Cavallari, F. Martelli, R. Rosini, C. Buratti och R. Verdone, "A survey on wireless body area networks: Technologies and design challenges," *IEEE Communications Surveys & Tutorials*, 2014.
- [14] S. Ullah et al, "A Comprehensive Survey of Wireless Body Area Networks," *Transactions of J. Med. Syst.*, juni 2012.
- [15] *IEEE Standard for Local and Metropolitan Area Networks – Part 15.6: Wireless Body Area Networks*, IEEE Std. 802.15.6TM-2012, februari 2012.
- [16] M. Seyed, B. Kibret, D.T.H. Lai och M. Faulkner, "A survey on intrabody communications for body area network applications," *IEEE Transactions on Biomedical Engineering*, augusti 2013.
- [17] K.S. Kwak, S. Ullah och N. Ullah, "An overview of IEEE802.15.6 standard," *Proceedings of International Symposium on Applied Sciences in Applied Medical and Communication Technologies (ISABEL)*, Rom, Italien, november 2010.
- [18] S. Ullah, M. Mohaisen och M.A. Alnuem, "A Review of IEEE 802.15.6 MAC, PHY, and Security Specifications," *Transactions of International Journal of Distributed Sensor Networks*, mars 2013.
- [19] T. Barber, T. Carvey, and A. Chandrakasan, "Designing for wireless LAN communications," *IEEE Circuits and Devices Magazine*, juli 1996.
- [20] G. I. Seffers, "Army develops one-man tactical operations center," *AFCEA Signal Magazine*, februari 2011.

- [21] A. Kostrzewski, K.S. Lee, E. Gans, C. Winterhalter, and T. Jannson, "Innovative, wearable snap connector technology for improved networking in electronic garments," *Proceedings of SPIE*, maj 2007.
- [22] C.A. Winterhalter, J. Teverovsky, P. Wilson, J. Slade, W. Horowitz, E. Tierney, and V. Sharma, "Development of electronic textiles to support networks, communications, and medical applications in future US military protective clothing systems," *IEEE Transactions on Information Technology in Biomedicine*, Vol. 9, No. 3, pp. 402-406, 2005.
- [23] N. Seyed Mazloun, "Body-coupled communications - Experimental characterization, channel modeling and physical layer design," Institutionen för signaler och system, Chalmers tekniska högskola, Göteborg, Rapport nr: EX084/2008, 2008.
- [24] Y. Davilis, A. Kalis och A. Ifantis, "On the use of ultrasonic waves as a communications medium in biosensor networks," *IEEE Transactions on Information Technology in Biomedicine*, maj 2010.
- [25] G. E. Santagati, T. Melodia, L. Galluccio och S. Palazzo, "Distributed MAC and rate adaptation for ultrasonically networked implantable sensors," *Proceedings of IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON)*, 2013.
- [26] R. Chandra, and A.J. Johansson, "A Link Loss Model for the On-Body Propagation Channel for Binaural Hearing Aids," *IEEE Transactions on Antennas and Propagation*, vol. 61, no. 12, pp. 6180-6190, december 2013.
- [27] Yazdandoost, K., and K. Sayrafian-Pour, *Channel model for body area network (BAN)*, IEEE p802.15-08-0780-12-0006, November 2010.
- [28] J. Ryckaert, P. De Donecker, R. Meys, A. de Le Hoye och S. Donnay, "Channel model for wireless communication around human body," *Electronic Letters*, Vol. 40, No. 9, april 2004.
- [29] R. Chandra, "Antennas, Wave Propagation, and Localization in Wireless Body Area Networks," Diss. Lunds Universitet, 2014.
- [30] S. L. Cotton, R. D'Errico and C. Oestges, "A review of radio channel models for body centric communications," *Radio Science*, Vol. 49, Nr. 6, s. 371-388, juni 2014.
- [31] *H TST Grunder (Handbok Totalförsvarets Signalskyddstjänst)*. Försvarsmakten Högkvarteret 12 839:63626, M7746-734002.

Appendix A – Robusthetsanalys

I detta appendix ges en detaljerad beskrivning av de ekvationer och antaganden som görs i analysen av WBAN-systemens robusthet mot radiokanalen men även vid avsiktlig störning.

Utan avsiktlig störning ges signal-brusförhållandet i radiomottagaren av

$$\frac{E_b}{N_0}, \quad (\text{A.1})$$

där N_0 är mottagarbrusets spektraltäthet och E_b är energi per informationsbit vid mottagaren. För en kommunikationslänk där sändaren har uteffekten P_t , och där G_t och G_r är antennvinster för sändare respektive mottagare, kan den mottagna effekten P_r i mottagaren uttryckas med en länkbudget enligt

$$P_r = \frac{P_t G_t G_r}{L_c}, \quad (\text{A.2})$$

där L_c är radiokanalens transmissionsförlust. Vid fri sikt mellan sändare och mottagare gäller att radiokanalens transmissionsförlust kan beräknas enligt

$$L_c = \left(\frac{4\pi r}{\lambda} \right)^2, \quad (\text{A.3})$$

där r är avståndet mellan sändare och mottagare och λ är våglängden. Om sändare och mottagare är placerade på kroppen så är det svårare att separera antennens och kanalens påverkan. Därför är det vanligt att i detta fall baka in antennvinster och transmissionsförluster på kanalen till en total länkdämpning L_l , se till exempel [30],[31]:

$$L_l = \frac{L_c}{G_t G_r}. \quad (\text{A.4})$$

Länkbudgeten kan då beräknas enligt

$$P_r = \frac{P_t}{L_l}. \quad (\text{A.5})$$

Energien per informationsbit vid mottagaren, E_b , kan då uttryckas som

$$E_b = \frac{P_r}{R} = \frac{P_t}{L_l R}, \quad (\text{A.6})$$

där R är informationsdatatakten. Mottagarbrusets spektraltäthet kan med hjälp av mottagarens systembrusfaktor F_r uttryckas som

$$N_0 = kT_0 F_r, \quad (\text{A.7})$$

där k är Boltzmanns konstant och $T_0 = 290$ K är referenstemperaturen för brusfaktorn F_r . Vi antar signal-brus-förhållandet (SNR) i mottagaren måste vara över en tröskelnivå γ_r för att kommunikation över länken ska vara möjlig:

$$\frac{E_b}{N_0} = \frac{P_t}{kT_0 F_r L_l R} > \gamma_r. \quad (\text{A.8})$$

$$P_t > \gamma_r k T_0 F_r L_l R. \quad (\text{A.9})$$

Under avsiktlig störning med bredbandigt brus ges signal-brusförhållandet i mottagaren av

$$\frac{E_b}{N_0 + N_j} \approx \frac{E_b}{N_j}, \quad (\text{A.10})$$

där N_j är störsignalens spektraltäthet vid mottagaren och approximationsfelet är mindre än 1 dB om förhållandet N_j/N_0 är större än ca 6 dB. Om störaren sprider uteffekten P_j likformigt inom bandbredden W_j (en fullbandsstörare antas, med bandbredd större än eller lika med signaleringsbandbredden) med antennvinsten G_j i riktning mot mottagaren, kan N_j uttryckas enligt

$$N_j = \frac{P_j G_j G'_r}{L_j W_j}, \quad (\text{A.11})$$

där L_j är transmissionsförlusten mellan störare och mottagare och mottagarens antennvinst i störarens riktning är G'_r . Analogt med villkor (A.8) får vi då följande villkor för att kommunikation över länken ska vara möjlig

$$\frac{E_b}{N_j} = \frac{P_t L_j}{P_j G_j G'_r L_l} \cdot \frac{W_j}{R} > \gamma_r \quad (\text{A.12})$$

Ur ekvation (A.12) erhålls ett krav på nödvändig utsänd effekt P_t som krävs för att klara av att kommunicera under störning:

$$P_t > \gamma_r P_j \cdot \frac{G_j G'_r L_l}{L_j} \cdot \left(\frac{W_j}{R}\right)^{-1} \quad (\text{A.13})$$

där vi antar att mottagarens antennvinst G'_r i störarens riktning är 0 dB.

FOI är en huvudsakligen uppdragsfinansierad myndighet under Försvarsdepartementet. Kärnverksamheten är forskning, metod- och teknikutveckling till nytta för försvar och säkerhet. Organisationen har cirka 1000 anställda varav ungefär 800 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
164 90 Stockholm

Tel: 08-55 50 30 00
Fax: 08-55 50 31 00

www.foi.se