



Robust PNT

Slutrapport

JOUNI RANTAKOKKO (RED.), MIKAEL ALEXANDERSSON,
ERIK AXELL, OSKAR KARLSSON, SARA NILSSON,
JONAS NYGÅRDS, GLÄDJE KARL OLSSON, JOAKIM RYDELL

Jouni Rantakokko (red.), Mikael Alexandersson,
Erik Axell, Oskar Karlsson, Sara Nilsson, Jonas
Nygårds, Glädje Karl Olsson, Joakim Rydell

Robust PNT

Slutrapport

Titel	Robust PNT – Slutrapport
Title	Robust PNT – Final report
Rapportnr/Report no	FOI-R--5414--SE
Månad/Month	Mars
Utgivningsår/Year	2023
Antal sidor/Pages	59
ISSN	1650-1942
Uppdragsgivare/Client	Försvarsmakten
Forskningsområde	Ledningsteknologi
FoT-område	Ledning och MSI
Projektnr/Project no	E716598
Godkänd av/Approved by	Christian Jönsson
Ansvarig avdelning	Telekrig

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

Förmågan att kunna genomföra operationer i telestörda miljöer är kritisk för Försvarmakten. Dagens PNT-system (Position, Navigering och Tid) är i stora delar beroende av satellitnavigeringssystem (Global Navigation Satellite System, GNSS). GNSS-mottagare är, på grund av de låga signalnivåerna, sårbara mot stör- och vilseledningsattacker. PNT-system med en avsevärt högre robusthet kan utvecklas genom att kombinera de kommande krypterade tjänsterna (M-kod och Public Regulated Service, PRS) med gruppantennner och detektion av störning och vilseledning, kompletterat med utvalda stöttande sensorer och delsystem.

Denna slutrapport beskriver den forskning som genomförts inom projektet Robust PNT och erhållna resultat. Projektets övergripande frågeställningar har styrt de olika forskningsaktiviteterna, som har varit inriktade mot: (i) att följa och analysera omvärldsutvecklingen inom PNT-området, (ii) utveckling av experimentsystem för utvärderingar och demonstrationer av en robust GNSS-modul, (iii) kunskapsuppbyggnad inom GNSS-området rörande framför allt de nya krypterade tjänsterna och metoder för detektion av stör- och vilseledningsattacker, samt (iv) kunskapsuppbyggnad av två utvalda stöttande tekniker (hastighetsstöttad tröghetsnavigering och kartstöttad positionering). Slutligen beskrivs prioriterade forskningsbehov på kort, medellång och lång sikt, samt prioriterade satsningar inom PNT-området.

Nyckelord: PNT, GNSS, GPS M-kod, Galileo PRS, gruppantenn, störskyddssystem, detektionsmetoder, störning, vilseledning, stöttande tekniker

Summary

The ability to operate efficiently in challenging electronic warfare environments is critical for the Swedish Armed Forces. Today's PNT-systems (Position, Navigation and Timing) have critical vulnerabilities due to the GNSS-receivers (Global Navigation Satellite System) inherent susceptibility towards jamming and spoofing. PNT-systems with significantly increased robustness can be developed by combining the future new encrypted services (M-code and Public Regulated Service, PRS) with anti-jam antenna arrays and detection of jamming and spoofing attacks, complemented with selected alternative navigation (AltNav) sensors and sub-systems.

This report provides a summary of the research that has been conducted within the R&D project Robust PNT, and its main results. The projects overarching research questions has guided the projects different research activities, which have been focused on: *(i)* follow and analyse the technology development in the PNT-area, *(ii)* design of an experimental system for evaluations and demonstrations of a robust GNSS-module, *(iii)* knowledge building within the GNSS-area primarily concerning the new encrypted signals and detection of jamming and spoofing attacks, and *(iv)* knowledge building concerning two selected alternative navigation technologies (velocity-aided inertial navigation and robust map-aided navigation). Furthermore, prioritized R&D needs in the short, medium and long term, and prioritized new investments within the PNT-area, are described.

Keywords: PNT, GNSS, GPS M-kod, Galileo PRS, antenna array, anti-jam, detection, jamming, spoofing, AltNav

Innehållsförteckning

1	Inledning	7
1.1	Rapportens målgrupp och struktur	7
1.2	Projektet Robust PNT	7
1.2.1	Projektets frågeställningar	8
1.2.2	Forskningsaktiviteter	8
1.2.3	Informationsspridning och samverkan	9
1.2.4	Avgränsningar	9
1.3	Publikationer	10
2	Framtida robusta PNT-system	11
2.1	GNSS	11
2.1.1	Sårbarheter	11
2.1.2	Robust GNSS-modul	12
2.2	Stöttande positioneringstekniker	14
3	Detektion av störning och vilseledning	17
3.1	Systembeskrivning	17
3.1.1	Arkitektur för detektion	17
3.1.2	Mjukvara och detektionsalgoritmer	17
3.2	Utvärderingar	21
3.2.1	Beskrivning av genomförda tester	21
3.2.2	Resultat	22
3.3	Slutsatser	25
4	Experimentsystem för robust GNSS-modul	27
4.1	Styrdator och seriekort	27
4.2	Sensorer	27
4.3	Gruppantenn	29
4.4	Anslutningar	29
4.5	Validering	30
5	Hastighetsstöttade tröghetsnavigeringssystem	33
5.1	Tröghetsnavigeringssystem	33
5.2	Simuleringsmiljö	34
5.3	Simuleringar	35
5.3.1	Inverkan av hastighetsmätningar	35
5.3.2	Inverkan av vattenströmmar	35
5.3.3	Inverkan av förlorad bottenkontakt	37
5.3.4	Rörelsemönster	38
5.4	Slutsatser	39
5.5	Fortsatt arbete	40
6	Kartbaserad positionering- och navigering	41
6.1	Bakgrund	41

6.2	Begränsningar	41
6.2.1	Icke-informativa miljöer	42
6.2.2	Inaktuella kartor och landmärkesdatabaser	42
6.2.3	Robusthetshöjande modifikationer	42
6.3	Kartstöttade positionerings- och navigeringsmetoder	43
6.3.1	Matchning av lodtittande kameravy mot satellitbild	43
6.3.2	Matchning mot segmenterad och klassindeldad satellitbild ..	44
6.3.3	Matchning mot information från GIS	44
6.3.4	Matchning mot 3D-modell	44
6.3.5	Matchning av bild från fordon mot 3D-punktmoln	45
6.3.6	Fusion av kartstöttad och relativ positionering, samt kartuppdatering	46
6.3.7	Kooperativ SLAM	47
6.4	Slutsatser	47
7	Internationella samarbeten	49
7.1	GPS and NAVWAR RDT&E MoU	49
7.2	NATO STO	49
8	Diskussion	51
8.1	Omvärldsutvecklingen inom PNT-området	51
8.2	Robusthet hos GNSS-mottagare med gruppantennbaserade störskyddssystem	52
8.3	Framtidens militära GNSS-mottagare	52
8.4	Stöttande deltekniker	53
8.4.1	Hastighetsstöttade TN-system	53
8.4.2	Robusthet mot fel i referenskartor vid kartstöttad positionering och navigering	53
9	Slutsatser	55
	Referenser	57

1 Inledning

Ryssland har en väl utvecklad förmåga att genomföra telekrigsinsatser och denna förmåga är även integrerad i förbanden. De ser telekrigsförmågan som ett viktigt medel för att motverka det tekniska försprång som västländerna besitter i form av exempelvis lednings-, sambands- och sensorsystem.¹ Förmågan att med bibehållen effektivitet kunna genomföra operationer i telestörda miljöer är därmed kritisk för Försvarmakten.

Dagens PNT-system² är i stora delar beroende av GNSS-mottagare (Global Navigation Satellite System). GNSS-mottagare är dock sårbara mot stör- och vilseledningsattacker då de mottagna signalnivåerna är mycket låga. En hög störtålighet kan erhållas genom att kombinera de nya krypterade tjänsterna (M-kod och Public Regulated Service, PRS) med gruppantenner och detektion av störning och vilseledning, kompletterat med ytterligare stöttande sensorer och delsystem.

1.1 Rapportens målgrupp och struktur

Denna rapport ger en sammanfattning av den forskning som genomförts i projektet Robust PNT inom ramen för FoT-område Ledning och MSI.³ Rapporten riktar sig primärt mot personal på Försvarmakten och FMV som arbetar med, eller är intresserade av, materielanskaffning, förmåge- och metodutveckling, teknisk utveckling eller forskning inom PNT-området. Fokus är mot små och medelstora plattformar då forsknings- och utvecklingsbehoven bedöms vara störst för dessa.

Ett förslag på en möjlig arkitektur för framtida militära PNT-system beskrivs i kapitel 2. Det baseras på ett multisensorsystem där någon typ av dödräkning (ofta i form av tröghetsnavigering) utgör grunden och där den stöts av en robust GNSS-modul och av ytterligare stöttande sensorer. Kapitlet utgör även en bakgrund till PNT-området. Kapitel 3 beskriver och utvärderar olika metoder för att detektera störning och vilseledning mot GNSS-mottagare som använder de öppna okrypterade signalerna. Utvecklingen av ett experimentsystem för en robust GNSS-modul beskrivs i kapitel 4. Tröghetsnavigering ger ett fel som växer över tiden men genom att stötta tröghetsnavigeringssystemet med hastighetsmätningar kan feltillväxten reduceras avsevärt. Den kompetensuppbyggnad som genomförts inom hastighetsstöttad tröghetsnavigering beskrivs i kapitel 5. Kartstöttad navigering kan ge absoluta positionsuppdateringar (liksom GNSS-mottagare) och de möjliggör därmed längre operationer i telestörda miljöer. Sårbarheter och möjliga lösningar för att öka robustheten hos kartstöttade positionerings- och navigeringssystem beskrivs i kapitel 6. I kapitel 7 beskrivs de internationella samarbeten som projektet har deltagit i. I kapitel 8 diskuteras projektets verksamhet och resultat utifrån projektets övergripande frågeställningar. Slutligen, i kapitel 9, sammanfattas de viktigaste slutsatserna och rekommendationerna som framkommit under projektets arbete.

1.2 Projektet Robust PNT

Syftet med projektet Robust PNT var att öka kunskapen om hur PNT-systemen bör designas och användas för att öka tillförlitligheten och reducera risken för negativa konsekvenser vid exempelvis stör- och vilseledningsattacker. Denna kunskap ger även möjlighet att öka förståelsen rörande prestanda och sårbarheter hos de PNT-system som används av potentiella motståndare. Kunskapen ska även, tillsammans med resultat från

¹ Värnkraft - Inriktningen av säkerhetspolitiken och utformningen av det militära försvaret 2021-2025, Ds 2019:8, publicerad 14 maj 2019.

² Positionering, navigering och tid. I tekniska sammanhang utgörs ett PNT-system av en kombination av sensorer och algoritmer som beräknar plattformens position (i tre dimensioner i ett valt koordinatsystem), orientering (t.ex. uttryckt i roll, pitch och yaw) och tid enligt en vald tidsreferens (ofta uttryckt i UTC – Coordinated Time Universal).

³ Beställningsnummer AT.9220219 och beställningsnamn Ledning och MSI FOI 22.

angränsande forskning som bedrivs på FOI, bidra till att ge ett högkvalitativt stöd till FMV i kommande inriktnings- och kravställningsarbeten, samt expertstödsuppdrag.

1.2.1 Projektets frågeställningar

Projektet har haft följande övergripande frågeställningar:

- Hur ser omvärldsutvecklingen ut inom PNT-området?
- I vilka scenarion kan en robust GNSS-mottagare stöttad med gruppantennor ge en tillfredställande prestanda, och när krävs stöttning från alternativa navigeringssystem?
- Hur bör multifrekvens- och multikonstellationsmottagare, som använder kombinationer av krypterade och/eller öppna signaler från olika GNSS, designas för framtidens militära plattformar?
- Vilka stöttande deltekniker bör integreras i ett multisensornavigeringssystem för att uppnå önskad prestanda?
- Hur bör felaktigheter i referenskartor (exempelvis Lantmäteriets 3D-kartor) hanteras för att inte kraftigt försämra navigeringssystemets noggrannhet vid kartstöttad navigering?

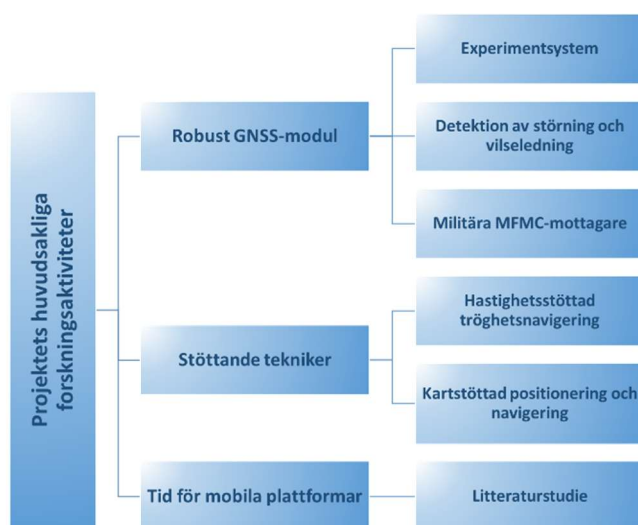
1.2.2 Forskningsaktiviteter

Projektet har genomfört tre huvudsakliga forskningsaktiviteter i syfte att adressera ovanstående frågeställningar: (i) robust GNSS-modul, (ii) stöttande tekniker och (iii) tid för mobila plattformar. Dessa delades upp i delaktiviteter enligt figur 1.1. Projektet har studerat tekniker som kommer att användas på ett flertal olika typer av plattformar.

1.2.2.1 Robust GNSS-modul

Forskningen som varit riktad mot kunskapsuppbyggnad kopplad till framtida robusta GNSS-moduler har studerat olika aspekter som bedömts vara kritiska för ett framtida militärt PNT-system med hög robusthet, tillförlitlighet och tillgänglighet. En delaktivitet har varit riktad mot att utveckla och utvärdera en arkitektur för detektion av oavsiktliga interferenser och avsiktliga stör- och vilseledningsattacker riktade mot GNSS-mottagare.

En annan delaktivitet har fokuserat mot kunskapsuppbyggnad rörande de nya krypterade signalerna GPS M-kod och Galileo PRS. Kunskapen rörande möjlig användning av civila okrypterade GNSS-signaler i militära tillämpningar har även förbättrats, framför allt sårbarheter mot olika typer av stör- och vilseledningsattacker.



Figur 1.1: Projektets huvudsakliga forskningsaktiviteter och tillhörande delaktiviteter.

Ett experimentsystem har även utvecklats i syfte att möjliggöra utvärderingar av en möjlig framtida robust GNSS-modul. Målet är att öka förståelsen för vilken nivå av robusthet som kan åstadkommas genom att kombinera:

- ett gruppantennbaserat störskyddssystem,
- algoritmer för detektion av stör- och vilseledningsattacker,
- krypterade GPS-signaler och civila multifrekvens- och multikonstellations-mottagare (Multi-Frequency Multi-Constellation, MFMC),
- tröghetsnavigeringssystem (TN-system) med olika kvalitet på tröghetssensorerna.

1.2.2.2 Stöttande positioneringstekniker

Två stöttande positionerings- och navigeringstekniker har valts ut och studerats under projektets gång. Syftet var att identifiera viktiga stöttande tekniker där det fanns ett behov av kunskapsuppbyggnad och de två områden som prioriterades var *kartstöttad navigering* samt *hastighetsstöttad tröghetsnavigering*. Kartstöttade positionerings- och navigeringssystem bedöms utgöra viktiga deltekniker framförallt i telestörda miljöer. Sådana tekniker utvecklas primärt inom FoT-område Sensorer och signaturanpassning men den delaktivitet som genomförts inom Robust PNT har kompletterat denna forskning genom att specifikt studera aspekter rörande hur felaktigheter och förändringar i referenskartor kan hanteras på ett mer robust sätt.

Ett behov av förbättrad kunskap i kunskapsavtappande FMV-projekt rörande hastighetsstöttad tröghetsnavigering för marina tillämpningar identifierades i projektberedningen inför 2021. Den genomförda delaktiviteten har därför fokuserat på att öka kunskapen rörande hur hastighetsstöttad tröghetsnavigering kan utvärderas för marina fartyg. Kunskapen är även applicerbar för markfordon och algoritmer för detta har implementerats.

1.2.2.3 Tid

En initial litteraturstudie riktad mot tid för mobila plattformar har påbörjats och planen är att slutföra detta arbete i december månad. Litteraturstudien avrapporteras i ett senare skede i ett separat FOI Memo.

1.2.3 Informationsspridning och samverkan

Forskningen inom PNT-området har historiskt sett varit uppdelad på olika projekt som genomförts inom flera FoT-områden (främst inom Ledning & MSI, Telekrig, Vapen och skydd, Sensorer och signaturanpassning samt Temaområde Autonomi och obemannat). Projektet Robust PNT, och dess föregångare, har initierat ett antal aktiviteter i syfte att sprida information internt mellan projekt och medarbetare som arbetat inom området. Syftet har varit att möjliggöra en synkronisering av forskningen och effektivisera kunskapsuppbyggnaden för de begränsade forskningsmedel som funnits tillgängliga. Exempel på interna aktiviteter som har genomförts inkluderar workshops, seminarier och introduktionsföreläsningar inom utvalda områden. Ambitionen är även att projekten gemensamt på sikt ska utveckla ett FOI-gemensamt simuleringsverktyg (*FOI Navtoolbox*).

Projektet har även initierat externa informationsspridningsaktiviteter inom området. En seminariedag genomfördes i januari 2023 under vilken olika FoT-projekt presenterade den forskning som genomförs inom området på FOI.

1.2.4 Avgränsningar

Projektets volym har varit begränsad i förhållande till bredden på forskningsområdet, vilket har begränsat hur stora resurser som har kunnat allokeras till de olika delaktiviteterna. Fokus har varit mot små och medelstora plattformar där kunskapsbehoven har bedömts vara störst, då det för dessa är svårast att skapa ett robust PNT-system som kan operera i längre perioder i telestörda miljöer. Generella tekniker har studerats som kan

komma att användas på ett stort antal militära plattformar i framtiden. Projektet har inte utvecklat eller utvärderat metoder för avsiktlig störning eller vilseledning mot en motståndares PNT-system. Vapentillämpningar har inte heller studerats.

1.3 Publikationer

Följande dokument har publicerats inom ramen för projektet:

- N. Stenberg, E. Axell och J. Rantakokko, *Smart störning mot GNSS – En undersökning av dess påverkan på en mottagare och en jämförelse med brusstörning*, Totalförsvarets forskningsinstitut, FOI-RH--2322--SE, december 2020. (Begränsat hemlig)
- J. Rydell, O. Karlsson, J. Nygårds och S. Nilsson, *Navigering genom robust kartmatchning och hastighetsstöttad dödräkning*, Totalförsvarets forskningsinstitut, FOI Memo 7719, december 2021.

Följande rapporter och Memo är under slutförande och publiceras i början av 2023:

- K. G. Olsson och E. Axell, *Utvärderingar av robusthetshöjande åtgärder för civil och militär GPS/GNSS*, Totalförsvarets forskningsinstitut. (Begränsat hemlig, under slutförande)
- F. Marsten-Eklöf och M. Alexandersson, *GPS M-kod – En översikt*, Totalförsvarets forskningsinstitut. (Begränsat hemlig, under slutförande)

Projektet har deltagit i framtagandet av följande publikationer inom Nato STO (Science and Technology Organization):

- NATO STO, *Navigation Sensors and Systems in GNSS Denied Environments – Final report*, STO Technical Report, STO-TR-SET-229, 2020.
- J. Nygårds och J. Rydell, "Cooperative navigation for UAV and ground units," *Proceedings of SET-275 Symposium on Cooperative Navigation in GNSS Degraded and Denied Environments*, STO-RSY-SET-275, Split, Kroatien, april 2021.

Projektet har även, i samarbete med FoT-projektet TK mot GNSS, handlett ett examensarbete:

- E. Beskow, *The Effect of Distortions Induced by Adaptive Antenna Arrays in GNSS Applications*, M.Sc. Thesis, Linköpings Universitet, LiTH-ISK-EX--22/5526--SE, oktober 2022.

Projektet har i samarbete med Linköpings Universitet fått en artikel publicerad:

- N. Stenberg, E. Axell, J. Rantakokko och G. Hendeby, "Results on GNSS Spoofing Mitigation Using Multiple Receivers," *NAVIGATION, Journal of the Institute of Navigation*, vol. 69, nr. 1, mars 2022.

2 Framtida robusta PNT-system

Den pågående forskningen och utvecklingen inom PNT-området pekar tydligt på att ett multisensorbaserat integrerat PNT-system är en förutsättning för att åstadkomma ett robust PNT-system som kan operera i militära scenarion (där telestörda miljöer är en realitet).

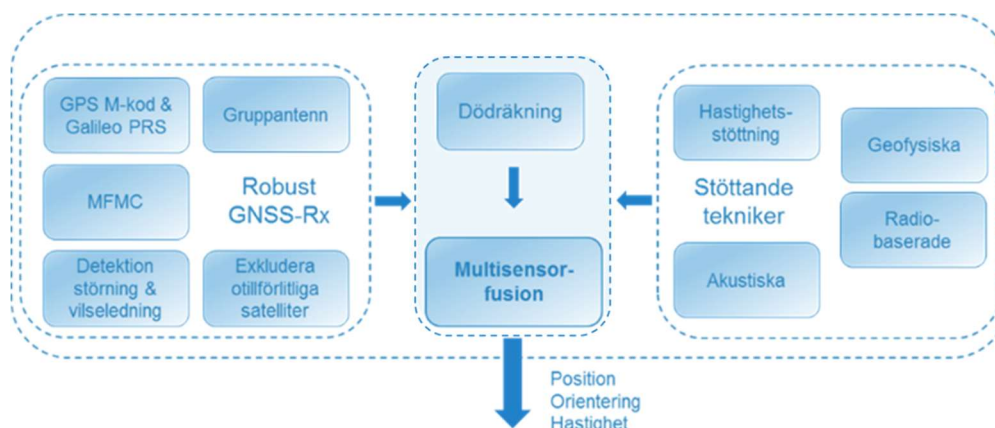
Framtida militära PNT-system kommer sannolikt att baseras på ett dödräkande system som beräknar position, hastighet och orientering. I de flesta fall kommer dödräkningen realiseras i form av ett tröghetsnavigeringssystem (TN-system). Dessa system uppvisar dock ett fel som växer kontinuerligt med tiden (eller förflyttning). En robust GNSS-modul kommer även att användas. GNSS-mottagare och TN-system har komplementär felkaraktäristik där TN-systemet ger hög noggrannhet under korta perioder men har ett fel som växer med tiden, medan en GNSS-mottagare ger (jämförelsevis) brusiga estimat av position och hastighet men där felet inte växer över tiden. I telestörda miljöer är dock risken hög att GNSS-mottagaren under kortare eller längre perioder, beroende på scenariot, inte ger tillförlitliga estimat. För att ”överbrygga” dessa perioder behöver ytterligare stöttande sensorer och delsystem integreras för att möjliggöra genomförandet av operationer under längre perioder i telestörda miljöer. Ett förslag på arkitektur för framtida militära PNT-system ges i figur 2.1 [1].

2.1 GNSS

Ett stort antal PNT-system är helt eller delvis beroende av GNSS-mottagare för att estimerar plattformens position, hastighet och för tidssynkronisering av olika elektroniska system. Det finns idag fyra globala satellitnavigeringssystem: GPS, GLONASS, Galileo och BDS-3/Beidou (figur 2.2). Det europeiska Galileo är det enda system som är under civil kontroll. Alla GNSS sänder flera tjänster, på flera frekvenser, varav vissa är öppet tillgängliga för alla att använda medan andra tjänster är kontrollerade och avsedda för framförallt militära användare. GPS sänder exempelvis på frekvenserna L1, L2 och L5 (figur 2.3). De frekvensband som de andra systemen använder överlappar delvis men inte helt och hållet.

2.1.1 Sårbarheter

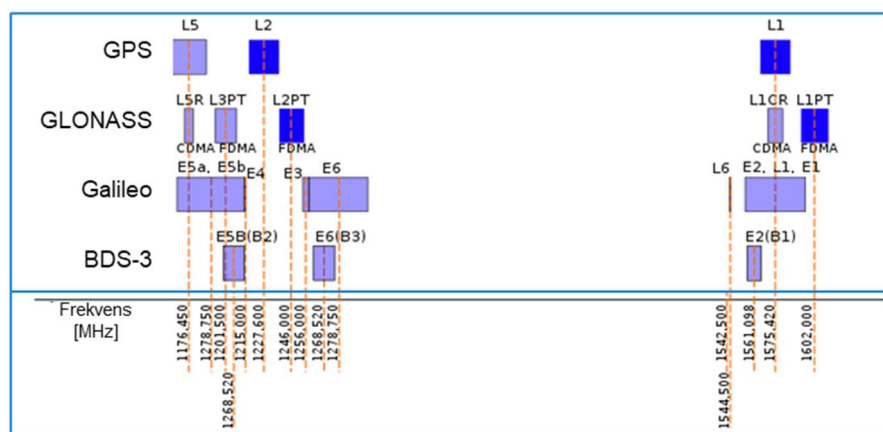
Satelliterna befinner sig typiskt på avstånd mer än 20 000 km från jordytan vilket medför att GNSS-signalerna är svaga när de når mottagarna (svagare än bakgrundsbruset). Detta medför att även små störsändare som sänder med låg effekt kan få ett stort effektovertag gentemot GNSS-signalerna när de befinner sig i närheten av mottagaren.



Figur 2.1: Förslag på övergripande arkitektur för ett robust multisensorbaserat PNT-system, bestående av ett dödräkande delsystem som stöts av en robust GNSS-modul och av ytterligare stöttande tekniker som ökar noggrannheten vid operationer i telestörda miljöer [1].



Figur 2.2: Fyra globala GNSS är i drift: GPS (USA), GLONASS (Ryssland), Galileo (EU) och BDS-3/Beidou (Kina). (Illustrationer: Wikipedia).



Figur 2.3: Frekvensanvändning för de olika GNSS-tjänsterna. (Illustration: Wikipedia).

Militära fordonsbaserade störsystem kan använda höga störeffekter (tiotals kW) vilket under frisiktsförhållanden resulterar i mycket långa störavstånd. Det är i praktiken ofta jordens kurvatur och dämpning från terräng och vegetation som begränsar störavstånden för dessa störsystem.

När en mottagare utsätts för störning påverkas mottagaren på olika sätt beroende på störsignalens effekt och delvis även av störarens egenskaper. En kraftig störsignal riskerar att helt slå ut mottagarens möjlighet att estimerar position, hastighet och tid medan en svagare störsignal istället resulterar i en försämrad noggrannhet i dessa estimat. I jämförelse så utgör vilseledningsattacker ett potentiellt allvarligare problem. När en mottagare utsätts för en vilseledningsattack kan den i värsta fall börja leverera en felaktig position och/eller tid. Vid en vilseledningsattack kan även en mottagare, som saknar tillförlitlig integritetsmonitorering och detektion av stör- och vilseledningsattacker, ange att dess positionsestimat är tillförlitligt. I vissa miljöer, såsom inomhus och i underjordiska komplex, dämpas GNSS-signalerna kraftigt vilket medför att tillgängligheten är begränsad i dessa miljöer. Sårbarheterna hos användar-, rymd- och kontrollsegmenten för GNSS sammanfattas i exempelvis [1-2].

2.1.2 Robust GNSS-modul

Robustheten mot störning och vilseledning i framtida GNSS-mottagare som används i militära tillämpningar (ca 2025) kan förbättras avsevärt (figur 2.1):

- Använd en GPS M-kodsmottagare och förbered för att införa mottagarkort även för Galileo PRS när dessa blir tillgängliga och tjänsten är operativ.

- Integrera ett gruppantennbaserat störskyddssystem.
- Implementera tillförlitliga detektionsmetoder som kan upptäcka (och varna) när mottagaren riskerar att vara påverkad av en stör- eller vilseledningsattack (dessa metoder beskrivs närmare i kapitel 3).

På längre sikt kan även öppna civila signaler komma att inkluderas (multifrekvens- och multikonstellationsmottagare, MFMC GNSS-mottagare).

På militära plattformar används oftast krypterade signaler (GPS P(Y)-kod), vilka ger en ökad robusthet exempelvis i form av en ökad robusthet mot vilseledningsattacker. En ny krypterad militär GPS-signal (M-kod) är under införande. Även Galileo utvecklar en krypterad tjänst, Public Regulated Service, som kommer att ha liknande egenskaper som GPS M-kod. Galileo PRS kommer att användas av militära användare inom EU men den är även avsedd att användas av andra aktörer inom civil säkerhet och beredskap. GPS M-kod och Galileo PRS kommer att ge ett antal viktiga fördelar såsom ett förbättrat störskydd och tillgänglighet, samt möjlighet att störa ut öppna signaler i samma frekvensband utan att PRS- eller M-kodsmottagarna störs ut (Blue-Force-Electronic-Attack, BFEA).⁴ Krypterade mottagare har även ett avsevärt bättre skydd mot många olika typer av vilseledningsattacker. Även dessa mottagare riskerar dock att störas ut vid operationer i telestörda miljöer.

Genom att använda ett gruppantennbaserat störskyddssystem kan stör- och vilselednings-signaler undertryckas genom spatiotemporal filtrering.⁵ Gruppantenner ger en kraftigt förbättrad robusthet och bör införas i militära PNT-system där så är praktiskt möjligt. De vanligaste gruppantennsystemen använder fyra eller sju antennelement, där de förstnämnda är utvecklade primärt för användning på mindre plattformar. Gruppantennbaserade störskyddssystem integreras internationellt på exempelvis stridsflygplan, marina fartyg, fordon och styrda vapen. Det är dock utmanande att integrera gruppantenner på plattformar med stringenta krav på storlek, vikt och effektförbrukning, såsom små obemannade farkoster (typ UAV05 och UAV06) och i soldatsystem.

Gruppantennbaserade störskyddssystem kan undertrycka starka störsignaler men det finns en övre gräns för hur starka störsignaler som de kan hantera. En gruppantenn med fyra antennelement kan typiskt undertrycka maximalt tre okorrelerade störsignaler som kommer från olika riktningar. Dagens gruppantennsystem kan även leda till att autentiska satellitsignaler undertrycks eller distorderas, vilket kan försämra mottagarens prestanda [3]. Nya mer avancerade algoritmer kan reducera dessa problem, men till priset av en ökad komplexitet i mjukvara och hårdvara. Moderna gruppantenner har även förmåga att estimerar störarnas effekt och infallsriktning och på så sätt bidra till lägesbilden.

Civila kommersiella mottagare använder flera GNSS och även signaler på flera frekvenser (MFMC-mottagare). Det finns flera potentiella fördelar med att även i militära tillämpningar använda de öppna civila GNSS-signalerna som komplement till de krypterade signalerna. Vissa av de moderna öppna signalerna har en stor bandbredd vilket ökar positionsnoggrannheten och reducerar påverkan från flervägsutbredning i exempelvis urbana miljöer. Genom att använda signaler från två konstellationer, som GPS och Galileo, kommer antalet synliga satelliter att approximativt fördubblas. Även detta ger en ökad positionsnoggrannhet samtidigt som det ger en ökad systemredundans. Att använda både GPS och Galileo kan även minska de problem som kan uppstå då gruppantenner används där även vissa GNSS-signaler undertrycks oavsiktligt. Det bedöms dock inte vara aktuellt att på bred front integrera även de civila öppna signalerna i militära mottagare under de närmaste åren. Det finns flera sårbarheter med dessa signaler, där känsligheten mot vilseledningsattacker är den allvarligaste. Då signalernas uppbyggnad är känd kan kopior av dessa genereras och sändas ut med relativt enkel och billig hårdvara.

⁴ www.gpsworld.com/new-military-code-about-to-board-700-platforms/ (besökt 2023-01-11).

⁵ www.gpsworld.com/anti-jam-technology-demystifying-the-crpa/ (besökt 2023-01-11).

För att civila signaler ska kunna användas som ett komplement till de krypterade signalerna i militära mottagare måste tillförlitlig integritetsmonitorering utvecklas och införas. Integritetsmonitoreringen bör helst appliceras på de enskilda GNSS-signalerna. Fortsatt forskning behöver även genomföras i syfte att utvärdera olika metoder för hur de civila signalerna (eller tjänsterna) ska fusioneras med de krypterade signalerna (eller tjänsterna). Att inkludera fler signaler på nya frekvenser och med större bandbredd ökar komplexiteten hos mottagaren och därmed även kostnaden.

2.2 Stöttande positioneringstekniker

Det finns ett stort antal sensorer och deltekniker som är möjliga att använda för att stötta PNT-systemet i situationer där GNSS-mottagaren är utstörd eller inte kan ge tillförlitliga estimat. Vilka sensorer och delsystem som bör användas beror på operationsmiljö, existerande sensorer på plattformen (och om exempelvis spaningssensorer på mindre farkoster även kan användas för att stötta PNT-systemet) och plattformens begränsningar (framförallt när det gäller storlek, vikt, effektförsörjning och kostnad). På grund av det stora antalet tekniker ges här endast en översiktlig beskrivning av olika typer av stöttande sensorer och delsystem. Tekniker som är lämpliga för marina tillämpningar beskrivs i [1].

Hastighetsstöttad tröghetsnavigering är en effektiv metod för att reducera feltillväxten för ett TN-system [4]. Hastighetsmätningar kan tillhandahållas med olika typer av sensorer, exempelvis genom odometri för markfordon, Dopplerhastighetsmätare (Doppler Velocity Log, DVL) för fartyg eller kameror (visuell odometri) för UAV:er. Då dessa sensorer ofta finns tillgängliga så bör hastighetsstöttningsmetoder inkluderas som en central del av ett framtida PNT-system. Tillförlitlig osäkerhetsestimering, som identifierar de tillfällen då hastighetsmätningarna riskerar att vara behäftade med stora fel, behöver dock integreras då exempelvis odometri från banddrivna fordon i vissa situationer kan ge stora fel.

Det finns ett stort antal radiobaserade system som potentiellt kan användas som komplement till GNSS beroende på tillämpning [1]. Ett system med markbaserade dedikerade radiosändare kan även byggas upp som, beroende på systemparametrar som frekvens och mästhöjder, täcker ett lokalt eller regionalt område. En mottagare beräknar avstånden till de kända sändarpositionerna och utifrån dessa mätningar beräknas mottagarens position. Även enstaka avståndsmätningar kan reducera felen och bör inkluderas om de är tillgängliga. Möjligheten att mäta avstånd kan exempelvis implementeras i kommunikationslänken till en obemannad farkost. Civila radiosystem kan användas om de fungerar och även bedöms vara tillförlitliga. Det finns även möjlighet att använda andra radiosändare, som inte är direkt avsedda för PNT-tillämpningar, i syfte att förbättra positionsestimatet (s.k. opportunistisk användning av radiosignaler). Ett alternativ till GNSS är att använda lågflygande satelliter (Low Earth Orbit, LEO) där signalerna på grund av det kortare avståndet till mottagarna kan vara avsevärt starkare. Utveckling av dedikerad PNT-nyttolast pågår, bland annat i syfte att på sikt komplettera Galileosatelliterna. Majoriteten av LEO-satelliterna kommer dock inte att ha sådan nyttolast men det är ändå ofta möjligt att mäta avståndet till satelliterna (som oftast kommer att sända information med radio) med opportunistiska signalbehandlingsmetoder. Även om dessa avståndsestimat kan ha relativt stora fel så kommer det stora antalet tillgängliga mätningar att reducera det resulterande positionsfelet för mottagaren.

En annan klass av PNT-tekniker som bör användas utnyttjar olika geofysiska egenskaper i omgivningen. Dessa tekniker använder framför allt information och mätningar av magnetfält, gravitationsfält eller olika egenskaper hos den omgivande miljön. Då dessa mätningar jämförs med föruppmätta georefererade kartor (databaser) så ger de även möjlighet att estimeras mottagarens absoluta position. Detta är en viktig egenskap eftersom de då, liksom GNSS-mottagare, på ett bra sätt kompletterar exempelvis dödräknande tekniker vars fel ökar med tiden (eller förflyttning). Exempel på tekniker som utnyttjar geofysiska egenskaper är kartmatchning baserat på kameror och referensbilder, terräng- eller batymetriskt stöttad navigering, stjärnnavigering och matchning av mätningar av magnetfält eller gravitation med databaser (typiskt mot lokala anomalikartor). Vissa

databaser innehåller dock begränsad information på så sätt att variationerna är små för korta förflyttningar. Det gäller exempelvis magnet- och gravitationsfält där anomali-kartorna i många miljöer har en låg upplösning och där variationerna typiskt är små (förutom i tätbebyggda områden där magnetfältet kan variera kraftigt). Ofta används speciella sensorfusionsmetoder, exempelvis olika typer av partikelfilter, för att inkludera denna typ av information i PNT-systemet. I situationer då kartor eller databaser inte finns tillgängliga i förväg så används ofta SLAM-metoder (Simultaneous Localization and Mapping) som kontinuerligt bygger en karta (landmärkesdatabas) samtidigt som den positionerar sig. Detta kan ge en ökad noggrannhet samtidigt som det möjliggör en reducering av felet (s.k. loop closure) när farkosten återvänder till ett tidigare passerat område.

I specifika marina tillämpningar kan eventuellt även aktiva akustiska metoder användas [1].

3 Detektion av störning och vilseledning

I detta kapitel beskrivs implementation och utvärderingar av en hård- och mjukvaru-arkitektur för detektion av stör- och vilseledningsattacker. Detta utgör en del av det experimentsystem som beskrivs närmare i kapitel 4. Arbetet baseras på tidigare arbete som genomförts på FOI [6-13]. Arkitekturen beskriver vilka detektionsalgoritmer som bör användas samt hur de kan kombineras för att ge en robust detektion av störning och vilseledning med låg falsklarmssannolikhet. Detektionssystemet består av två antenner med separata GNSS-mottagare och en delmängd av algoritmerna för detektion av vilseledningssignaler utnyttjar att information från två (eller fler) geografiskt separerade mottagare är tillgängliga.

Utvalda resultat redovisas nedan medan både algoritmer och resultat beskrivs mer utförligt i [5].

3.1 Systembeskrivning

Detta avsnitt beskriver hur hårdvara, mjukvara och detektionsalgoritmer har kombinerats och implementerats.

3.1.1 Arkitektur för detektion

Figur 3.1 visar en översiktlig skiss av arkitekturen för det föreslagna detektionssystemet. Hårdvaran inkluderar två civila GNSS-mottagare (u-blox), med rumsligt separerade antenner, och en USRP (Universal Software Radio Peripheral). USRP:n används endast för energidetektion.⁶ Systemet kan även användas med enbart en GNSS-mottagare, med begränsningen att de detektionsmetoder som baseras på data från flera mottagare inte kan användas.

Detektionsalgoritmerna är implementerade i mjukvaruramverket ARM-PIT som är en vidareutvecklad version av den öppet tillgängliga mjukvaran PNT Integrity Toolkit som släpptes 2021.⁷ PNT Integrity Toolkit inkluderar implementationer av flera av de algoritmer som FOI har studerat och ger även möjlighet att i realtid demonstrera möjligheterna till detektion av störning och vilseledning. ARM-PIT har implementerats i det experimentsystem för en framtida robust GNSS-modul som beskrivs i kapitel 5.

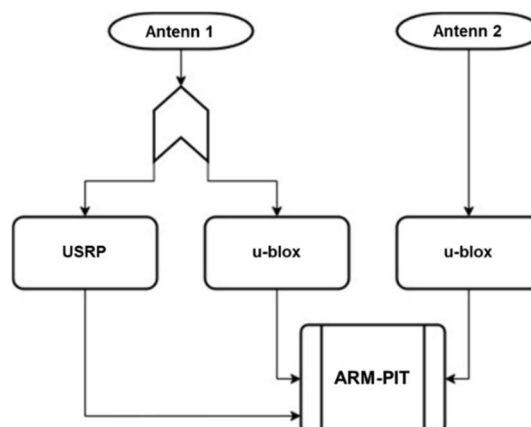
Ett detektionssystem bestående av två militära GPS-mottagare, istället för civila GNSS-mottagare, har också utvärderats [5].

3.1.2 Mjukvara och detektionsalgoritmer

Ett tillförlitligt detektionssystem bör innehålla en kombination av flera detektionsalgoritmer som kan upptäcka olika typer av störning och vilseledning. I detta avsnitt beskrivs den mjukvara som har använts och intressanta detektionsalgoritmer beskrivs översiktligt. Ett urval av dessa algoritmer bör kombineras för att uppnå en hög tillförlitlighet (detektionssannolikhet).

⁶ I en framtida utveckling kan data från USRP användas i en mjukvarubaserad GNSS-mottagare (t.ex. GNSS-SDR, gnss-sdr.org) vilket kan ge tillgång till mottagarintern information som inte är tillgänglig från kommersiella GNSS-mottagare.

⁷ PNT Integrity Toolkit (PIT) är ett ramverk med ett antal komplementära algoritmer för detektion av störning och vilseledning av GNSS-mottagare. Ramverket är utvecklat av IS4S (Integrated Solutions for Systems) och har släppts som öppen källkod på GitHub av CISA (Cybersecurity and Infrastructure Security Agency). Se: github.com/cisagov/PNT-Integrity-Toolkit (besökt 2022-12-16).



Figur 3.1: Arkitektur för detektionssystemet med två separerade antenner, två civila GNSS-mottagare och en USRP. Detektionsalgoritmerna finns implementerade i mjukvaruramverket ARM-PIT.

3.1.2.1 Implementation av detektionsalgoritmer

För att kunna upptäcka olika typer av vilseledning bör en kombination av detektionsalgoritmer implementeras. I [6-7, 9, 14] beskrivs olika typer av stör- och vilseledningsattacker, hur detektionsalgoritmer kan kombineras samt vilka sorters attacker de kan detektera. För att nå en hög tillförlitlighet föreslås att en kombination av *energidetektion*, *rimlighetskontroller* av utdata samt *mottagarintern övervakning* (av oväntade plötsliga ändringar i mottagarinterna data) implementeras. Om det är möjligt att använda information från flera mottagare (med geografiskt separerade antenner) bör detektionsmetoder som utnyttjar information från flera antenner användas då de ger en god förmåga att upptäcka vanliga typer av vilseledningsattacker.

Detektionsramverket ARM-PIT utvärderar pålitligheten hos GNSS-mottagarna genom att utföra ett antal olika kontroller, för att sedan vikta ihop alla delresultat till ett slutgiltigt utlåtande om mottagaren är utsatt för störning eller vilseledning. Genom att välja ett urval av kontroller (detektionsalgoritmer), och anpassa detektionströsklar och hur algoritmerna viktas ihop, så kan utvärderingen anpassas efter hur scenariot ser ut. För en stillastående plattform så kan till exempel denna kunskap utnyttjas för att upptäcka när en mottagare blir utsatt för vilseledning, men om mottagaren istället är monterad på ett fordon som är i rörelse behöver positionen från GNSS-mottagaren istället kontrolleras mot en rörelsemodell (som i dess enklaste form kan ange fordonets maxhastighet) för fordonet.

Den ursprungliga mjukvaran PNT Integrity Toolkit har modifierats, dels de individuella detektionsalgoritmerna och dels genom utökad funktionalitet. Ramverket har även utökats med funktionaliteten att använda inspelade data, vilket ger möjlighet att utvärdera inspelade scenarion i efterhand. Denna möjlighet har använts för att utvärdera olika algoritmer på data från fältförsök där störning och vilseledning har genomförts, varefter framför allt olika kombinationer av detektionsmetoder har utvärderats.

3.1.2.2 Detektion av störning

Flera sammanställningar av detektion av störning har gjorts tidigare bl.a. i [6-7, 14-16]. Baserat på dessa arbeten kan de mest intressanta algoritmerna för detektion av störning grupperas enligt följande:

- energidetektion,
- befintliga mottagarinterna detektorer,
- analyser av utdata från GNSS-mottagare (t.ex. analyser av C/N_0),
- multipla antenner eller syntetisk array (förflyttning av antenn).

Energidetektion har visat sig vara ett effektivt och relativt enkelt mått och det kan implementeras genom direkt mätning av mottagen energi där den mottagna signalen

normalt digitaliseras varefter denna energi estimeras [7]. Alternativt kan det göras via analyser av data som kan finnas tillgängliga från kommersiella mottagare t.ex. AGC (Automatic Gain Control) [17-18].

Enskilda detektorer kan inte alltid skilja mellan störning och dåliga signalförhållanden, exempelvis om mottagaren befinner sig inomhus eller miljön orsakar kraftig flervägs-utbredning [19]. Det gäller exempelvis detektorer som använder estimat av C/N_0 . På liknande sätt så kan exempelvis en energidetektor inte avgöra om mottagaren är utsatt för störning eller vilseledning. Genom att kombinera flera algoritmer, eller olika typer av data, förbättras möjligheten att diskriminera mellan dessa olika fall [14].

I ARM-PIT finns följande metoder implementerade för detektion av störning (tabell 3.1):

- *EnergyDetectionCheck* räknar ut den totala mottagna energin hos den signal som digitaliseras med hjälp av USRP:n och rapporterar störning ifall energin når över en fördefinierad tröskelnivå.
- *AgcCheck* markerar ifall AGC-nivån från GNSS-mottagaren sjunker under ett visst tröskelvärde.
- *LowCnoCheck* rapporterar störning då en förutbestämd andel av alla C/N_0 -estimat sjunker under en angiven nivå.

3.1.2.3 Detektion av vilseledning

Baserat på [6, 8-14] bedöms följande tre generella typer av metoder för detektion av vilseledning vara relevanta för denna studie: (i) energidetektion, (ii) multipla antenner och (iii) rimlighetskontroller av informationen i, eller från, en GNSS-mottagare, där en möjlighet är att jämföra resultaten med information från stöttande sensorer (t.ex. från tröghetssensor [20]).

Energidetektion kan upptäcka vilseledningssignaler som är starka. Vid energidetektion används även för detektion av vilseledning mätten *EnergyDetectionCheck* och *AgcCheck*.

Flerantennsystem kan användas för detektion på olika sätt. En gruppantenn kan effektivt undertrycka stör- och vilseledningssignaler och moderna gruppantennsystem kan dessutom estimeras infallsriktningen för dessa. Om flera mottagare används, med geografiskt separerade antenner, kan vilseledning detekteras genom att exempelvis jämföra deras positionsestimat eller genom analyser av deras pseudoavståndsmätningar eller fasskillnadsmätningar (genom att beräkna s.k. dubbeldifferenser) [8, 10-13]. Avståndet mellan antennerna bör då vara fixt (och känt), vilket i praktiken innebär att antennerna är placerade på samma plattform, eller kontinuerligt mätas upp i scenarion där olika plattformar samverkar. I praktiken bör antennerna i detta fall vara separerade åtminstone ett par meter men prestanda förbättras om avståndet ökar ytterligare.

Ett stort antal rimlighetskontroller kan genomföras i syfte att försöka detektera när en mottagare har utsatts för en vilseledningsattack [6]. Dessa ger dock utslag först efter att mottagaren har blivit påverkad och redan börjat leverera felaktiga mätningar.

- Vilseledning av en delmängd av konstellationer och frekvenser kan upptäckas genom jämförelser av position, hastighet och tid mellan de resultat som erhålls för olika konstellationer eller frekvensband.
- Interna data i mottagare, t.ex. plötsliga förändringar i bärvågens amplitud och fas, eller övervakning av distorsioner av korrelationsfunktioner kan indikera att en mottagare blivit påverkad av vilseledning [14, 21].
- Avkodade navigationsdata. Kontrollera rimlighet hos data t.ex. för satellitpositionerna.
- Leta efter kopior av GNSS-signalerna i acquisitionfasen, vilket indikerar att mottagaren utsätts för flervägsutbredning eller vilseledning (s.k. brute-force acquisition) [14].

Tabell 3.1: Exempel på mått som används i ARM-PIT vid detektion av stör- och vilseledningsattacker.

Typ	Benämning	Beskrivning
Energi	<i>EnergyDetectionCheck</i>	Räknar ut den totala mottagna energin och varnar för misstänkt störning eller vilseledning ifall energin överstiger ett tröskelvärde.
	<i>AgcCheck</i>	Varnar ifall AGC-nivån från GNSS-mottagaren sjunker under ett visst tröskelvärde.
C/N ₀	<i>LowCnoCheck</i>	Rapporterar störning då en förutbestämd andel av alla C/N ₀ -estimat sjunker under en given nivå.
	<i>HighCnoCheck</i>	Ger varning för vilseledning om estimaten för C/N ₀ är orimligt höga.
	<i>CnoCheck</i>	Beräknar typnivåer för C/N ₀ och varnar för vilseledning ifall för många estimat har samma värde.
Position & hastighet	<i>AltitudeCheck</i>	Jämför höjden och varnar om höjdestimatet är orimligt enligt rörelsemodell (eller karta för markfordon).
	<i>VelocityCheck</i>	Jämför hastigheten mot vad som är möjligt enligt angiven rörelsemodell.
	<i>StaticPositionCheck</i>	Används för stationära plattformar/system. Markerar ifall den rapporterade positionen har rört sig bort från en bestämd position.
	<i>PositionJumpCheck</i>	Jämför nuvarande position med den senaste position som är markerad som pålitlig (den senaste positionen där vilseledning inte har detekterats). Förberedd för att använda position från stöttande sensorer och jämföra med GNSS-mottagarens position.
	<i>PositionVelocity ConsistencyCheck</i>	Använder föregående position och hastighet för att ta fram en rimlig gräns för var mottagaren bör befinna sig i nästa tidpunkt. Om nästa position befinner sig utanför denna gräns ger den en varning.
Flera mottagare	<i>AngleOfArrivalCheck</i>	Jämför estimerade pseudoavstånd och markerar ifall skillnaden mellan ankomstvinklar är för små.
	<i>RangePositionCheck</i>	Jämför ifall mottagarnas rapporterade positioner stämmer överens med det faktiska avståndet mellan mottagarna.

Genom att analysera utdata från mottagaren som levereras i t.ex. NMEA-meddelanden kan indikationer på att mottagaren är utsatt för vilseledningsattacker erhållas [6, 9]. Exempel på analyser som kan genomföras är:

- Tid. Den rapporterade tiden skall öka monotont och avvikelser indikerar att mottagaren är vilseledd. Vissa typer av vilseledning, t.ex. repeterstörsändning (dvs. mottagning och återutsändning av de autentiska GNSS-signalerna) kan detekteras genom abrupta avvikelser i klockbias [22].⁸
- Position och hastighet. Genom att jämföra positionen och/eller hastigheten från en GNSS-mottagare med en rörelsemodell för plattformen kan avvikelser detekteras. Rörelsemodellen kan t.ex. innehålla maximal acceleration, hastighet och altitud. Även kartunderlag kan nyttjas i en rörelsemodell. Resultaten från mottagaren kan även jämföras mot de positioner och hastigheter som erhålls från stöttande sensorer (t.ex. jämförelse med data från tröghetssensor [20]) eller andra GNSS-mottagare [10-11]).
- Pseudoavstånd kan utnyttjas i jämförelser med en rörelsemodell på liknande sätt som position och hastighet, men det kan göras separat för varje satellitsignal. Pseudoavstånd från flera mottagare kan också kombineras för att upptäcka vilseledning [10, 12]. Pseudoavståndsestimat finns dock inte tillgängligt som utdata från alla typer av mottagare.
- Orimligt höga C/N₀-estimat, eller att den naturliga variationen mellan satelliterna saknas, utgör indikationer på pågående vilseledningsförsök.

De olika metoder som finns implementerade i ARM-PIT för detektion av vilseledningsattacker beskrivs i tabell 3.1. Hur beslutströsklarna för detektionsalgoritmerna bör sättas beror på hur resultatet ska användas. För en detektionsalgoritm är det alltid en kompromiss mellan falsklarmssannolikhet och detektionssannolikhet (eller sannolikhet för missad detektion).

⁸ Även avvikelser i 1PPS-signal kan användas, men detta förutsätter att en extern noggrann oscillator finns tillgänglig för jämförelser.

Vilken typ av fel, falsklarm eller missade detektioner, som är viktigast att minimera beror på hur resultatet ska användas. I vissa fall kan det vara viktigast att varna om det finns en liten risk för störning eller vilseledning, men i andra fall kan det skapa problem om algoritmen ofta varnar felaktigt för störning eller vilseledning. I denna rapport har besluts-trösklarna bestämts så att falsklarm undviks med marginal i de utvärderingar som gjorts.

3.1.2.4 Kombinationer av detektionsalgoritmer

Detektionsalgoritmer kan kombineras på olika sätt, t.ex. genom en lämplig linjärkombination av individuella kontroller. I ARM-PIT kan detta anpassas efter situation och det ger användaren möjlighet att välja vilka algoritmer som ska kombineras för att besluta ifall systemet är utsatt för störning eller vilseledning. I ARM-PIT avgörs det slutgiltiga beslutet genom att vikta och summera ihop resultatet från de individuella kontrollerna.

Varje kontroll tar ett värde $T_m \in \{-1, 0, 1\}$ där $T_m = -1$ då detektionsalgoritmen markerar en störning, $T_m = 1$ avser ingen störning och $T_m = 0$ är ett mellanläge, ett osäkert läge. Till varje kontroll hör en individuell vikt, w_m , som kan användas för att prioritera vissa kontroller över andra. Samtliga vikter är i detta arbete satta till 1. Att utvärdera detta val av vikter och finna en väl avvägd uppsättning av individuella vikter bör studeras vidare.

Det sammanvägda detektionsmålet beräknas som

$$D_m = \frac{\sum_{m=1}^M w_m T_m}{\sum_{m=1}^M w_m} \in [-1, 1],$$

där M är antalet olika detektionsmål som används. D_m avrundas slutligen till närmaste heltal och kommer (likt de individuella kontrollerna) därmed anta tre olika nivåer:

- $D_m = -1$ är en varning för att mottagaren med hög sannolikhet är utsatt för en stör- eller vilseledningsattack,
- $D_m = 1$ innebär att sannolikheten för att mottagaren är utsatt för en stör- eller vilseledningsattack är låg,
- $D_m = 0$ indikerar att det råder en stor osäkerhet rörande huruvida mottagaren är utsatt för en stör- eller vilseledningsattack.

3.2 Utvärderingar

Följande avsnitt beskriver de fältförsök och utvärderingar som har genomförts av ovanstående metoder för detektion av förekomsten av stör- och vilseledningssignaler.

3.2.1 Beskrivning av genomförda tester

I de genomförda testerna användes två GNSS-mottagare (u-blox F9P) med lagring av data via ARM-PIT. En USRP B210 mini användes även för lagring av komplexa basbandsdata med 4 MHz bandbredd. Testerna genomfördes med stationära sändar- och mottagarpositioner enligt figur 3.2.

Under fältförsöket utfördes följande tre tester:

- *Test 1:* Bredbandig brus (24 MHz). Mottagarantennerna var placerade på ett avstånd under två meter från varandra (figur 3.2).
- *Test 2:* Repeterstörning. Mottagarantennerna var placerade på ett avstånd under två meter från varandra (figur 3.2).
- *Test 3:* Repeterstörning. Mottagarantennerna var placerade på ca 10 meters avstånd från varandra.

Vid repeterstörning ändras sändareffekten i steg om 2 dB med en minuts intervall, upp till 70 dB, medan den maximala relativa störnivån vid bredbandig brusstörning går upp till 60 dB. Även de absoluta effektnivåerna skiljer vid brusstörning respektive vilseledning. Ytterligare tester och utvärderingar genomfördes med militära GPS-mottagare (GPS 6510), störskyddsantenn Novatel GAJT och detektionssystemet BroadSense Nano [5].



Figur 3.2: Stationärt test sett från sändarpositionen (vänster) respektive mottagarpositionen (höger). (Foto: FOI).

3.2.2 Resultat

För detektion av störning användes detektionsalgoritmerna *AgcCheck*, *LowCnoCheck* och *EnergyDetectionCheck*. Vid detektion av vilseledning användes istället metoderna *AgcCheck*, *EnergyDetectionCheck*, *AltitudeCheck*, *PosJumpCheck*, *RangePositionCheck*, *StaticPositionCheck* samt *VelocityCheck*.

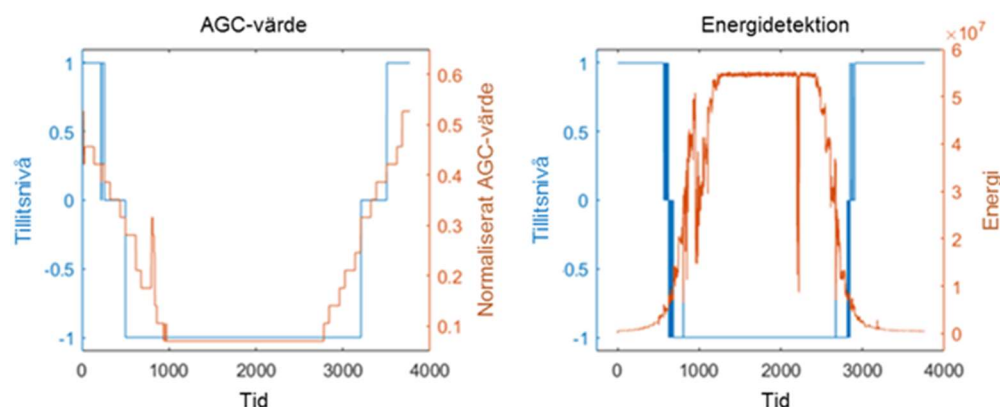
Metoderna *AgcCheck* och *EnergyDetectionCheck* ger båda ett mått av signalens energi. AGC är en mottagarintern adaptiv förstärkning av den ingående signalen som försöker hålla signalens amplitud approximativt konstant i mottagaren. Det innebär att AGC-värdet är omvänt proportionellt mot störeffekten, dvs. AGC-värdet minskar när störeffekten ökar. Eftersom detektion baserat på AGC-värdet kan ses som en kvantiserad version av energidetektion så bör energidetektion kunna ge lika bra resultat (i form av detektionskänslighet för motsvarande falsklarmssannolikhet) som att använda AGC-värden.

Att kontrollera AGC-värdet eller energinivån är ett effektivt sätt att upptäcka både en störattack och en vilseledningsattack, se figur 3.3 och 3.4. Både energidetektionen och AGC-värdet indikerar tidigt att mottagaren är utsatt för störning eller vilseledning. Brusstörning kan exempelvis detekteras innan den använda mottagarens positionsestimat påverkas. Hur repeterstörning påverkar mottagaren varierar beroende på typ av mottagare men figur 3.4 indikerar att även vilseledningssignaler kan detekteras vid motsvarande låga signalnivåer. Att *AgcCheck* indikerar störning tidigare än *EnergyDetectionCheck* orsakas av att tröskelvärdena är empiriskt valda baserat på begränsade mängder mätdata. Trösklarna för energidetektionen kan sänkas utan att ge en högre feldetektionssannolikhet än för metoden som använder AGC-värden.

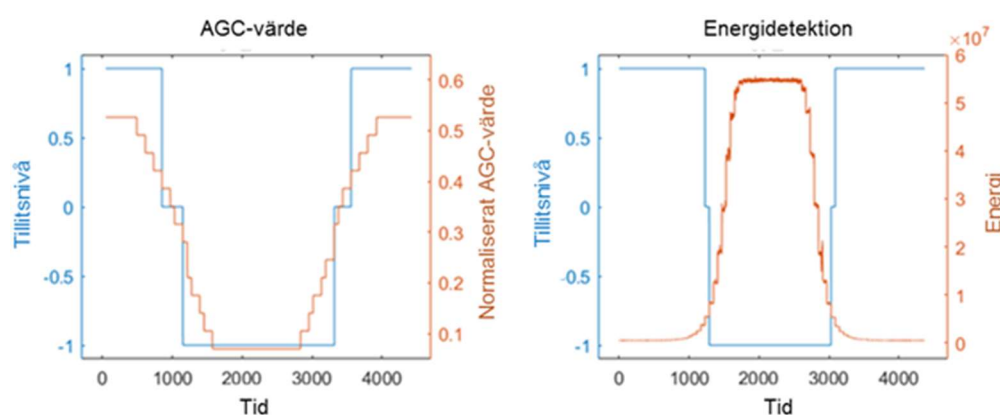
Om varken AGC-nivåerna är tillgängliga ut från mottagaren, eller energinivåerna kan estimeras, så behöver andra metoder användas för att detektera störning. En störsignal kommer att öka den upplevda brusnivån i mottagaren och därmed reducera C/N_0 -värdena vilket kan användas för att detektera störning (med *LowCnoCheck*).

Dessa detektionsmetoder kan dock inte ge information om huruvida mottagaren är utsatt för störning eller vilseledning. Fler metoder behöver kombineras för att kunna klassificera olika typer av attacker.

Så länge mottagaren kan estimeras C/N_0 -värden så kan den varna för att mottagaren kan vara utsatt för störning. I figur 3.5 visas resultaten för denna metod vid brusstörning (vänster) och vilseledning (höger). Denna detektionsmetod har två allvarliga svagheter. Den första är att mottagaren när den blir utstörd inte längre kan estimeras C/N_0 -värden. Vid brusstörning så visar metoden i detta fall nivån -2, vilket sker när data är otillgängliga, dvs. när C/N_0 inte längre kan estimeras. Då får kontrollen vikten 0 och räknas därmed inte med i den slutgiltiga sammanvägda bedömningen. Den andra svagheten är att C/N_0 -värden inte kan ses som ett tillräckligt bevis på att störning förekommer då låga värden även kan orsakas av att mottagaren befinner sig i miljöer (t.ex. inomhus) där signalerna är svaga.



Figur 3.3: Detektion med hjälp av AGC-värden (*AgcCheck*) och energidetektion (*EnergyDetectionCheck*) vid bredbandig brusstörning (test 1).

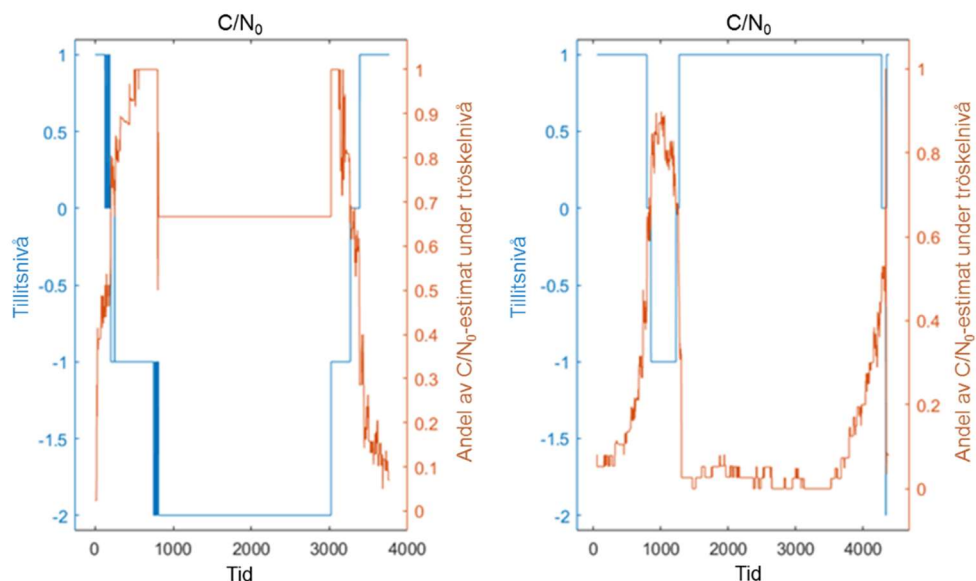


Figur 3.4: Detektion med hjälp av AGC-värden (*AgcCheck*) och energidetektion (*EnergyDetectionCheck*) vid repeterstörning (test 3).

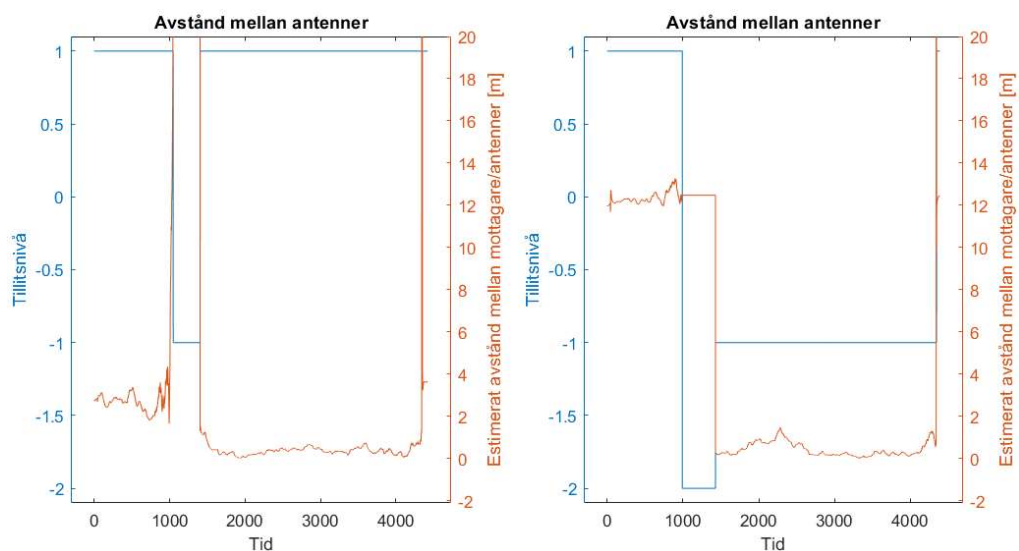
Denna metod kan inte heller användas för att detektera en typisk vilseledningsattack som genererar signaler med höga C/N_0 -värden. Detta syns i figur 3.5 där andelen C/N_0 -värden under tröskelnivån är lågt under själva vilseledningsattacken, efter det att mottagaren har släppt följningen av de autentiska GNSS-signalerna och istället har låst på och följer vilseledningssignalerna.

För test 2 och 3 presterar metoderna som beskrivs i tabell 3.1 snarlikt, med undantag för *RangePositionCheck* som baseras på det beräknade avståndet mellan mottagarnas rapporterade positioner jämfört med deras kända avstånd. Resultatet från en jämförelse av en metod (*RangePositionCheck*) som använder flera (geografiskt separerade) antenner och mottagare visas i figur 3.6. I test 2 är det sanna avståndet mellan mottagarna litet (< 2 m) vilket innebär att avståndet för de vilseledda positionerna fortfarande är inom felmarginalen för mottagarnas positionsestimat. Detta är inte längre fallet när avståndet mellan mottagarna ökas till 10 m, vilket kan ses i figur 3.6. I test 3 ger metoden under en period nivå -2, det vill säga otillgänglig kontroll vilket i detta fall innebär att (minst) en av mottagarna inte rapporterar någon position.

När de två mottagarna blir utsatta för en vilseledningsattack kommer de att släppa de sanna satellitsignalerna vid olika tidpunkter, och börja följa vilseledningssignalerna istället, vilket även innebär att mottagarnas positionsestimat blir vilseledda vid delvis olika tidpunkter. Det är vid sådana tillfällen som skillnaden mellan de estimerade positionerna för de två mottagarna bli stort.



Figur 3.5: Kontroller av C/N_0 (LowCnoCheck) för test 1 (vänster) och test 3 (höger).

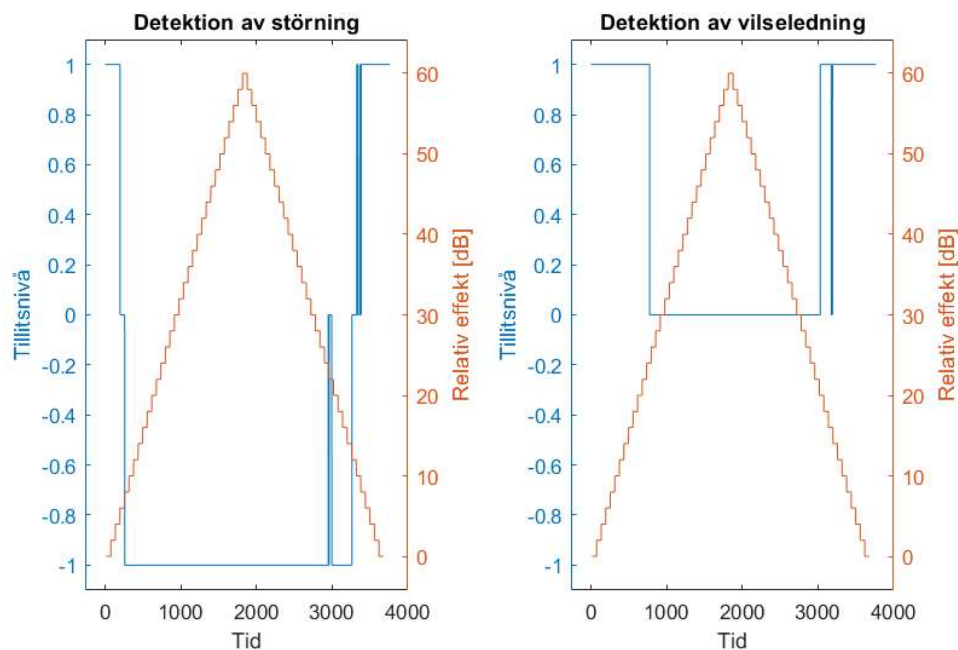


Figur 3.6: Jämförelse av avstånd mellan mottagare/antennerna (RangePositionCheck) vid detektion av vilseledning, för test 2 (vänster) och test 3 (höger).

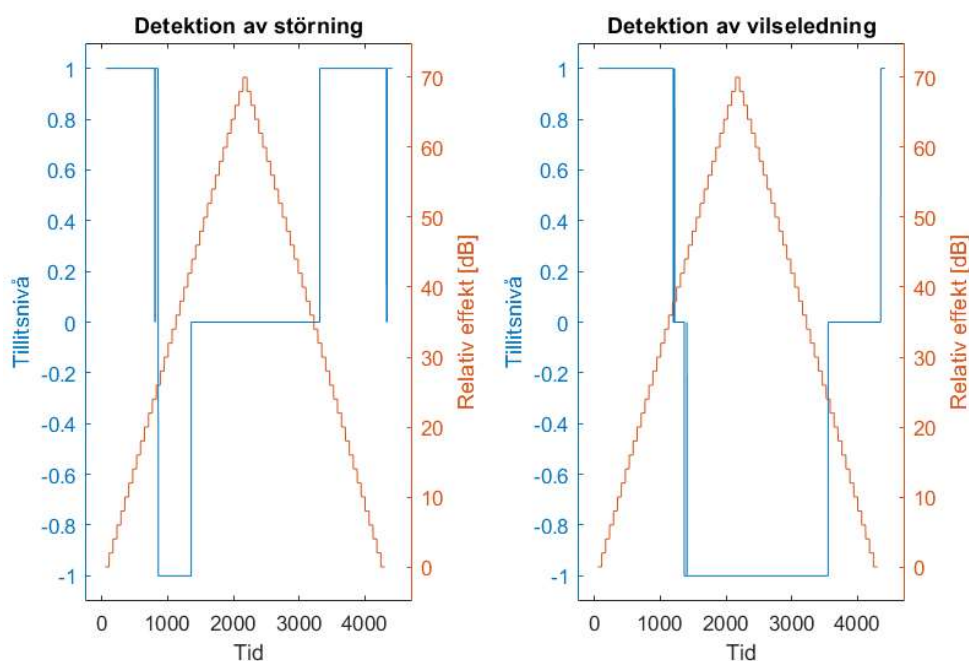
I figur 3.7 till 3.9 visas den sammanvägda bedömningen från en kombination av detektionsmetoder för störning respektive vilseledning.⁹ De relativa effektnivåerna på stör- respektive vilseledningssignalerna visas även. Samtliga metoder markerar att mottagarna är utsatt för störning eller vilseledning. I viss mån kan de även ge information huruvida mottagaren är utsatt för brusstörning eller vilseledning (repeaterstörning).

I test 1 markeras tidigt att mottagaren är utsatt för störning medan bedömningen om vilseledning är osäker (figur 3.7). När brusnivån ökar får mottagarna sämre precision på positionen, vilket gör att positionsestimaten från mottagaren kan börja röra sig iväg från den riktiga positionen. Detta medför att vissa av metoderna som detekterar vilseledning löser ut. Positionsfelet sker däremot inte tillräckligt fort för att andra metoder, som till exempel *VelocityCheck*, ska lösa ut. Detta medför att tillitsnivån sätts till 0, se figur 3.7, vilket indikerar att detektionssystemet har en hög osäkerhet när det gäller detektion av vilseledning.

⁹ För störning används *LowCnoCheck* och *AgcCheck* och för vilseledning används *RangePositionCheck*, *StaticPositionCheck*, *AltitudeCheck*, *PositionJumpCheck*, *VelocityCheck* och *AgcCheck*.



Figur 3.7: Detektionsresultat för Test 1 – Brusstörning.

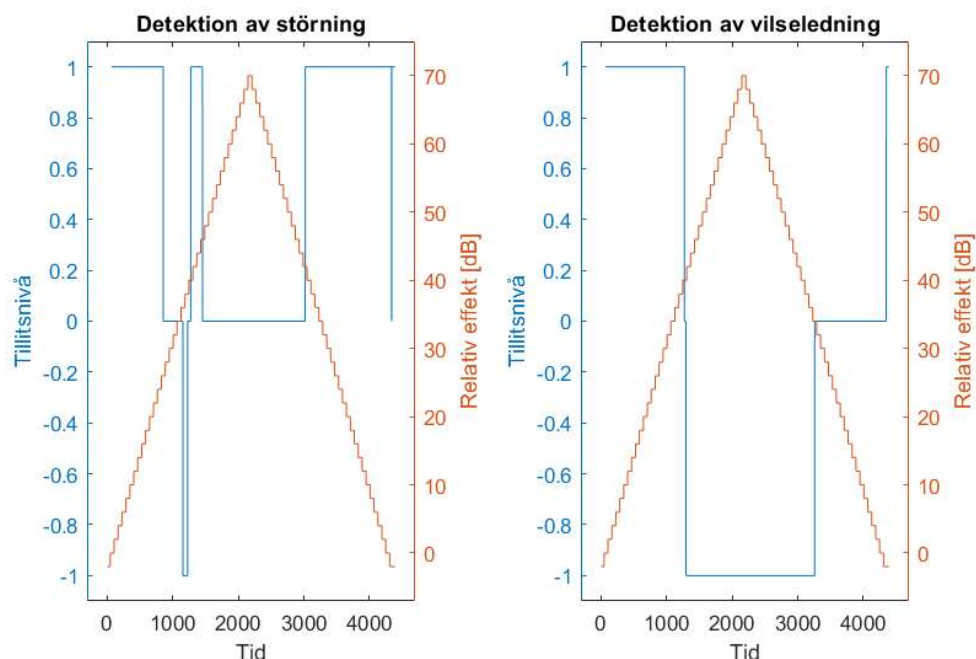


Figur 3.8: Detektionsresultat för Test 2 – Repeterstörning med knappt 2 m mellan mottagarantennerna.

I test 2 och 3, vilka visas i figur 3.8 och 3.9, indikerar det sammanvägda detektionsresultatet tydligt att en vilseledningsattack sker. Att detektionssystemet för störning visar nivå 0 (osäkert läge) under en stor del av tiden beror på att C/N_0 -nivåerna vid vilseledning är höga vilket medför att *LowCnoCheck* inte indikerar störning.

3.3 Slutsatser

Det är möjligt att detektera brusstörning innan mottagarens positionsestimat har hunnit försämrats märkbart, genom att använda information om mottagarens AGC-nivåer (då dessa finns tillgängliga) eller genom att estimerar den mottagna energin i de specifika frekvensbanden. Energidetektion förutsätter dock i nuläget att en separat mottagare används för att digitalisera signalen varefter signalens energi kan estimeras och jämföras



Figur 3.9: Detektionsresultat för Test 3 – Repeterstörning med 10 m mellan mottagarantennerna.

mot en tröskelnivå. Estimat av C/N_0 -nivåerna i mottagaren för de olika GNSS-signalerna kan även användas men metoden har stora osäkerheter då dessa värden påverkas av miljön (t.ex. inomhus) och då C/N_0 inte längre kan estimeras då mottagaren blir utstörd. Analyser av C/N_0 -nivåerna bör endast användas som metod för att detektera störning om varken energidetektion eller AGC-värden finns tillgängliga. Denna metod kan dock vara användbar för att stödja klassificeringen mellan störning och vilseledning, eftersom höga C/N_0 -nivåer i kombination med hög mottagen energi (eller låga AGC-värden) är en tydlig indikator för att mottagaren är utsatt för vilseledning.

I de tester där en vilseledningsattack har genomförts visar resultaten att det går att upptäcka när repeterstörningen påverkar mottagaren. Sannolikheten att detektera vilseledningsattacker förbättras om mätningar från geografiskt separerade mottagare kan jämföras (där avstånden mellan antennerna är kända eller kan mätas upp). Genom att kombinera energidetektion med jämförelser av utdata från mottagaren bör det även vara möjligt att med god tillförlitlighet avgöra när mottagaren inte längre är påverkad av en vilseledningsattack. Även detektionsmetoder som nyttjar flera antenner har vid den här typen av repeterstörning en god förmåga att avgöra när en vilseledningsattack upphör (inte längre påverkar mottagarna). Andra scenarion och vilseledningssignaler kan försvåra framförallt detektionen av när mottagaren inte längre är utsatt för vilseledning. De utvärderingar som har presenterats i denna rapport har varit för en stationär mottagare. Ett mobilt scenario presenteras och utvärderas i [5]. Fler utvärderingar behöver genomföras i syfte att ge möjlighet att förbättra valen av tröskelnivåer samt förbättrade val av hur de olika metoderna bör viktas i det sammanlagda beslutet som detektionssystemet tar rörande om den bedömer att mottagaren är utsatt för vilseledning eller ej.

I situationer då gruppantennerna används kan de, förutom att undertrycka oönskade signaler, även varna då de detekterar stör- eller vilseledningssignaler som är starkare än bakgrundsbrusnivåerna. Moderna gruppantennerna kan även ge ett estimat av hur stark störnsignalen är samt dess infallriktning.

4 Experimentsystem för robust GNSS-modul

En central delaktivitet i projektet har varit att utveckla ett experimentsystem för en robust GNSS-modul. Målet var att möjliggöra utvärderingar och demonstrationer av en integrerad robust GNSS-modul.

Följande deltekniker har integrerats i experimentsystemet:

- en gruppantenn (störskyddssystem),
- algoritmer för detektion av stör- och vilseledningsattacker mot GNSS,
- militär GPS-mottagare,
- två civila kommersiella GNSS-mottagare och
- ett tröghetsnavigeringssystem (TN-system).

I figur 4.1 beskrivs den hårdvara som integrerats direkt i experimentsystemet.

Experimentsystemet är inbyggt i ett ca 30 cm långt aluminiumchassi. Datorkort och kort för seriell kommunikation är monterat i ena änden av chassit och de kyls (passivt) via aluminiumchassit. En liten IMU (Inertial Measurement Unit) är monterad på insidan av chassits översida och den är ansluten via en serieport till styrdatorn. Denna kan även fungera som ett TN-system och i realtid beräkna position, orientering och hastighet då den har algoritmerna för tröghetsnavigering integrerade. Övriga sensorer är monterade på ett 3D-utskrivet skal som skjuts in i chassit från baksidan. Datorkortet i systemet använder Linux operativsystem Ubuntu. Experimentsystemet har en intern hårddisk för datalagring.

Det finns två antenningångar för GNSS-antennerna. Då en extern gruppantenn används så kopplas den in till den nedre antenningången. Ytterligare sensorer kan kopplas in via USB- eller serieportar för specifika mätningar, t.ex. tröghetssensorer som använder en IMU av högre kvalitet och extern utrustning för detektion av störning och vilseledning av GNSS-frekvenserna.

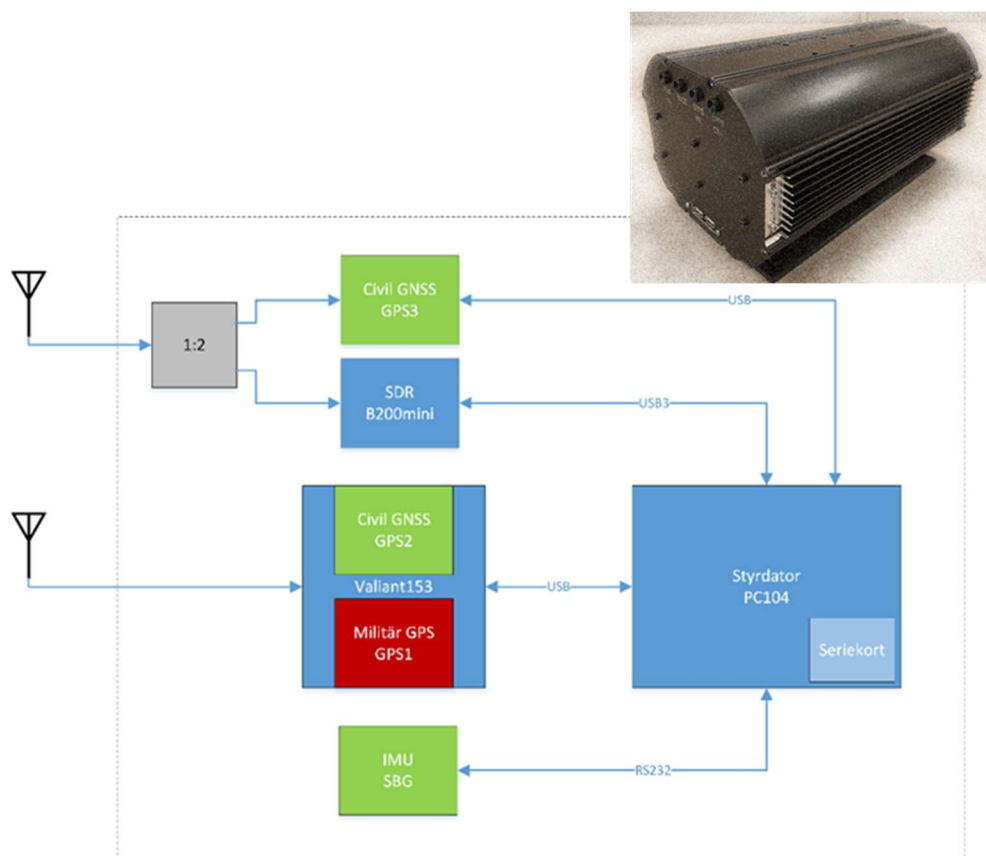
4.1 Styrdator och seriekort

Den integrerade styrdatorn (GEMINI från Diamond Systems) har en formfaktor enligt PC/104 och den har följande funktioner och konfiguration: intern hårddisk för datalagring och operativsystem, USB-portar (USB2.0/USB 3.0), HDMI för anslutning av bildskärm och olika serieportar (RS422 och RS232). Styrdatorn strömförsörjs med 12-28 VDC via kontaktdonet på baksidan märkt "PWR IN" och har en intern kontakt för att ta ut +5 VDC/500mA och +3.3 VDC/500mA. Dessa spänningar är utdragna på baksidan i kontakten märkt "PWR OUT". Ovanpå styrdatorn är även ett seriellt gränssnittskort (Diamond Emelard-MM-8Plus) monterat så att upp till åtta serieportar kan användas.

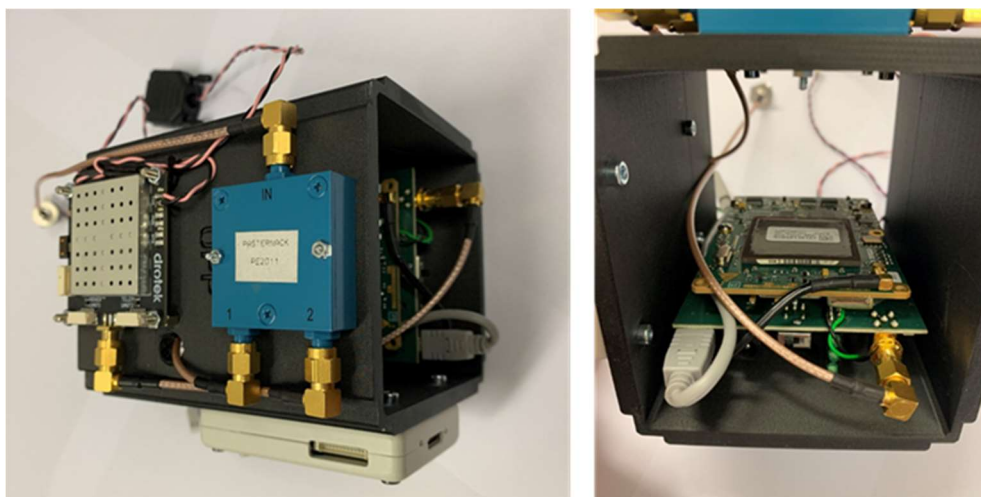
4.2 Sensorer

Tre GNSS-mottagare och en IMU har monterats internt i experimentsystemet (figur 4.2):

- Valiant 153M som består av ett moderkort för militär GPS, där en GPS P(Y)-kodsmottagare är monterad (benämnd "GPS1"), samt en civil GNSS-mottagare (u-blox ZED-F9P, benämnd "GPS2").
- GNSS-mottagare u-blox ZED-F9P (benämnd "GPS3").
- Ettus B200 mini mjukvaruradio.
- Signalsplitter (kopplad till "GPS3" och Ettus B200 mini).
- SBG Systems Ellipse 2 Micro INS.



Figur 4.1: Skiss av experimentsystemets uppbyggnad, samt det aluminiumchassi som de interna delarna av experimentsystemet har integrerats i. (Foto: FOI).



Figur 4.2: De inre delarna av experimentsystemet. Till vänster ses bland annat antensplitter (blå), Ettus B200 mini (vit) och GNSS-mottagarkort u-blox F9P (metall). Till höger ses moderkortet för Valiant 153M och det militära SAASM (Selective Availability Anti-Spoofing Module) GPS-mottagarkortet från Rockwell Collins. (Foto: FOI).

Fyra serieportar av höghastighetstyp (konfigurerade för RS422) finns utdragna till baksidan (märkta "SER2 – SER5") där exempelvis IMU:er av högre kvalitet kan kopplas in. Experimentsystemet har i nuläget stöd för tre IMU:er (Honeywell KVH 1775 och 1725, samt Sensoror STIM 320).

Till USB-porten kan en extern stördetektor för GNSS anslutas (Orolia BroadSense Nano). Den har en extern inbyggd antenn och behöver placeras utanpå fordonet, tillsammans med

GNSS-antennerna. På baksidan av systemet finns även två serieportar ("SER 0" och "SER 1") konfigurerade för RS232, som kan användas för att koppla in ytterligare sensorer med lägre dataakt.

En CSAC (Chip-Scale Atomic Clock) av typen SA.45s från Microchip har även anskaffats men den har ännu inte integrerats i experimentsystemet.

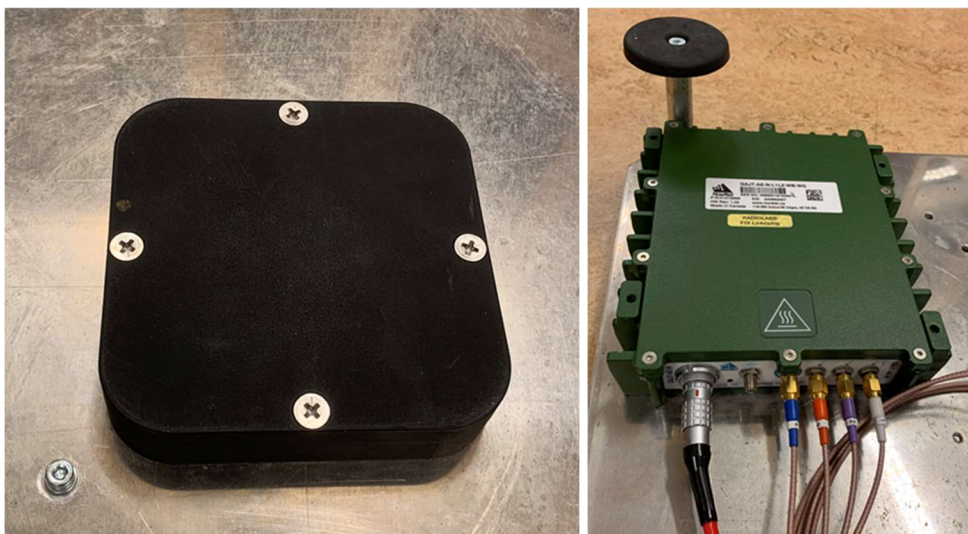
4.3 Gruppantenn

Ett störskyddssystem av typen GAJT AE-N från Novatel med tillhörande gruppantenn kan användas tillsammans med experimentsystemet för att påvisa nyttan med en gruppantenn i en telestörd miljö (figur 4.3). Systemet bygger på en elektronikenhet med fyra RF-kanaler som ansluts till en gruppantenn med fyra antennelement. Genom spatiotemporal filtrering kan upp till tre bredbandiga brusstörssignaler undertryckas och därmed kan mottagaren fortsätta fungera även när störning förekommer. Ett gruppantennbaserat störskyddssystem ger även ett skydd mot vilseledningsattacker. Den gruppantenn som används har storlek $10 \times 10 \times 2 \text{ cm}^3$ och kan hantera frekvenserna GPS L1 och GPS L2. Elektronikenheten gör undertryckning på L1 och L2 samtidigt och har enligt datablad en undertryckningsförmåga på 40 dB. Störskyddssystemet anges vidare vara anpassad för att även fungera på den nya krypterade GPS M-kodssignalen. Störskyddssystemet lämnar en RF-signal som ansluts till antenningången till den militära GPS-mottagaren och den civila GNSS-mottagaren.

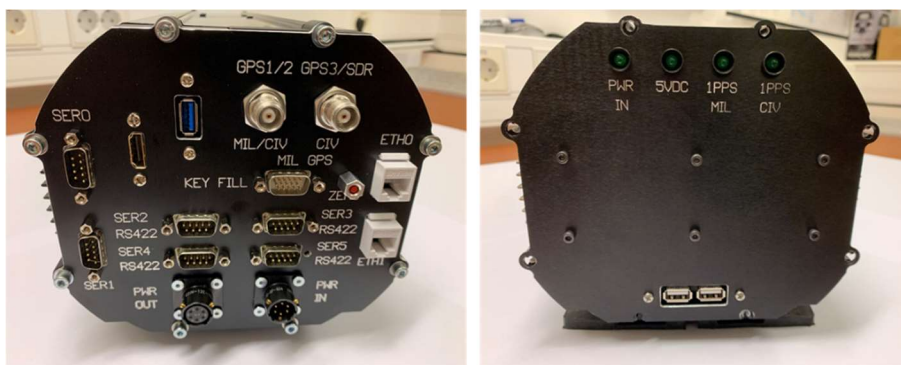
4.4 Anslutningar

På baksidan av systemet är alla anslutningar placerade, förutom två USB 2.0 kontakter som återfinns på systemets framsida. På framsidan är även följande indikeringar placerade (figur 4.4):

- "Power In" – indikerar att systemet är anslutet till en strömförsörjning och har matningsspänning.
- "5 VDC" – Indikerar att datorkortet är uppstartat och att dess inbyggda kraftaggregat fungerar.
- "1PPS CIV" – indikerar att den civila GNSS-mottagaren (GPS3) har en positionslösning. Lysdioden blinkar med frekvensen 1 Hz.
- "1PPS MIL" – indikerar att den militära GPS-mottagaren (GPS1) har en positionslösning. Lysdioden blinkar med frekvensen 1 Hz.



Figur 4.3: Gruppantenn, 4-elements NOVATEL GAJT antenn (vänster) och tillhörande antennelektroniksystem (höger). (Foto: FOI).



Figur 4.4: Experimentsystemets bak- och framsida. (Foto: FOI).

Följande kontaktdon är placerade på baksidan av systemet:

- HDMI – för anslutning till bildskärm, kontaktdonet är omärkt.
- USB 3.0 – kontaktdonet är omärkt.
- ”ETH0” – Nätverksuttag (RJ45).
- ”ETH1” – Nätverksuttag (RJ45).
- ”SER 0” – Serieport 0, konfigurerad för RS232.
- ”SER 1” – Serieport 1, konfigurerad för RS232.
- ”SER 2” till ”SER 5” – Serieportar 2-5, konfigurerade för RS422.
- ”PWR IN” – ingång för strömförsörjning 12-28 VDC.
- ”PWR OUT” – utgång för strömförsörjning av externa sensorer (5 VDC och 3.3 VDC).
- ”GPS1/2 MIL/CIV” – antenningång för GPS1 och GPS2.
- ”GPS3/SDR CIV” – antenningång för GPS3 och SDR Ettus B200 mini.
- ”KEY FILL MIL GPS” – kontaktdon för laddning av kryptonycklar till den militära GPS-mottagaren.

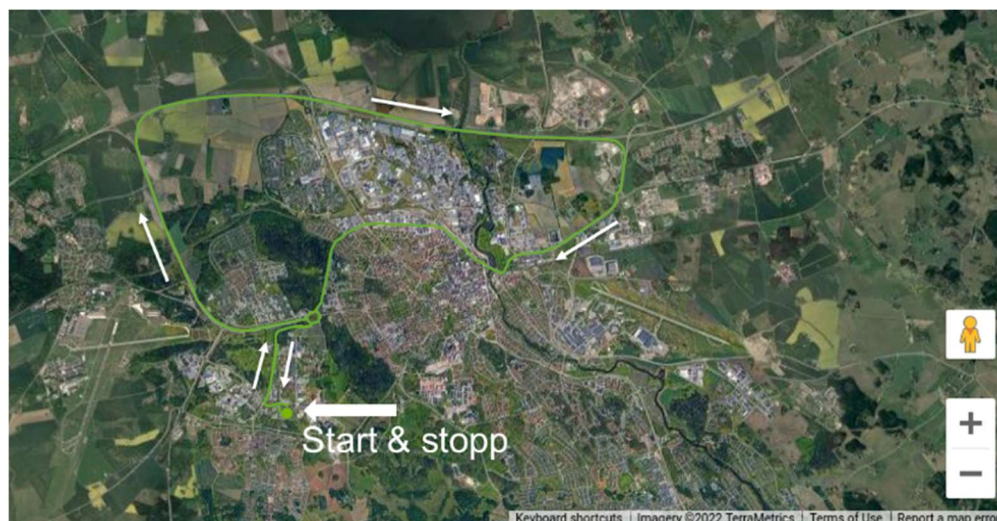
Förutom ovanstående kontaktdon finns även en skyddad strömbrytare för att nollställa den militära mottagarens kryptonycklar.

4.5 Validering

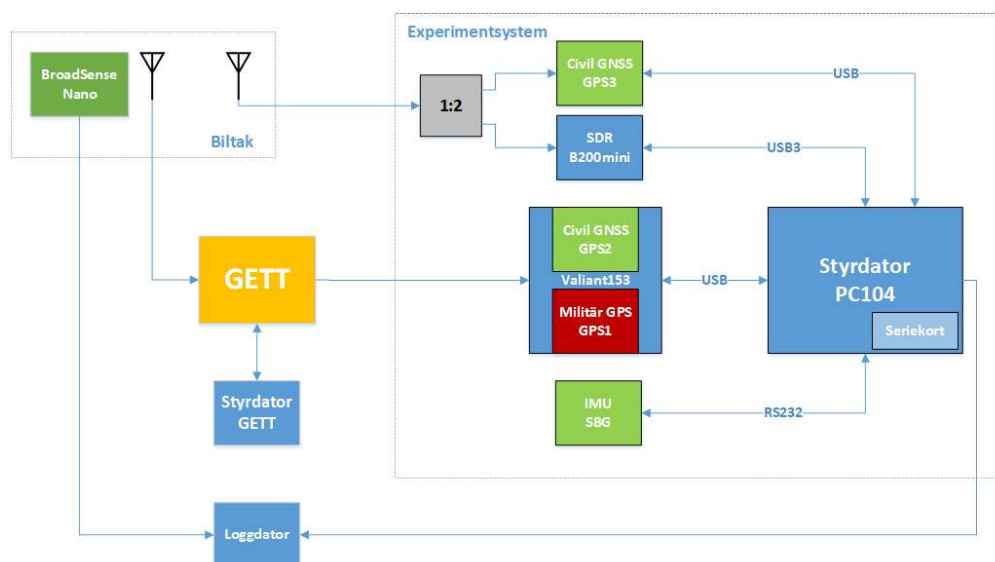
Experimentsystemets funktionalitet har validerats genom prov och försök i labbmiljö och vid ett initialt fältförsök. Syftet var att validera att sensorer och GNSS-mottagare kan leverera data och att resultaten är rimliga. En mer utförlig utvärdering av det färdiga experimentsystemets detektionsalgoritmer kommer att genomföras under 2023.

Under verifieringsmätningarna med experimentsystemet användes systemet GETT¹⁰ för att generera en störsignal som adderades till två av mottagarnas antenningångar under försöket (kabelbunden ”störinjektion”). Detta möjliggjorde att en variabel störsignal kunde skapas, vars effekt anpassades efter mottagarens geografiska position, och på sätt kunde implementationerna av experimentsystemets stördetektionsalgoritmer (ARM-PIT) verifieras. Vid valideringsmätningen placerades experimentsystemet på ett fordon som körde runt enligt figur 4.5. GNSS-antennerna och det externa detektionssystemet (BroadSense Nano) placerades på fordonets tak medan GETT och experimentsystemet placerades inne i fordonet (figur 4.6). De zoner där bredbandig brusstörning injicerades i GNSS-mottagarna från GETT, samt störnivåerna, visas i figur 4.7. Störnivåerna varierade mellan 30 och 87 dB.

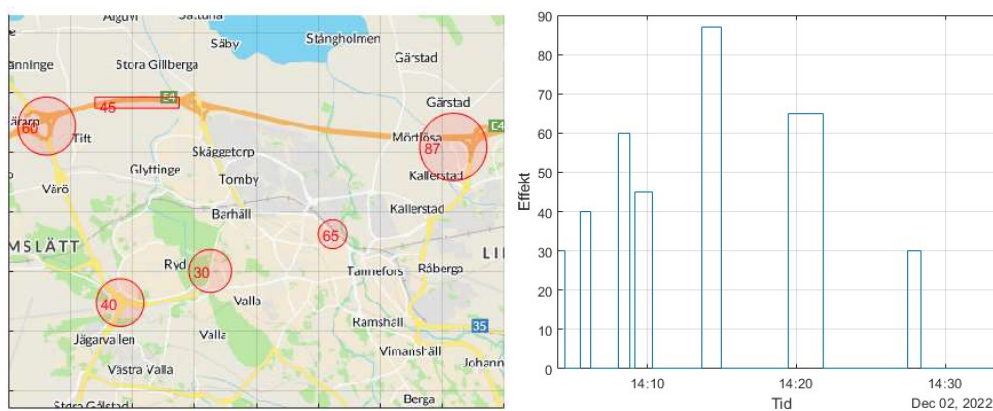
¹⁰ GETT är ett system utvecklat på beställning av Försvarmakten som möjliggör övning med, och utvärderingar av prestanda vid, GNSS-störning utan att verkliga störsignaler behöver sändas i luften.



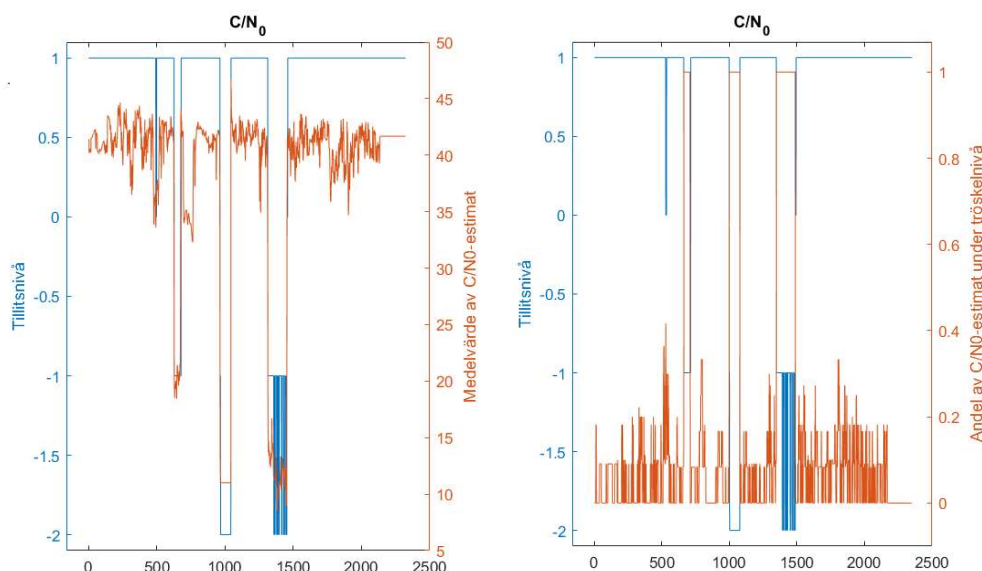
Figur 4.5: Körd sträcka vid valideringsmätning i Linköpingsområdet. Start- och stopposition angivna med gröna punkter och körväg markerad i grönt. Vita pilar indikerar färdriktning.



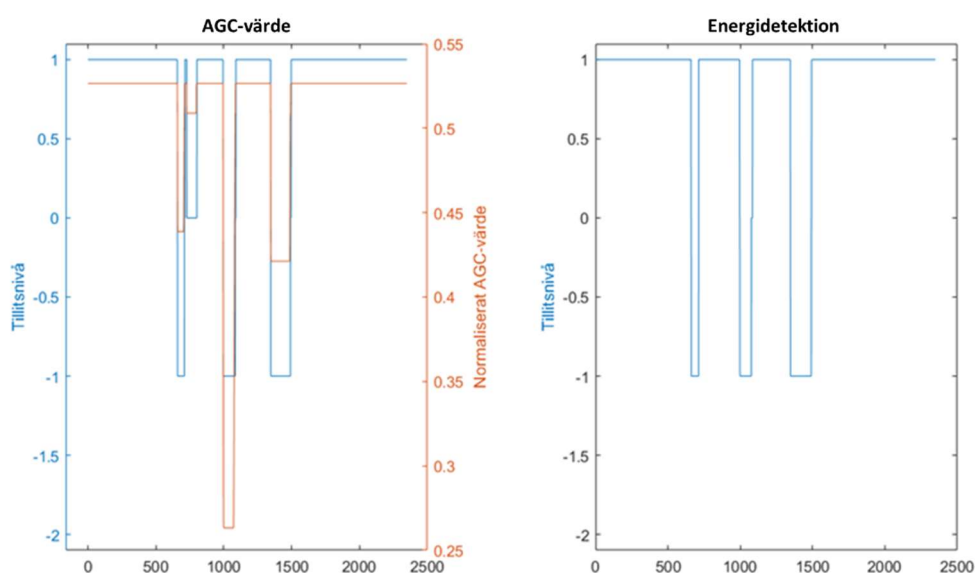
Figur 4.6: Skiss av experimentsystemet och GETT vid valideringsmätning.



Figur 4.7: Karta med störzoner markerade i rött (vänster) samt störnivåer som genereras med GETT, och injiceras kabelbundet till mottagaren, som funktion av tid under körningen (höger).



Figur 4.8: Detektion av störning med detektionsmetod baserad på uppmätta C/N_0 -värden. Estimerad tillitsnivå visas tillsammans med medelvärdet av C/N_0 -värdena (vänster) respektive andel av C/N_0 -värden som är under en ansatt tröskelnivå (höger).



Figur 4.9: Detektion av störning baserat på AGC-värden från mottagaren (vänster) och energidetektion (höger).

I figur 4.8 ges exempel på förmågan att detektera brusstörning baserat på uppmätta C/N_0 -värden. Störning detekteras vid tre tillfällen då den överstiger 60 dB. Vid det tredje detektionstillfället estimerar inte GNSS-mottagaren alla C/N_0 -värden då vissa signaler inte kan följas på grund av störningen. Det är orsaken till att tillitsnivån (blå linje) varierar mellan -1 och -2 under denna period. Även energidetektion och detektion baserat på AGC-värden ger detektion vid motsvarande störnivåer (figur 4.9). AGC-metoden indikerar dock att estimatet är osäkert vid ett tillfälle, då störnivån är något svagare (55 dB).

5 Hastighetsstöttade tröghetsnavigeringssystem

Tröghetsnavigeringssystem, TN-system, används idag på olika plattformar för att beräkna position, hastighet och orientering. De används typiskt som ett delsystem i ett multisensorbaserat PNT-system.

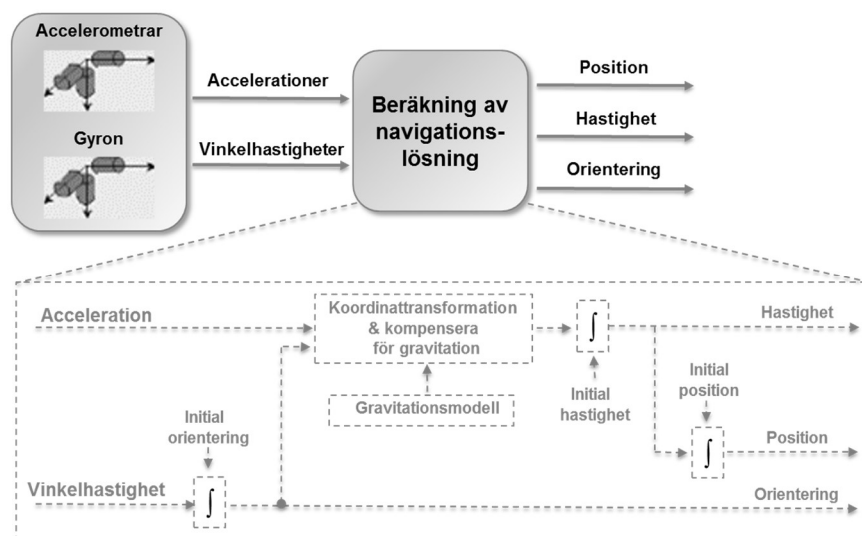
5.1 Tröghetsnavigeringssystem

Ett TN-system använder mätningarna från en IMU som mäter vinkelhastigheter och accelerationer med treaxliga gyron respektive accelerometrar. Dessa mätningar kan därefter användas för att estimerar en plattforms position, hastighet och orientering. Principen för ett TN-system illustreras i figur 5.1, där estimat av förändringar i orientering, hastighet och position erhålls genom att integrera vinkelhastigheter och accelerationer.

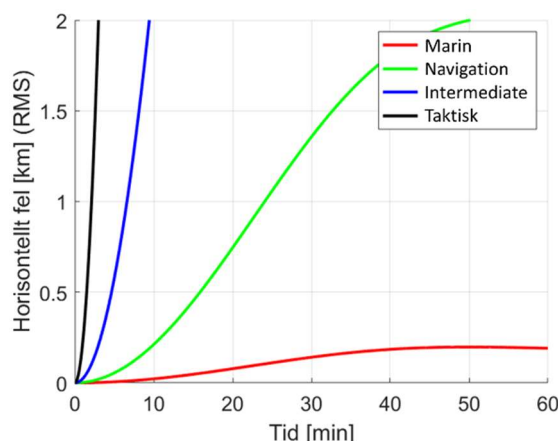
Ett TN-system är beroende av att den förses med ett estimat av plattformens ursprungliga orientering, hastighet och position (s.k. initialisering). Ett litet fel i mätningarna kommer att ge upphov till snabbt ökande fel. Felen växer kontinuerligt över tid där feltillväxten avgörs av kvaliteten på tröghetssensorerna. Under en begränsad period (ca 10 min) kan positionsfelet vid ren tröghetsnavigering approximativt sägas öka med tiden i kvadrat. För längre tidsintervall växer höjdfelet exponentiellt och obegränsat medan det horisontella felet växer långsammare och en analys av felet förutsätter mer detaljerade felmodeller.

Feltillväxten i TN-system för olika prestandanivåer på IMU:er illustreras i figur 5.2. Dessa simuleringsresultat är baserade på förenklade felmodeller och de är avsedda att ge läsaren en förståelse för hur snabbt felet växer för olika klasser av sensorer. Även noggrannheten på initialiseringen av ett TN-system är avgörande för dess prestanda. I tabell 5.1 anges att en IMU av taktisk klass kan ha en feltillväxt på ca 15 m efter 15 s i horisontell position medan även IMU:er av högre kvalitet såsom navigationsklass får ett fel som efter 10 minuter kan överstiga ca 200 m (figur 5.2).

För att TN-systemen ska ge korrekta positionslösningar under längre tidsperioder är de beroende av stöttning från andra sensorer. GNSS-mottagare används i stor omfattning men de kan störas ut och för att få ett robust system behöver även andra sensorer användas. Genom att fusionera med hastighetsmätningar från andra sensorer kan felets tillväxt i ett TN-system avsevärt minskas. På så sätt kan ett hastighetsstöttat TN-system klara sig under längre perioder vid operationer i telestörda miljöer där GNSS-mottagarna är utstörda.



Figur 5.1: Illustration av principerna för ett tröghetsnavigeringssystem.



Figur 5.2: Simulering av feltillväxt i TN-system baserat på förenklade felmodeller och antagande om perfekt initialisering. Feltillväxten för den horisontella positionen illustreras för olika klasser av IMU:er under en timme (i kilometer) [1].

Tabell 5.1: Exempel på olika klasser av IMU:er (baserad på [1]). Positionsfel enligt figur 5.2.

Klass	Positionsfel	Gyrobias	Acc.bias	Exempelsystem
Marin	<0,2 km efter 1 h	0,001 °/h	0,01 mg	Militära fartyg, ubåtar, vissa ICBM
Navigation	>200 m efter 10 min	0,01 °/h	0,03–0,1 mg	Militära och kommersiella flygplan
Intermediate (Mellannivå)	>20 m efter 60 s	0,1 °/h	0,1–1 mg	Mindre flygplan, helikoptrar
Taktisk	~15 m efter 15 s	1 °/h	1–10 mg	Styrda vapen, obemannade farkoster

En vanlig hastighetssensor som används i marina farkoster är en DVL (Doppler Velocity Log) eller en CVL (Correlation Velocity Log), medan odometrar används på markfarkoster. Huvudfokus för detta arbetspaket var att studera inverkan av hastighetsmätningar på ett TN-system. Fokus var mot hastighetssensorer för marina farkoster, men mycket av kunskapen går att generalisera även till markfarkoster. Sensorerna har undersökts och simulerats utifrån gemensamma felmodeller.

Till skillnad från GNSS-mottagares globala mätningar i ett jordfast koordinatsystem är de studerade hastighetsmätningarna lokala i ett farkostfast koordinatsystem. De är därför mindre informativa och de kan t.ex. inte direkt mäta kursriktningen. För mer utförlig information om olika hastighetssensorer se [4].

5.2 Simuleringsmiljö

En FOI-utvecklad mjukvara för multisensorfusion har använts i simuleringarna, benämnd *Navtoolbox*. När farkostens bana genereras är det viktigt att kunna simulera en realistisk fysik vid svängar och fånga den kursavvikelse som uppstår. Under en sväng kommer till exempel ett fartygs hastighet inte (i dess tyngdpunkt eller en annan referenspunkt) vara riktad längs med kroppen utan det kommer även finnas en lateral hastighetskomponent (i referenspunkten). Vissa marina fartyg är utrustade med loggar som kan mäta den laterala hastigheten, men det finns även loggar som inte gör det. På markfarkoster där konventionell odometri används mäts endast den transversala hastigheten (i farkostens riktning).

Ett öppet Matlabbaserat kodbibliotek (Marine Systems Simulator, MSS¹¹) används för fysiksimulering av de marina farkosterna. Den marina farkost som simuleras är ett 160 meter långt fraktfartyg av Marinerklass. Rörelsemodellen med tillhörande fel för

¹¹ se.mathworks.com/matlabcentral/fileexchange/86393-marine-systems-simulator-mss och github.com/cybergalactic/MSS (besökta 2022-12-04).

markfordon simuleras med hjälp av en egenutvecklad s.k. skid-steer¹² modell som är baserad på [23].

5.3 Simuleringar

Tre olika IMU:er har simulerats i *Navtoolbox*. Prestanda för dessa beskrivs i tabell 5.2 och exempel på produkter som har motsvarande prestanda beskrivs även.

Nedan illustreras effekterna från hastighetsmätningar, vattenströmmar och inverkan från förlorad bottenmätning med DVL. Resultaten bör ses som indikativa och det är främst de relativa förbättringarna som är av intresse i simuleringarna som visas nedan. De framtagna simuleringmodellerna och parametervärderna kan förfinas och uttömmande utvärderingar av teknikerna har inte genomförts. Simuleringarna avser visa på principiella fenomen samt påvisa vilka typer av utvärderingar som den utvecklade mjukvaran möjliggör.

5.3.1 Inverkan av hastighetsmätningar

För att visa på vikten av hastighetsstöttning exempelvis i situationer då GNSS-mottagaren blir utstörd simuleras en båt i havsmiljö omgiven av öar utan någon form av strömning i vattnet. Båten är i dessa två exempel utrustad med en IMU med prestanda som liknar KVH 1775 respektive KVH 1725. Simuleringen motsvarar ungefär 30 minuters färd med en hastighet på omkring 18 m/s. Utfallen från tio simuleringar presenteras nedan.

I figur 5.3 tar det en stund innan TN-systemet (utan stöttning och med en IMU med motsvarande prestanda som en KVH 1775) börjar få en större feltillväxt. Med hastighetsstöttning håller sig filtret till den sanna banan under en avsevärt längre tid. Positionsfelet i slutet av simuleringen var ca 2,5 km utan hastighetsstöttning medan positionsfelet vid slutpositionen reduceras till ca 35 meter för fallet med en 2D-logg (som mäter den laterala och transversala hastigheten) och omkring 150 meter med en 1D-logg.

I figur 5.4 används istället en enklare IMU med en prestanda som motsvarar en KVH 1725. Vid ren tröghetsnavigering (röd linje) ökar positionsfelet snabbt och slutpositionen, som har ett positionsfel på över 10 km, syns inte i figuren. Då filtret stötts med en hastighetsmätande logg blir de kvarvarande positionsfelen i storleksordningen 900 (2D-logg) och 1 000 m (1D-logg). Dock kan noteras att även om medelfelen och maxfelen är likartade för båda logg-alternativen så är fortfarande spridningen (1σ) större med 1D-logg, 640 m jämfört med 400 m som erhöles med en 2D-logg.

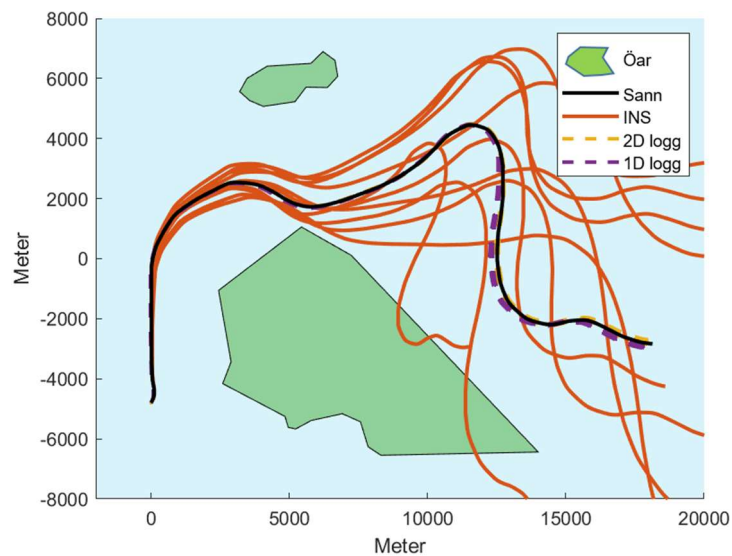
5.3.2 Inverkan av vattenströmmar

För att visa vikten av att få in information i flera axlar till TN-systemet simulerades en båt som färdas i en havsmiljö med starka vattenströmmar. En IMU med liknande prestanda som KVH 1775 användes i denna simulering. Liksom i de tidigare simuleringarna pågick de i ungefär 30 minuter och båten hade en hastighet på runt 18 m/s. Utfallet från de tio simuleringarna visas i figur 5.5.

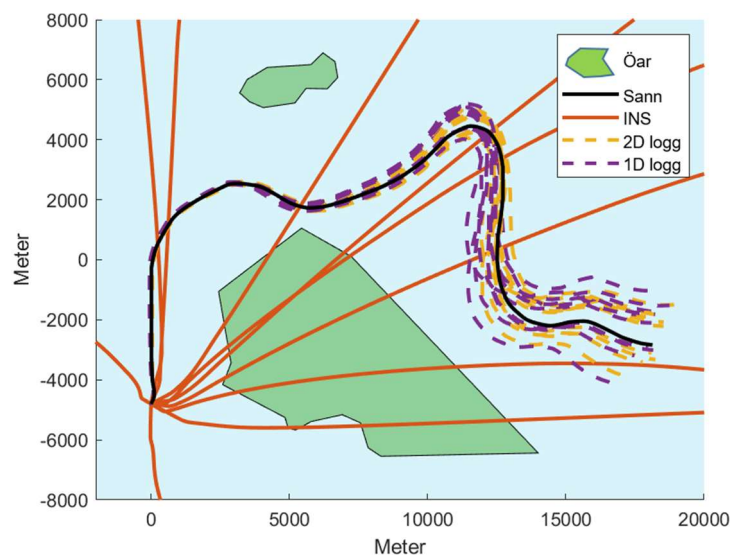
Tabell 5.2: Simulerade prestandaparametrar för tre IMU:er (ungefär motsvarande KVH 1775, KVH 1725 och HG9900). De befinner sig i det lägre spannet av respektive klass som anges (tabell 5.1).

IMU #	Gyrobias [°/h]	Acc. bias [mg]	Angle random walk [°/√h]	Velocity random walk [m/s/√h]	Klass	Motsvarighet
1	0,0035	0,025	0.002	0.0015	Navigation, enkel	HG9900
2	0,5	0,5	0.012	0.07	Mellanivå, enkel	KVH 1775
3	5	25	0.017	0.07	Taktisk, enkel	KVH 1725

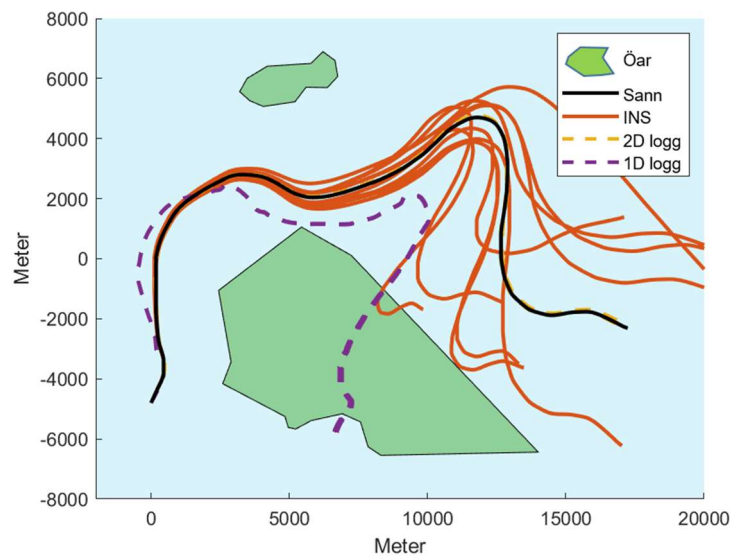
¹² Markfordonet styrs som ett bandfordon med hjälp av olika hjul- eller bandhastighet på höger och vänster sida. Då hjulvinkeln inte styrs innebär det att hjulen slirar vid sväng (därför benämningen skid-steer).



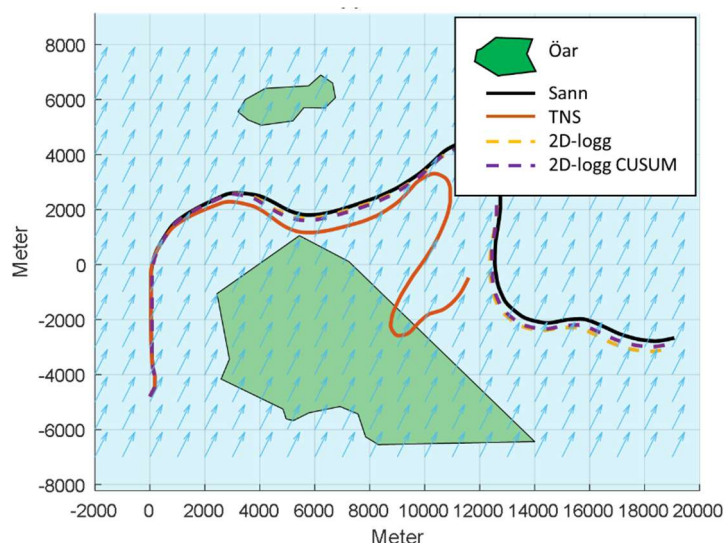
Figur 5.3: Simulering (tio realiseringar) av hastighetsstöttad tröghetsnavigering av fartyg med IMU #2 (liknande KVH 1775). Stilla hav.



Figur 5.4: Simulering (tio realiseringar) av hastighetsstöttad navigering av fartyg med IMU #3 (liknande KVH 1725). Stilla hav.



Figur 5.5: Simulering (tio realiseringar) av hastighetsstöttad tröghetsnavigering av fartyg med IMU #2 (motsvarande KVH 1775) i ett scenario med kraftiga strömmar.



Figur 5.6: Simulering av förlust av bottenkontakt i samband med slutet av den första manövern med IMU #2 (motsvarande KVH 1775). Två fall har simulerats, ett utan att anpassa filtret för förlusten av bottenkontakt medan i det andra fallet har en enkel modell baserad på en CUSUM detektor använts för att upptäcka mätfelet och då har en högre osäkerhet ansatts på mätningarna (2D-logg CUSUM). Blå pilar indikerar vindriktningen.

2D-loggen mäter både den laterala och transversala hastigheten vilket i detta scenario ger en hög positionsnoggrannhet. Positionsfelet för det sämsta utfallet där TN-systemet stötts med mätningar från en tvådimensionell logg blir ca 60 m. Både vid tröghetsnavigering och då TN-systemet stötts med mätningar från en endimensionell logg erhålls en snabb feltillväxt vilket resulterar i ett slutligt positionsfel på mer än 10 km. Notera att eftersom samma bana och ström simulerats i alla tio simuleringar så är spridningen i felet för den endimensionella loggen litet, dvs. felet domineras av den bias som ges av strömmens inverkan.

Det bör dock vara möjligt att få ner positionsfelet för båda hastighetsloggarna om en bättre initiering av bias är tillgänglig eller genom att utveckla modelleringen så att hänsyn tas till hur vattnet strömmar om det är känt, t.ex. genom tidigare GNSS-mätningar.

5.3.3 Inverkan av förlorad bottenkontakt

Ett viktigt scenario att undersöka är även när loggar tappar kontakt med sjöbotten då detta kan påverka felet i hastighetsestimatet signifikant. Både DVL och CVL är känsliga för när de tappar kontakt med sjöbotten. I dessa situationer mäter de istället fartygets hastighet i relation till vattnets hastighet istället för dess hastighet över botten som filtret är designat för. Vissa loggar kan dock detektera och meddela att mätmoden har ändrats vilket gör det möjligt att då ändra filtrets mätmodell för att förbättra dess prestanda. Generellt har DVL med högre mätnoggrannhet (upplösning) en sämre räckvidd då de använder högre frekvenser [24-25].

I figur 5.6 har ett bortfall av bottenkontakten simulerats för en period av 100 s efter den första manövern norr om den stora ön. För att illustrera hur systemet kan tänkas detektera och kompensera för denna typ av fel användes en standard CUSUM-detektor ("Cumulative Sum") [26] och filtret anpassades genom att osäkerheten för mätningarna ökades så länge ett fel detekterades.¹³

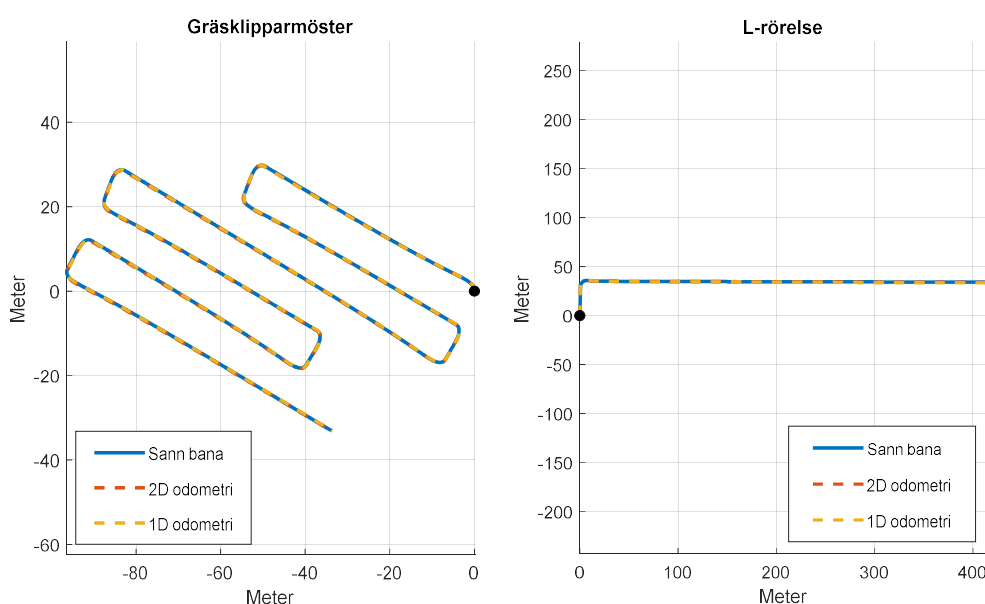
¹³ En CUSUM-detektor är en sekventiell detektor som är känslig för förändringar i modellantaganden. Den använder den ackumulerade summan av avvikelser mellan mätningar (i detta fall från hastighetslogg) och systemets prediktioner och larmar när en vald tröskel överskrids. En viss förbättring kan skönjas men denna enkla modell (som endast tar hänsyn till den ökade osäkerheten men inte till att felet har ett tidsvariabelt bias) är otillräcklig och bör förfinas.

En viss förbättring kan skönjas med denna enkla modell som endast tar hänsyn till den ökade osäkerheten, men som inte tar hänsyn till att felet har ett tidsvariabelt bias. Modellen är väl enkel och bör enbart ses som en initial illustration på hur störningar kan simuleras, detekteras och åtgärdas.

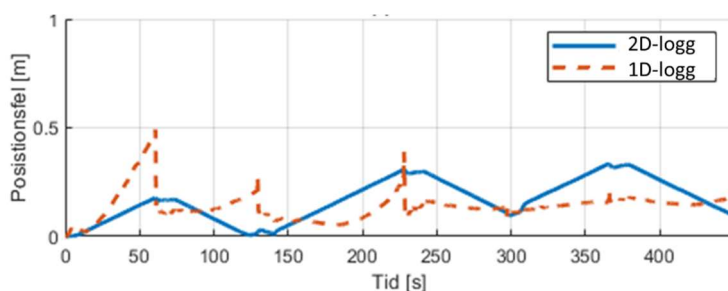
5.3.4 Rörelsemönster

Tidigare arbeten som publicerats av bland annat FFI i Norge har visat att feltillväxten för TN-system stöttade med hastighetsensorer påverkas av hur plattformen rör sig. Om den rör sig med en rak kurs blir positionsfelet högre än om plattformen rör sig i ett så kallat ”gräsklipparmönster” där plattformen med jämna mellanrum svänger åt höger respektive vänster. I det senare scenariot erhåller sensorfusionsfiltret mer information om centripetalaccelerationen (från hastighetsmätningarna från loggen) när plattformen svänger och det kan på så sätt hålla nere positionsfelet [25]. När kursen är rak går det inte att skilja på hastighetsfel från bias i acceleration och fel från vinkelfel i projektionen av gravitationskraften, men vid en sväng bryts detta samband så att filtret kan skatta bias bättre. Den här principen testas i simuleringsmiljön med både 2D-logg och 1D-logg för en AUV (Autonomous Underwater Vehicle) som förflyttar sig längs två olika banor, dels i ett gräsklipparmönster och dels i form av ett L. Den IMU som används i simuleringarna (dvs. IMU #1) har liknande nominell prestanda som en HG9900. Farkosten rör sig med en hastighet av en meter per sekund.

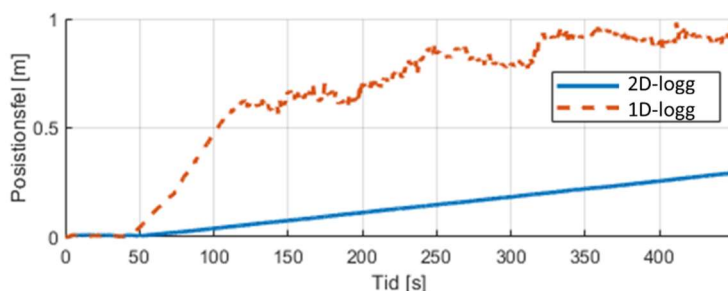
I figur 5.7 visas resultaten för gräsklipparmönstret respektive L-rörelsen. Plattformen som rör sig i gräsklipparmönstret håller sig nära den sanna banan men för L-rörelsen börjar positionslösningen för båda filtren att sakta avvika med tiden. I figur 5.8 och 5.9, där positionsfelet visas som funktion av tid, blir detta tydligare. I fallet då plattformen rör sig i ett gräsklipparmönster håller sig positionsfelet konsekvent under 0,5 m och i slutet av simuleringen trendar positionsfelet neråt för fallet med 2D-logg. När plattformen istället rör sig i en L-rörelse med endast en sväng i början ökar positionsfelet under hela simuleringen för båda typerna av hastighetsloggar. Genom att stötta TN-systemet med hastighetsmätningar så har feltillväxten övergått från att öka som en funktion av tiden i kubik och det ökar istället approximativt linjärt med förflyttad sträcka under tidsperioden för denna mätning (drygt sju minuter). I jämförelse så ger en IMU av mellanklass vid ostöttad tröghetsnavigering ett positionsfel över 20 m efter en minut (tabell 5.1).



Figur 5.7: Positionestimater (medel) med tvådimensionell respektive endimensionell hastighetsmätning, baserat på tio simuleringar. Plattformen startar i origo, markerat med en svart punkt. Simulering baserad på IMU #1 (liknande en HG9900).



Figur 5.8: Jämförelse av positionsfel (medel) för förflyttning i "gräsklipparmönster" med två- respektive endimensionell hastighetsmätning. Simulering baserad på IMU #1 (liknande en HG9900).



Figur 5.9: Jämförelse av positionsfel (medel) för förflyttning i "L-mönster" med två- respektive endimensionell hastighetsmätning. Simulering baserad på IMU #1 (liknande en HG9900).

FFI har i praktiska försök med ett hastighetsstöttat TN-system, baserat på en HG9900 IMU, begränsat feltillväxten till ca 0,08 % av färdad sträcka vid rörelse längs en linje och ned till 0,01 % då AUV rör sig i ett gräsklipparmönster [27]. I simuleringarna nedan erhöles för den L-formade trajektorien en positionstillväxt på drygt 0,05 % av sträckan. Liksom i FFI:s försök visar resultaten att manövrar förbättrar positioneringen då den centripetalinducerade accelerationen bidrar med information som kan separera vinkelfel från bias i acceleration och gör hastighetsfelen från IMU:n observerbara. När hastighetsfelen är observerbara kan de hållas nere med följden att positionsfelet växer linjärt med färdad sträcka (givet att gyrot är av så hög klass att det kan agera som en gyrokompass). Simuleringsresultaten är av samma magnitud som de som beskrivs i [27], men deras modell tog även hänsyn till att DVL har ett skalfaktorfel som skattades vilket gav ytterligare fördelar för gräsklipparmönstret jämfört med de genomförda simuleringarna. Sågtandsmönstret på felet för gräsklipparmönstret i figur 5.8 beror förmodligen på effekten av ett initialt orienteringsfel.

5.4 Slutsatser

Ett TN-system förväntas utgöra den grundläggande sensorn i PNT-system som även ska kunna operera i teilstörda miljöer. Feltillväxten för ett TN-system beror av kvaliteten på framförallt gyrosensorerna, men även med dyra och tunga sensorer behövs extra stöttning från andra sensorer för att öka tiden som farkosten kan operera utan tillgång till stöttning från GNSS-mottagaren. Att stötta TN-systemet med hastighetsmätningar är ett effektivt sätt att kraftigt reducera feltillväxten.

Hastighetsstöttning från DVL eller CVL har visat sig ge ett värdefullt bidrag till TN-system. Det gäller framförallt TN-system som använder IMU:er från taktisk klass upp till navigationsklass. Med den simuleringsmiljö som har utvecklats kan svårigheter som avdrift modelleras och utvärderas med avseende på till exempel DVL-loggar som enbart mäter hastigheten i en dimension, samt i situationer när de tappar kontakt med botten och istället mäter hastigheten jämfört med vattenvolymen.

5.5 Fortsatt arbete

Enkla statistiska test kan användas för att detektera och kompensera för momentana avvikelser. Fortsatta studier bör genomföras i syfte att ge svar på hur långa avvikelser som kan tolereras och hur väl de kan upptäckas. För en endimensionell logg är det intressant att implementera modeller för avdrift och skattad vattenhastighet för att kompensera för felet som uppstår då sensorn inte direkt kan mäta den resulterande avdriften. Ett naturligt nästa steg är att utvärdera och förfinas algoritmerna baserat på experimentell data från sjöförsök.

Filtret och simuleringsmodellerna kommer även utvärderas i fordonstillämpningar, baserat på mätdata som genererats tillsammans med FFI inom Nordefco Robust Navigation WG [28]. Vid dessa fältförsök samlades data in från flera IMU:er placerade på en Land Cruiser respektive en liten UGV. Båda fordonen ger hastighetsmätningar, baserat på odometri, men då framdrivningen för dessa fordon fungerar enligt olika principer resulterar det i olika felmodeller.

6 Kartbaserad positionering- och navigering

Metoder för positionering kan delas in i två kategorier: *relativ positionering* som mäter förflyttning relativt en startposition och *absolut positionering* som estimerar position i förhållande till ett fixt koordinatsystem.

6.1 Bakgrund

Relativa positioneringsmetoder är oberoende av förinstallerad infrastruktur och förutsätter inte tidigare kännedom om omgivningen. De är flexibla och kan användas baserat enbart på sensorer som är placerade på en plattform. Utmaningen med dessa tekniker är att felen i positions- och orienteringsestimaten i allmänhet växer som en funktion av tid eller plattformens förflyttning. Anledningen till denna feltillväxt är att positionen kontinuerligt estimeras i förhållande till tidigare estimat och felen därmed adderas.¹⁴

Positioneringsmetoder som estimerar den absoluta positionen undviker denna feltillväxt. Radiobaserade positioneringssystem som använder förinstallerad infrastruktur, t.ex. fasta sändarmaster (som eLoran eller R-mode Baltic [1]) eller satelliter vars banor är kända (som GNSS-satelliter), är exempel på absoluta positioneringssystem. Positionen mäts baserat på uppmätta avstånd till ett antal satelliter. Dessa avstånd kombineras med kännedom om satelliternas omloppsbanor för att beräkna en absolut position, som vanligen uttrycks som latitud, longitud och höjd. Tekniker som, sporadiskt eller kontinuerligt, kan ge ett estimat av en plattformens absoluta position och orientering är värdefulla vid operationer i miljöer där GNSS-mottagarna är utstörda eller ger otillförlitliga estimat. Det gäller telestörda miljöer men även inomhus och i underjordiska komplex och grottssystem.

Många positionerings- och navigeringsmetoder som använder bildalstrande sensorer estimerar plattformens relativa position och orientering. Vanligt förekommande metoder är så kallad visuell odometri eller SLAM (Simultaneous Localization and Mapping). Många av dessa metoder estimerar plattformens förflyttning genom att följa väldefinierade punkter genom en sekvens av bilder [29-30]. Genom att matcha mätningarna mot en karta eller en landmärkesdatabas kan dock även dessa sensorer estimerar plattformens position (och orientering) i ett känt koordinatsystem.

Vid kartstöttad navigering matchas data från en kamera, LiDAR eller annan sensor mot en georefererad karta över omgivningen. Resultatet av matchningen ger ett estimat av var sensorn befinner sig i relation till kartan. Begreppet *karta* bör i detta sammanhang tolkas brett. Det kan syfta på till exempel ett ortografiskt foto, en 3D-modell eller en uppsättning georefererade landmärken. Kamerabaserad stjärnnavigering utgör ett exempel på en metod som estimerar absolut position och orientering, i relation till vald stjärndatabas.

6.2 Begränsningar

Ett stort antal forskningsgrupper har demonstrerat att det med kamerabaserade system är möjligt att nå en hög noggrannhet under goda visuella förhållanden och det finns flera produkter som exempelvis positionerar en UAV.¹⁵ Begränsad information finns dock tillgänglig rörande hur väl denna teknik fungerar i mörker då exempelvis termiska IR-kameror används och vilka svagheter den då har. Tekniken har även begränsad nytta i vissa typer av (icke-informativa) miljöer.

¹⁴ Ett undantag är om alla rörelser sker inom samma geografiska område, då även metoder för relativ positionering kan känna igen sig över tid (s.k. loopslutning).

¹⁵ www.unmannedsystemstechnology.com/2022/11/jam-proof-navigation-solution-integrated-into-tactical-uavs/ (besökt 2022-12-07).



Figur 6.1: Satellitbilder från Google Earth tagna vid två olika årstider. (Foto: Google Earth, www.google.com/intl/sv/permissions/geoguidelines/).

6.2.1 Icke-informativa miljöer

Kartstöttade tekniker förutsätter att den observerade miljön kan matchas till kartmaterialet. Därför fungerar tekniken bättre i en miljö där unika särdrag kan urskiljas, än i ett område med repetitiv eller obefintlig struktur. Två av de svåraste fallen är över vatten och i mörker, där inga beständiga särdrag enkelt kan observeras. Även vid flygning på låg höjd över skog, eller vid förflyttning genom skogen, är kartmatchning i allmänhet svårt, eftersom enskilda träd oftast inte är karterade. På högre höjd kan däremot gränsen mellan skog och omkringliggande område utgöra ett väldefinierat särdrag, som kan detekteras i sensordata och matchas mot en karta. I bebyggd miljö utgör vägar, korsningar och byggnader ofta tydliga särdrag.

Det är viktigt att notera att det inte är nödvändigt att varje enskild bild kan matchas mot kartunderlaget. Många metoder för kartstöttad positionering och navigering kombineras med relativa positioneringsmetoder, som kan överbrygga kortare perioder utan säkra matchningar mellan observationer och karta. Dessa relativa positioneringsmetoder har dock normalt en snabbare feltillväxt. Om perioden utan tydliga särdrag är lång kan positionosäkerheten bli oacceptabelt hög. Då behöver fortsatta observationer jämföras med en större del av kartan, vilket ökar risken för att ingen entydig matchning kan erhållas. Detta innebär att kartmatchningsmetoder kan falla även om plattformen återvänder till ett område med tydliga särdrag, efter en alltför lång tid över ett område utan sådana. Dylka situationer kan hanteras med mer avancerade sensorfusionsfilter, exempelvis partikelfilter, men dessa ökar beräkningskomplexiteten hos algoritmerna vilket kan göra det svårt att implementera dessa i realtid på mindre plattformar.

6.2.2 Inaktuella kartor och landmärkesdatabaser

Inaktuella kartor riskerar att kraftigt försämra noggrannheten hos matchningsbaserade positioneringsmetoder. Problem kan till exempel orsakas av att byggnader eller vägar har tillkommit eller försvunnit sedan kartan genererades. I många fall kan även tillfälliga avvikelser från kartan medföra felaktiga matchningsresultat. Dessa kan exempelvis orsakas av väder, nederbörd, ändrade ljusförhållanden eller årstidsväxlingar med dess tillhörande förändringar i växtlighet.

I figur 6.1 visas exempel på effekter från årstidsvariationer och skuggeffekter. De två bilderna (tagna från Google Earth) är tagna vid olika årstider. Bilderna har betydande olikheter, delvis på grund av snö men också på grund av skuggor orsakade av en lågt stående sol i vinterbilden. Dessa skillnader i fotografierna förväntas medföra svårigheter för algoritmer som gör en direkt matchning mellan bilderna.

6.2.3 Robusthetshöjande modifikationer

Robustheten mot tillfälliga förändringar kan förbättras genom att matcha extrastraherade särdrag i sensor- och referensdata i stället för att använda obearbetade sensordata. I exemplet med ljusvariationer kan en kamerabild påverkas kraftigt, vilket riskerar att leda

till fel vid matchning av bilden mot ett referensfoto. Genom att istället detektera exempelvis vägar i kamerabilden och matcha dessa mot en karta över vägnätet, så kan problemet elimineras i de flesta situationer (förutsatt att förhållandena medger att vägar syns i kamerabilden). Ett annat sätt att uppnå robusthet mot variationer i ljussättning och textur (exempelvis på grund av snö) är att istället matcha geometrisk information, till exempel en höjdmmodell, mot mätningarna. I fallet med mer permanenta förändringar av miljön bör kartan istället uppdateras. På så sätt förbättras robustheten över en längre tidshorisont, eftersom kartan då stämmer bättre överens med verkligheten nästa gång den används.

En viktig aspekt av robusthet är integritetsmonitorering. Detta syftar ofta på förmågan hos en positioneringsmetod att detektera när den riskerar att ge ett felaktigt resultat där den samtidigt underestimerar osäkerheten i mätningen.¹⁶ I [31] presenteras ett antal metoder för integritetsmonitorering i kamerabaserade positioneringsmetoder. I [32] beskrivs två mått som kan användas för att utvärdera robustheten hos positioneringssystem med fokus på fel i initialgissning och hur ofta uppdatering från ett globalt system, som t.ex. GNSS, sker.

Förutom att öka robustheten inom varje separat positioneringsmetod, genom exempelvis integritetsmonitorering, bör resultat från matchningsbaserade metoder även kombineras med information från andra sensorer i ett multisensorbaserat PNT-system. Genom att använda flera oberoende metoder parallellt kan systemets integritet övervakas genom att delresultat från de olika metoderna jämförs med varandra. Till exempel kan tröghets-sensorer eller andra metoder för relativ positionering användas. GNSS-mottagarnas information bör också användas då dessa är tillgängliga och tillförlitliga.

6.3 Kartstöttade positionerings- och navigeringsmetoder

I detta avsnitt presenteras utvalda exempel på kartstöttade positionerings- och navigeringsmetoder. De exempel som ges beskriver tillämpningar för UAV:er och markfordon, där flera av metoderna beskrivs mer detaljerat i [4]. En litteraturöversikt rörande batymetri-stöttad navigering för yt- och undervattensfarkoster ges i [1] medan terrängnavigering för exempelvis styrda vapen beskrivs i [33].

6.3.1 Matchning av lodtittande kameravy mot satellitbild

Ett relativt enkelt sätt att med låg beräkningskomplexitet (som därmed kan implementeras i realtid på små farkoster) positionera en UAV är att matcha bilder från en gimbalstabiliserad lodtittande kamera ombord på UAV:n mot en flyg- eller satellitbild över operationsområdet. Varianter på denna teknik har utvecklats för små UAV:er såväl på FOI [34] som av andra forskargrupper [35]. I [34] matchas kamerabilder direkt mot referensbilden, vilket innebär att metoden inte är robust mot avvikelser i fråga om ljus, årstider etc.

Positionsestimeringen använder ett partikelfilter där varje partikel representerar en hypotes om UAV:ns position. Hypoteserna uppdateras utifrån bildbaserad hastighetsmätning (s.k. optiskt flöde) och dessa hypoteser utvärderas baserat på likheten mellan kamerabilden och referensbilden på den position som motsvaras av respektive partikel. Därigenom kombineras en relativ positioneringsmetod (hastighetsmätning) med en absolut metod (kartmatchning). Metoden uppskattar sin egen osäkerhet, representerad som spridningen hos partiklarna. Ingen explicit integritetsmonitorering är i nuläget implementerad, men det är möjligt att kvantifiera risken för felaktiga positionsestimat genom att beräkna avvikelserna mellan kamerabild och referensbild för den estimerade positionen.

¹⁶ Integritetsmonitorering kan dels utföras på enskilda tekniker och delsystem, dels i multisensorsystemet där resultaten från olika delsystem på olika sätt kan jämföras för att detektera mätningar som är behäftade med stora fel.

6.3.2 Matchning mot segmenterad och klassindeldad satellitbild

Ett sätt att förbättra robustheten i metoden ovan är att dela upp både kamerabild och referensbild i ett antal klasser, och därefter matcha klassindelningen istället för de ursprungliga bilderna. Detta görs exempelvis i [36]. Där används en manuellt skapad referenskartan med klasserna gräs, asfalt och hus utifrån en satellitbild. Sedan segmenteras och klassificeras bilden från UAV:n i samma klasser och systemet använder informationen från båda dessa för att matcha ihop dem och uppskatta sin position och orientering på kartan. Tack vare segmenteringen blir metoden mindre känslig för ljussättning och andra mindre avvikelser i bilderna.

Integritetsmonitorering kan exempelvis integreras i algoritmen genom att utvärdera hur väl de klassificerade kamera- och referensbilderna matchar varandra för den estimerade positionen.

6.3.3 Matchning mot information från GIS

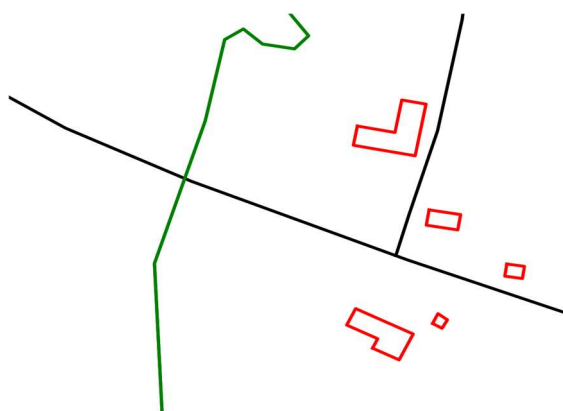
I [37] extraheras objekt som byggnader, vägar och broar ur kamerabilden från en UAV. Dessa matchas sedan mot samma typer av objekt i ett kartunderlag (Geographic Information System, GIS), för att estimeras position och orientering relativt kartan. Precis som i fallet med segmentering ovan leder detta till en högre robusthet mot exempelvis ljusvariationer och årstider, förutsatt att den typ av objekt som extraheras är synliga i bilderna.

Ett annat exempel på denna typ av tillämpning är i vilken en 3D-skannande LiDAR används på ett markgående fordon för att hitta korsningar [38]. Dessa korsningar har sedan matchats mot en förenklad karta i form av ett vägnät där sedan ett filter har använts för att estimeras fordonets position och orientering relativt kartan. Figur 6.2 visar ett exempel på hur data från OpenStreetMap¹⁷ kan visualiseras där vägar, hus och grönområden är representerade.

Även i GIS-baserade metoder finns en möjlighet att övervaka integriteten genom att observera hur väl extraherade objekt matchar kartunderlaget.

6.3.4 Matchning mot 3D-modell

En utökning av de tre positioneringsmetoderna som beskrivs ovan, är att matcha bilder från kameran mot en 3D-modell istället för att matcha mot en tvådimensionell bild, segmentering eller karta. En metod för sådan 3D-matchning är under utveckling [39]. I nuläget är matchningen baserad på textur, vilket gör den känslig för ljussättning.

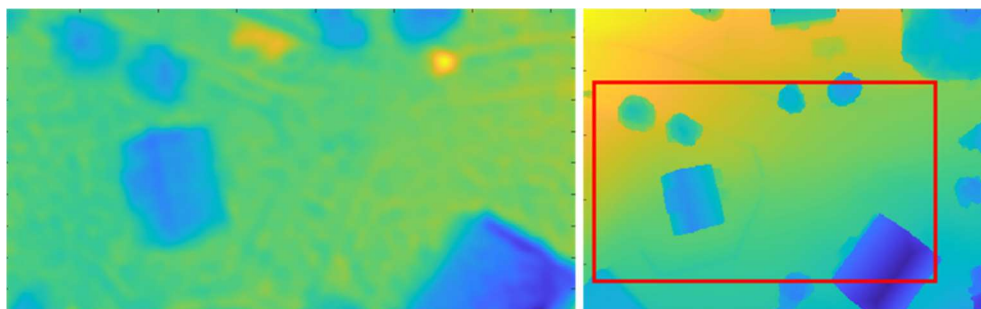


Figur 6.2: Visualisering av referenskartan från OpenStreetMap. Svart utgör vägar, rött representerar byggnader medan grönt representerar gränsen för grönområde.

¹⁷ www.openstreetmap.org (besökt 2023-01-06).



Figur 6.3: Två bilder tagna med 0,2 sekunders mellanrum med UAV:ns kamera. (Bilder publicerade med tack till SENTA Range Commandant).



Figur 6.4: Vänster: Estimerat avstånd från kameran till scenen. Höger: avstånd till scenen enligt 3D-modellen, renderat från en position nära kamerans (på något högre höjd för att ge en mer utzoomad vy). Den röda rektangeln markerar ungefär var den estimerade avståndsbilden passar in.

Pågående arbete syftar till att öka robustheten genom att estimeras scenens geometri utifrån kamerabilder, och därefter matcha mot geometrin i 3D-modellen. Detta förväntas medföra att förändringar på grund av ljus och årstider får mycket liten inverkan på matchningsresultatet. Metoden kommer däremot fortfarande att vara känslig för mer permanenta förändringar som nybyggda, ombyggda eller rivna hus.

Figur 6.3 visar två kamerabilder tagna med 0,2 sekunders mellanrum. I figur 6.4 visas de estimerade avstånden till objekt i bilden (baserat på de två bilderna¹⁸) och även de estimerade avstånden till objekt som beräknas utifrån en 3D-modell (givet en hypotetisk UAV-position rakt ovanför området). Den estimerade avståndsbilden kan vid en visuell inspektion enkelt matchas till modellen vilket gör det troligt att det även kan implementeras automatiskt.

6.3.5 Matchning av bild från fordon mot 3D-punktmoln

Lantmäteriets laserdata¹⁹, är ytterligare en typ av kartinformation som kan användas i ett system för lokalisering mot karta. En bild tagen från marken kan då matchas mot en karta i form av ett georefererat 3D-punktmoln med hjälp av särdrag extraherade från både karta och bild som sedan matchas mot varandra.

Ett exempel på detta (dock ej med Lantmäteriets laserdata) beskrivs i [40]. Här segmenteras 3D-punkterna till olika klasser, såsom mark, byggnadstak och övrigt. Därefter anpassas en modell till varje hustak och fasad. Sammantaget används sedan denna karta, bestående av 3D-modeller av hustak och mark, till att rendera en markvy i form av en djupbild. Särdrag från dessa kartgenererade bilder, i form av hörn och linjer från

¹⁸ Vid estimeringen av avstånd används bildparet på liknande sätt som med en stereokamera, där avståndet i varje pixel beräknas utifrån hur mycket det som avbildas i pixeln har rört sig från den ena bilden till den andra. Dock är avståndet mellan de två kamerapositionerna okänd i detta fall, vilket leder till att endast relativa avstånd kan estimeras. Områden med blå färg har ett kortare estimerat avstånd än områden med gul färg, men de absoluta avstånden är okända.

¹⁹ Lantmäteriets laserdata innehåller ett punktmoln med klassificerade punkter baserat på flygburen laserskanning (www.lantmateriet.se/sv/geodata/vara-produkter/produktlista/laserdata-nedladdning-skog/, besökt 2022-12-07).

byggnader, matchas sedan mot motsvarande särdrag extraherade från den bild som genereras från fordonets sensorer. Detta används i kombination med begränsningar från en vägnätskarta baserad på OpenStreetMap för att uppskatta fordonets position och orientering gentemot kartan.

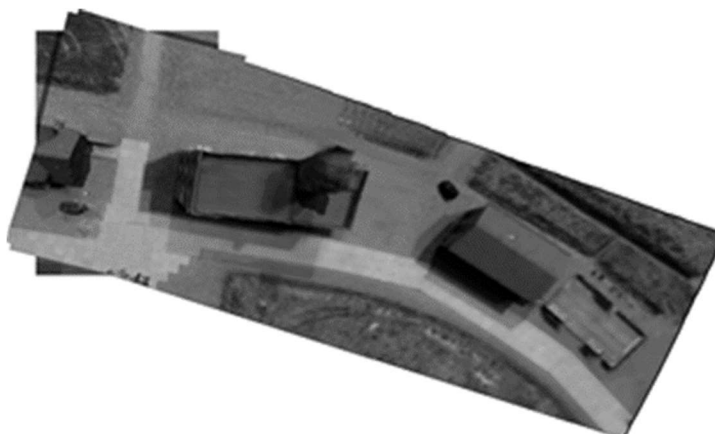
Ett annat exempel presenteras i [41], där stereokameravyn från ett markfordon används med 3D-punktmoln som referensskarta. Här används ett högupplöst 3D-punktmoln för att rendera en syntetisk djup- och intensitetsbild utifrån en markposition. En transformation estimeras sedan mellan den syntetiska bilden och den från stereokameran för att estimeras position och orientering av markfordonet.

6.3.6 Fusion av kartstöttad och relativ positionering, samt kartuppdatering

Genom att kontinuerligt estimeras en UAV:s förflyttning fås ett komplement till den kartstöttade positioneringen. Estimatet av förflyttning är en typ av relativ positionering, som beskriver UAV:ns position relativt en tidigare punkt. Fördelen med den typen av positionering är att den är oberoende av kartan, och alltså fungerar även i miljöer där kartan är okänd eller felaktig.

Ett sätt att genomföra relativ positionering är att inkrementellt bygga upp en ny karta, som plattformen kan positionera sig i relation till. Detta är alltså en variant av visuell odometri alternativt SLAM. I fallet med en lodtittande kamera på en UAV kan detta implementeras genom att bygga upp en mosaik²⁰. Ett exempel på en sådan mosaikbild visas i figur 6.5. Vid skapande av mosaiken behöver en sekvens av bilder transformeras så att de passar ihop med varandra. Om flyghöjden och kamerans parametrar (fokallängd, linsdistorsion etc.) är kända så ger dessa bildtransformationer även information om UAV:ns förflyttning mellan bilderna.

Att bygga en sådan mosaik parallellt med kartbaserad positionering möjliggör en enkel typ av integritetsmonitorering. Om den relativa och den kartbaserade positioneringen är överens, är det sannolikt att positionsestimatet är korrekt. Fusion av relativ och kartbaserad positionering är också användbart för att upprätthålla positioneringsförmåga i fall där miljön innehåller för få unika särdrag för att kartmatchningen ska ge entydiga resultat, men där strukturen ändå är tillräcklig för att relativ positionering ska fungera. En ytterligare fördel är att mosaiken utgör en aktuell beskrivning av hur området ser ut, vilket kan användas för att vid behov uppdatera kartan om den har förändrats.



Figur 6.5: Mosaikbild skapad från ett antal kamerabilder tagna vid flygning över ett område.

²⁰ En mosaik refererar här till en bild som byggs upp av delar från flera andra bilder. Varje delbild bidrar med information om en del av världen, och delbilderna sätts ihop så att mosaikbilden avbildar ett större område än vad som får plats inom kamerans synfält.

Det är dock inte uppenbart hur positionsestimat från den kartbaserade och den relativa positioneringen ska fusioneras i de fall då algoritmerna ger olika resultat. Detta medför också att det kan vara svårt att veta när och var kartan bör uppdateras baserat på den genererade mosaiken.

I [42] ges ett exempel där kamerabilder från ett fordon användes för att uppdatera en 3D-modell av miljön och därmed upptäcka och införa förändringar i kartan.

6.3.7 Kooperativ SLAM

En typ av kartmatchning kan ske genom att flera SLAM-baserade system samverkar, så kallad kooperativ SLAM. En variant av detta beskrivs i [43] där flera fordon bygger upp sina egna kartor (utan tidigare kartinformation från området) med hjälp av 3D-LiDAR och sedan delar varandra dessa kartor för att tillsammans skapa en bättre lägesbild.

Positioneringssystem baserade på SLAM har inbyggd skattning av sin osäkerhet och därmed viss integritetsmonitorering. Detta kan användas om ett system rapporterar en hög osäkerhet och då får hjälp av en mer noggrann skattning från andra system i närheten.

6.4 Slutsatser

Kartstöttade positionerings- och navigeringssystem utgör ett viktigt komplement till GNSS-mottagare i exempelvis telestödda miljöer, då även dessa kan ge estimat av absolut position och orientering. Därmed kan den drift som många andra stöttande tekniker erfar elimineras (där felen ökar som funktion av tid eller förflyttad sträcka).

Vilken noggrannhet som kan uppnås med kartstöttad positionering beror till stor del på förutsättningarna avseende sensorer, kartunderlag och den miljö där systemet används. I de försök som genomförts, med tvådimensionell kartmatchning och tredimensionell modellmatchning från UAV, har positionsfel omkring 1-10 meter observerats. Dessa försök har genomförts i dagsljus på relativt låga flyghöjder (40-80 meter), med aktuella och högupplösta kartor och 3D-modeller. Flygning har skett över bebyggelse och över en flygplats, där rullbana och taxivägar utgjort tydliga visuella särdrag.

På högre höjd, då avståndet mellan sensorn och objekt på marken ökar, förväntas positionsfelet växa. Detta är dels en följd av att den effektiva upplösningen (uttryckt i pixlar per meter) avtar med ökande höjd, och dels av att vinkelfel i kamerans montering på UAV:n ger upphov till positionsfel som ökar med avståndet mellan UAV och mark. Den senare effekten påverkar dock endast estimatet av UAV:ns position, medan positionen för det område på marken som avbildas av kameran är opåverkat. Detta innebär att inmätning av mål, som detekteras i kamerabilderna, kan vara mer precis än UAV:ns positionsestimat.

Hur positioneringsfelet påverkas av övriga förutsättningar (kartunderlag, miljö och ljusförhållanden) har inte undersökts, men metoderna för kartstöttad positionering och navigering är beroende av att miljön är informativ och av att kartan och verkligheten stämmer överens med varandra. Då en visuell kamera används medför detta vissa krav på ljusförhållanden. Andra sensortyper som till exempel termiska kameror har bättre förutsättningar att fungera i mörker, men tillgången till kartunderlag i det termiska våglängdsområdet är sämre än i det visuella. Aktiva avbildningsmetoder som LiDAR har fördelar genom att de ser i mörker och mäter geometri, vilket gör dem okänsliga för variationer i fråga om både ljus och textur hos avbildade objekt. Nackdelarna är dels att sensorn emitterar ljus och därmed lätt kan upptäckas, dels dess begränsade räckvidd (få LiDAR-sensorer, som är tillräckligt små och lätta för att monteras på en liten lågflygande UAV, kan mäta avstånd längre än cirka 100 meter).

Många typer av kartor kan användas som underlag (referenskartor) för kartstöttade metoder, såsom satellitbild, 3D-punktmoln, 3D-modell och GIS-data. Dessa har sina olika för- och nackdelar, t.ex. är satellitbild ofta lättillgänglig medan 3D-data i form av punktmoln eller 3D-modeller ger mer detaljerad information som kan fungera bra även vid kraftigare årstidsvariationer. GIS-data kan underlätta för positioneringssystemet i bebyggd

miljö med hus och korsningar men kan få svårare att bidra för obebyggd och homogen landsbygd. Även databaser med georefererade landmärken kan användas i detta syfte.

Oavsett vilken metod som används så är integritetsmonitorering viktig för att veta dels vad som kan orsaka högre osäkerhet och dels hur dessa situationer ska hanteras, t.ex. att tillfälligt gå över till en metod baserad på relativ positionering eller att multisensorfusionsfiltret ska förlita sig mer på andra stöttande sensorer och delsystem.

7 Internationella samarbeten

Projektet har deltagit i två internationella samarbeten: *GPS and NAVWAR RDT&E MoU*²¹ och SET-RTG-229 *Cooperative Navigation in GNSS Degraded and Denied Environments*. Projektet har även i en begränsad omfattning delfinansierat EU-projektet *PRS Pilot Project for Demonstration* (3PfD).

7.1 GPS and NAVWAR RDT&E MoU

Deltagandet i *GPS and NAVWAR RDT&E MoU* finansieras gemensamt av projekten Robust PNT och TK mot GNSS (FoT-område Telekrig). Detta internationella samarbete är centralt för den svenska militära forskningen och teknikutvecklingen inom GNSS-området och det ger viktig information rörande moderniseringen av GPS, och prestanda samt tidsplan för införandet av GPS M-kod.

7.2 NATO STO

Flera FoT-projekt på FOI deltog under perioden 2017 till 2020 i gruppen SET-RTG-229 som fokuserade på att utveckla och demonstrera robusta PNT-tekniker i telestörda miljöer. FOI deltog med flera PNT-tekniker, bland annat kartstöttade navigeringstekniker (baserade på en kamera på UAV eller LiDAR på fordon), automatisk rörelsedetektion av fordon och soldater baserat på UAV:ns visuella kamera, samt estimering av position för detekterade fordon och soldater med stöd av karta och visuell kamera. Positionerna kan därefter sändas till respektive fordon och soldat som kan använda dessa estimat för att uppdatera sin positionslösning. Den senare delen genomfördes dock inte i realtid. Utöver detta genomförde FOI även kartering av utomhus- och inomhusmiljöer, med UAV respektive ett buret stereokamerasystem. Under 2020 utvärderades resultaten från demonstrationen och en slutrapport sammanställdes [44].²²

FOI deltog även i anordnandet av ett forskningssymposium inom ”Cooperative Navigation in GNSS Degraded and Denied Environments” som genomfördes i september 2021 i Split, Kroatien. Detta symposium arrangerades som en separat aktivitet (SET-RSY-275). FOI presenterade under symposiet ett bidrag som baserades på det arbete som genomfördes inom ramen för SET-229 [45].

Deltagandet i SET-229 och SET-275 var värdefullt då det bland annat gav en god bild av mognadsgraden för olika deltekniker. Det gav även möjlighet att förbättra kunskapen om forskningsfronten inom detta område, verifiera kvaliteten på vår egen forskning och ge underlag för inriktning av exempelvis framtida FoT-verksamhet.

SET-RTG-309 *NATO PNT Open System Architecture & Standards to Ensure PNT in NAVWAR Environments* är en efterföljare till SET-229. Där studeras framtida multisensor-fusionsarkitekturer med öppen arkitektur och standardiserade gränssnitt, som även kan möjliggöra modularitet och enklare integration av nya sensorer (”plug-and-play”-funktionalitet). Målet är att utveckla och även demonstrera en öppen standardiserad arkitektur för ett modulärt PNT-system som ska kunna genomföra operationer i telestörda miljöer.²³ Deltagandet i SET-309 har under 2022 finansierats primärt genom projektet *Obemannade farkoster och autonoma system – teknik och operatörer* som genomförs under Temaområde Autonomi och obemannat. Detta forskningsområde utgör en central del av det nya FoT-projektet Militära PNT-system som påbörjas 2023 inom FoT Ledning och MSI och det fortsatta deltagandet finansieras inom ramen för det projektet.

²¹ Försvarsmakten är formell avtalspart i detta MoU.

²² Vid SET-panelens möte i maj 2022 belönades deltagarna i SET-229 med SET Panel Excellence Award. Det är ett pris som årligen delas ut till deltagarna i en utvald aktivitet som genomförts inom området.

²³ www.sto.nato.int/Pages/activitieslisting.aspx (besökt 2023-03-15).

8 Diskussion

Projektet har haft fem övergripande frågeställningar som inriktat forskningsaktiviteterna:

- Hur ser omvärldsutvecklingen ut inom PNT-området?
- I vilka scenarion kan en robust GNSS-mottagare stöttad med gruppantennor ge en tillfredställande prestanda, och när krävs stöttning från alternativa navigeringssystem?
- Hur bör multifrekvens- och multikonstellationsmottagare, som använder kombinationer av krypterade och/eller öppna signaler från olika GNSS, designas för framtidens militära plattformar?
- Vilka stöttande deltekniker bör integreras i ett multisensornavigeringssystem för att uppnå önskad prestanda?
- Hur bör felaktigheter i referenskartor (exempelvis Lantmäteriets 3D-kartor) hanteras för att inte kraftigt försämra navigeringssystemets noggrannhet vid kartstöttad navigering?

I detta kapitel diskuteras projektets forskning och resultat utifrån dessa frågeställningar.

8.1 Omvärldsutvecklingen inom PNT-området

Det pågår en omfattande modernisering av GNSS med nya tjänster, inklusive krypterade tjänster (GPS M-kod och Galileo PRS), som bland annat kommer ge en ökad robusthet mot störning och vilseledning. En kritisk ny förmåga som möjliggörs är även störning av civila mottagare inom ett operationsområde (BFEA), utan att möjligheten att använda M-kod eller PRS påverkas allvarligt.

Gruppantennor ger ett kraftigt ökat skydd mot störning och vilseledning. En del moderna gruppantennor gör numera en spatiotemporal filtrering individuellt för de enskilda GNSS-signalerna. Dessa gruppantennor har en avsevärt högre komplexitet, både i form av beräkningskomplexitet men även i hårdvara då exempelvis plattformens orientering måste estimeras kontinuerligt. Fördelen med dessa gruppantennorsystem är bland annat att de minskar problemen med oavsiktlig undertryckning av de autentiska GNSS-signalerna [3].

GNSS-mottagare som inte utrustas med moderna gruppantennor (som typiskt har inbyggd detektions- och pejlförmåga) förses i allt större omfattning av algoritmer som detekterar när den är påverkad av stör- och vilseledningsattacker. Denna information är viktig i ett multisensorbaserat PNT-system.

Det pågår en snabb utveckling av kartstöttade positioneringssystem som utgör ett potentiellt viktigt komplement för att nå en hög noggrannhet vid längre operationer i telestörda miljöer. Relativt lite information har publicerats öppet rörande användning av passiva sensorer (såsom termiska IR-kameror) i mörker och detta är ett område som bör adresseras med högre intensitet i den fortsatta forskningen.

Det pågår civilt en snabb utveckling av LEO-satellitssystem där ett stort antal satelliter redan idag är operativa. Vissa LEO-satelliter, både militära och civila, kommer i framtiden även utrustas med PNT-nyttolaster som kan ge en högre robusthet och noggrannhet än dagens GNSS. Flera kommersiella operatörer planerar att bygga upp LEO-baserade satellitssystem för PNT-tillämpningar. Majoriteten av LEO-satelliterna kommer dock inte att utrustas med dedikerade nyttolaster för PNT, men de kan användas opportunistiskt för att estimeras avstånd till satelliterna (signals-of-opportunity, SoOp). Detta kan ge en ökad robusthet i telestörda miljöer om kommunikationen sker på frekvensområden som är tillräckligt separerade från GNSS-signalernas frekvenser.

Det pågår även en utveckling av metoder som använder sig av magnet- och gravitationsfält som stöd vid navigering, baserat på jämförelser med kartor över lokala variationer alternativt med SLAM-tekniker. Utvecklingen av högkänsliga kvantbaserade sensorer förväntas medföra ett uppsving för den här typen av tekniker. Utmaningen är dock ofta

kopplad till att minimera, eller kompensera för, plattformens bidrag till det uppmätta magnetfältet.

Den viktigaste militära utvecklingen inom multisensorfusion rör utvecklingen av arkitekturer med standardiserade öppna gränssnitt som medger en hög grad av modularitet och ”plug-and-play”-funktionalitet. Detta kan i framtiden medföra att samma multisensorsystem och fusionsalgoritm kan användas på ett antal olika plattformar, men där sensorerna anpassas till respektive plattformers möjligheter och krav. Det bör även ge möjlighet att snabbt uppgradera PNT-systemet med nya förbättrade sensorer när sådana blir tillgängliga. Upphandlingen av sensorer och multisensorfusionsalgoritm kan även separeras och läggas på olika industrier. En viktig möjliggörare för sådana modulära standardiserade PNT-system är att tillförlitliga osäkerhetsestimater av sensorer, delsystem och i själva PNT-systemets sensorfusionskärna utvecklas.

8.2 Robusthet hos GNSS-mottagare med gruppantennbaserade störskyddssystem

Gruppantennbaserade störskyddssystem kan ge en kraftigt ökad robusthet vid operationer i telestörda miljöer. Enligt datablad kan de undertrycka störsignaler med omkring 40 dB.²⁴ De kan även undertrycka starka vilseledningssignaler. Moderna gruppantennor kan dessutom detektera störning, och hur stark den är och dess infallsriktning. Det finns dock situationer där kombinationen av en krypterad mottagare och gruppantenn behöver kompletteras med ytterligare sensorer för att nå önskad robusthet. Det är angeläget att genomföra ytterligare utvärderingar av experimentsystemet med dess gruppantenn men dylika försök är komplexa att genomföra då de förutsätter störning med hög effekt. Detta kan genomföras på provplats Vidsel i samband med andra försök som FOI genomför.

8.3 Framtidens militära GNSS-mottagare

Försvarmakten använder idag militära GPS-mottagare, som baseras på den krypterade P(Y)-koden och säkerhetsmodulen SAASM (Selective Availability Anti-Spoofing Module), på ett flertal plattformar. Nya SAASM-baserade mottagare kan inte längre beställas utan Försvarmakten måste nu påbörja införandet av GPS M-kodsmottagare som utvecklas i USA under MGUE-programmet (Modernized GPS User Equipment). Serieleveranser av M-kodsmottagare kommer sannolikt att påbörjas under 2024, men FOI och Försvarmakten förväntas få tillgång till M-kodsmottagare under 2023 för utvärderingar. Dessa mottagare bör utgöra grunden i *alla* framtida militära PNT-system.²⁵

PRS är en liknande tjänst som är under utveckling inom Galileoprogrammet. PRS-tjänsten kan bli operationell redan inom ett par år. Baserat på status för europeisk industris utvecklingsprojekt kopplade till mottagarutveckling för Galileo PRS är det sannolikt att *robusta* PRS-mottagare²⁶ anpassade för militär användning kommer att finnas tillgängliga först några år efter M-kodsmottagare. Det finns dock flera fördelar kopplade till redundans, robusthet och prestanda med att integrera både M-kodskort och PRS-kort i en mottagare. Vid installationer av första generationen av M-kodsmottagare bör därför, om möjligt, tas höjd för att i ett senare skede även kunna föra in PRS-mottagare (utan större modifikationer i exempelvis hårdvara).

På 5-10 års sikt är det möjligt att även civila okrypterade GPS- och Galileosignaler kommer att användas som *komplement* till krypterade tjänster (M-kod eller PRS). Det kan

²⁴ Se t.ex. [novatel.com/products/anti-jam-antenna-systems-gajt/gajt-710ml-anti-jam-antenna](https://www.novatel.com/products/anti-jam-antenna-systems-gajt/gajt-710ml-anti-jam-antenna) (besökt 2023-01-11)

²⁵ Notera att rekommendationen är att M-kodsmottagare utgör *minimivån* i militära PNT-system, dvs. okrypterade civila mottagare ska inte användas. En motivering är att användare av civila mottagare i exempelvis bakre logistikförband, där i framtiden kan utsättas för egen störning (BFEA) av allierade förband i syfte att skydda baser eller kritisk infrastruktur.

²⁶ Serverbaserade mottagare kommer finnas tillgängliga tidigare men de är beroende av en kommunikationslänk och de förväntas inte heller få motsvarande nivå av robusthet mot störning.

ge en ökad robusthet och noggrannhet men till priset av en ökad komplexitet. På kort sikt är dock rekommendationen att de inte integreras då det fortfarande saknas tillförlitliga metoder för att bedöma osäkerheten (noggrannheten) för de olika signalerna och pseudoavståndsmätningarna.

8.4 Stöttande deltekniker

Det finns ett stort antal tekniker som kan användas för att öka robustheten hos ett PNT-system i telestörda miljöer där GNSS-mottagaren kan bli utstörd. Kunskapsuppbyggnad har genomförts i projektet rörande två potentiellt viktiga tekniker, hastighetsstöttad tröghetsnavigering och kartstöttad navigering.

8.4.1 Hastighetsstöttade TN-system

Hastighetsstöttning kan genomföras på olika sätt beroende på plattform. I marina tillämpningar kan aktiva akustiska sensorer som DVL eller CVL användas för att mäta hastigheten. I fordonstillämpningar används typiskt hjulodometri för att få en hastighetsmätning. Banddrivna fordon, samt vissa UGV:er, använder sig av s.k. skid steer för styrning vilket resulterar i andra felmodeller än för hjulodometri. Visuell odometri är ytterligare ett sätt att erhålla en hastighetsmätning som kan användas för att stötta TN-systemet. Det används exempelvis i mindre UAV:er och det finns experimentsystem där visuell odometri används även i soldatsystem.

Hastighetsstöttning är ett effektivt sätt att reducera feltillväxten i TN-system. Detta bör inkluderas i framtida PNT-system. Det är dock kritiskt att utveckla algoritmer för tillförlitlig osäkerhetsestimering av hastighetsmätningarna.

8.4.2 Robusthet mot fel i referenskartor vid kartstöttad positionering och navigering

Kartstöttad positionering och navigering är en potentiellt viktig stöttande teknik som kan möjliggöra längre operationer i telestörda miljöer. Metoden ger, liksom en GNSS-mottagare, estimat av plattformens absoluta position och därmed kan den kumulativa feltillväxt elimineras som dödräknande tekniker drabbas av. Vid operationer i telestörda miljöer där GNSS-mottagaren är utstörd under en längre period så utgör kartstöttade tekniker därmed ett viktigt tillskott. De kan dock uppvisa stora fel i positions- och orienteringsestimaten i situationer då referenskartorna inte längre är korrekta. En försvårande faktor är även om det osäkerhetsestimat som anges inte återspeglar de stora fel som kan uppstå på grund av felaktiga referenskartor.

Felaktigheter i referenskartor kan vara orsakade av olika fenomen. Bestående felaktigheter kan exempelvis orsakas av nyttillkomna eller rivna byggnader eller vägar. Varierande ljusförhållanden och årstidsväxlingar kan istället medföra tillfälliga avvikelser i kartunderlaget. Genom att matcha extrasträdda särdrag från sensordata till kartan, istället för att matcha insamlade sensordata direkt, är det möjligt att minska effekten av avvikelser orsakade av ljusförhållanden, väder, och årstidsväxlingar. Särdrag kan vara geometriska (exempelvis höjdvariation) eller detekterade objekt som byggnader och vägar.

Kartstöttade positionerings- och navigeringstekniker behöver förse med funktioner för integritetsmonitorering, som automatiskt upptäcker då algoritmen riskerar att underskatta sin osäkerhet eller fungera dåligt på andra sätt. Sådana funktioner kan till exempel utvärdera hur väl sensordata matchar kartunderlaget på den position som estimeras av metoden.

Vid avvikelser i kartunderlaget, orsakade av till exempel nyttillkomna eller raserade byggnader, bör referenskartan även uppdateras. Detta är ur ett tekniskt perspektiv inte svårt att genomföra. Att göra detta automatiskt baserat på insamlade data kan dock vara riskabelt, eftersom felaktiga uppdateringar kan orsaka stora fel vid senare användning av

kartan. Ett alternativ är att automatiskt markera områden där avvikelser upptäckts och föreslå ett nytt kartunderlag, men att en operatör måste granska och godkänna uppdateringen manuellt innan den förs in.

Kartbaserade positionerings- och navigeringsmetoder utgör en viktig teknik som i många situationer har potential att möjliggöra längre operationer i telestörda miljöer. Det finns dock ett behov att vidareutveckla dessa metoder, dels genom att utveckla sensorer och algoritmer för kartmatchning under dåliga visuella förhållanden och dels genom att utveckla algoritmer som kan ge tillförlitliga osäkerhetsestimater.

9 Slutsatser

GNSS-mottagare är sårbara mot fientliga telekrigsinsatser och framtida militära PNT-system bör baseras på multisensorsystem där flera olika stöttande tekniker används. Störtålgigheten hos GNSS-mottagare kan redan idag förbättras avsevärt genom att integrera gruppantennbaserade störskyddssystem och algoritmer för detektion av stör- och vilseledningsattacker. Rekommendationen är att dessa tekniker införs på alla plattformar där det är praktiskt möjligt.

Det är angeläget att snabbt öka kunskapen nationellt rörande GPS M-kod. Försvarmakten behöver i närtid påbörja införandet av GPS M-kod och det är av kritisk vikt att under 2023 påbörja utvärderingar av olika mottagaralternativ. Kunskapsuppbyggnad rörande GPS M-kod genomförs inom ramen för samarbetet *GPS and NAVWAR RDT&E MoU*. Om finansiering för utvärderingar av M-kodsmottagare inte kan lösas i närtid så behöver genomförandet av dessa utvärderingar istället prioriteras inom FoT-verksamheten. Det är även viktigt att fortsätta kunskapsuppbyggnaden rörande Galileo PRS, dels allmänt rörande funktion och prestanda och dels rörande praktiskt handhavande av mottagare gällande kryptohantering osv.

På medellång sikt bör kunskapsuppbyggnad prioriteras inom två områden: (i) utveckling av tillförlitliga positioneringsmetoder baserade på passiva bildalstrande sensorer under visuellt utmanande miljöer (exempelvis i mörker) och (ii) utveckling av tillförlitliga metoder för osäkerhetsestimering i både delsystem och i multisensorfusionsalgoritmen.

Flera långsiktiga kunskapsuppbyggnadsbehov har identifierats. Ett område som bör prioriteras är studier av standardiserade PNT-system (multisensorsystem) med öppna gränssnitt som möjliggör en hög grad av modularitet och ”plug-and-play”-funktionalitet vid exempelvis uppgraderingar av sensorer. Denna utveckling, som drivs internationellt inom exempelvis Nato (SET-RTG-309), nationella militära forskningsorganisationer och av industri, förväntas möjliggöra att samma kärna (multisensoralgoritmer och utvalda sensorer) används på många olika plattformar. Det är även möjligt att integrera ytterligare sensorer och algoritmer beroende på plattformens möjligheter och behov utan att byta sensorfusionskärnan. Ett annat potentiellt viktigt område är rymdbaserade PNT-tekniker i form av LEO-satelliter med dedikerad nyttolast för PNT och mottagare som utnyttjar radiokommunikation från LEO-satelliter (”signals-of-opportunity”).²⁷

Slutligen så är rekommendationen att inom FoT-verksamheten prioritera genomförandet av ett Transferprojekt inom vilket ett experimentsystem för demonstrationer av ett robust PNT-system (primärt avsett för markfordon) byggs upp. För att nå tillräcklig robusthet i telestörda miljöer förutsätts att GNSS-mottagarens robusthet ökas (med gruppantennor och detektionsalgoritmer) samt att ytterligare stöttande tekniker integreras i ett multisensorbaserat PNT-system. Erfarenheter från utvärderingar, och den kunskapsspridning som genomförs via demonstrationer, förväntas ge ett viktigt stöd till Försvarmaktens förmågeutveckling inom PNT-området. I förslaget till Transferprojekt ingår även kompetensuppbyggnad och prov och försöksverksamhet med prototypmottagare för Galileo PRS.

²⁷ Flera av de identifierade behoven avseende kunskapsuppbyggnad på medellång och lång sikt kommer att beaktas inom det nya projekt som påbörjats inom FoT-område Ledning och MSI (Militära PNT-system), medan andra delar bör inkluderas inom andra FoT-områden (exempelvis Rymd och Sensorer och signaturanpassning).

Referenser

- [1] J. Rantakokko, P. Strömbäck och M. Linné, *GNSS-oberoende navigering – Omvärldsanalys*, Totalförsvarets forskningsinstitut, FOI-R--5328--SE, augusti 2022.
- [2] J. Rantakokko, E. Axell, J. Nygårds, J. Rydell och N. Stenberg, *Tekniker för navigering i urbana och störda GNSS-miljöer – Slutrapport*, Totalförsvarets forskningsinstitut, FOI-R--4907--SE, december 2019.
- [3] E. Beskow, *The Effect of Distortions Induced by Adaptive Antenna Arrays in GNSS Applications*, M.Sc. Thesis, Linköpings Universitet, LiTH-ISY-EX--22/5526--SE, oktober 2022.
- [4] J. Rydell, O. Karlsson, J. Nygårds och S. Nilsson, *Navigering genom robust kartmatchning och hastighetsstöttad dödräkning*, FOI Memo 7719, december 2021.
- [5] K.G. Olsson och E. Axell, *Utvärderingar av robusthetshöjande åtgärder för civil och militär GPS/GNSS*, Totalförsvarets forskningsinstitut. (under slutförande)
- [6] T. Lindgren, P. Eliardsson, E. Axell och P. Johansson, *Rekommendationer avseende detektion av störning och vilseledning av GNSS*, Totalförsvarets forskningsinstitut, FOI-R--4694--SE, 2019.
- [7] E. Axell, *GNSS interference detection*, Totalförsvarets forskningsinstitut, FOI-R--3839--SE, 2014.
- [8] T. Lindgren och E. Axell, *Multiantenntekniker för detektion av vilseledningsattack mot GNSS*, Totalförsvarets forskningsinstitut, FOI-R--4500--SE, 2017.
- [9] E. Axell och T. Lindgren, *Increased Robustness in GNSS Receivers Through Detection of Spoofing Attacks*, Totalförsvarets forskningsinstitut, FOI-R--4105--SE, 2015.
- [10] E. Axell, M. Alexandersson och T. Lindgren, "Results on GNSS Meaconing Detection with Multiple COTS Receivers," i *International Conference on Localization and GNSS (ICL-GNSS)*, Göteborg, 2015.
- [11] E. Axell, E. G. Larsson och D. Persson, "GNSS Spoofing Detection Using Multiple Mobile COTS Receivers," i *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Brisbane, Australien, 2015.
- [12] N. Stenberg, E. Axell, J. Rantakokko och G. Hendeby, "GNSS Spoofing Mitigation Using Multiple Receivers," i *IEEE/ION PLANS*, Portland, 2020.
- [13] N. Stenberg, E. Axell, J. Rantakokko och G. Hendeby, "Results on GNSS Spoofing Mitigation Using Multiple Receivers," i *NAVIGATION*, vol. 69, nr 1, 2022.
- [14] M. L. Psiaki och T. E. Humphreys, "GNSS Spoofing and Detection," *Proceedings of the IEEE*, vol. 104, nr 6, pp. 1258-1270, 2016.
- [15] J. Rantakokko, F. M. Eklöf, T. Lindgren och J. Nygårds, *Robusta positioneringssystem; Slutrapport*, Totalförsvarets forskningsinstitut, FOI-RH--1792--SE, 2017.
- [16] E. Axell, F. M. Eklöf, P. Johansson, M. Alexandersson och D. Akos, "Jamming Detection in GNSS Receivers: Performance Evaluation of Field Trials," i *NAVIGATION*, vol. 62, nr 1, pp. 73-82, 2015.
- [17] D. Akos, "Who's Afraid of the Spoofer? GPS/GNSS Spoofing Detection via Automatic Gain Control (AGC)," *Navigation*, vol. 59, nr 4, pp. 281-290, 2012.
- [18] G. K. Olsson, E. Axell, E. G. Larsson och P. Papadimitratos, "Participatory Sensing for Localization of a GNSS Jammer," i *Proc. International Conference on Localization and GNSS (ICL-GNSS)*, Tampere, Finland, 2022.
- [19] E. Axell, P. Johansson, M. Alexandersson och J. Rantakokko, *Estimation of the position error in GPS receivers*, Totalförsvarets forskningsinstitut, FOI-R--3840--SE, 2014.
- [20] C. Tanil, *Detecting GNSS Spoofing Attacks using INS Coupling*, Ph.D. Thesis, Illinois Institute of Technology, 2016.
- [21] K. D. Wesson, J. N. Gross, T. E. Humphreys och B. L. Evans, "GNSS Signal Authentication Via Power and Distortion Monitoring," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 54, nr 2, pp. 739-754, 2018.

- [22] D. Marnach, S. Mauw, M. Martins och C. Harpes, "Detecting Meaconing Attacks by Analysing the Clock Bias of Gnsr Receivers," *Artificial Satellites*, vol. 48, nr 2, pp. 63-83, 2013.
- [23] G. Reina och R. Galati, "Slip-based terrain estimation with a skid-steer vehicle," *Vehicle System Dynamics*, vol. 54, p. 1384-1404, 2016.
- [24] J. Bjørn, K. Gade, S. Kristian, A. Willumsen och S. Robert, "DVL velocity aiding in the HUGIN 1000 integrated inertial navigation system," *Modeling, Identification and Control*, vol. 25, 10 2004.
- [25] J. Bjørn, K. Gade, och E. Bovio, "Integrated inertial navigation systems for AUVs for REA applications", [Online]. www.navlab.net/Publications/Integrated_Inertial_Navigation_Systems_for_AUVs_for_REA_Applications.pdf (besökt 2022-12-04).
- [26] F. Gustafsson, *Adaptive filtering and change detection* (Vol. 1). New York: Wiley, 2001.
- [27] Nordefco COPA CAPA, *Study report on Unmanning of Systems - Robust Navigation*, april 2019.
- [28] J. Rantakokko (redaktör), *Obemannade farkoster och autonoma system – Årsrapport 2022*, Totalförsvarets forskningsinstitut, FOI-R--5397--SE, februari 2023.
- [29] M. J. Veth och J. Racquet, *Fusion of low-cost imaging and inertial sensors for navigation*, Air Force Institute of Technology (AFIT), 2007.
- [30] K. Yousif, A. Bab-Hadiashar och R. Hoseinnezhad, "An Overview to Visual Odometry and Visual SLAM: Applications to Mobile Robotics", *Intelligent Industrial Systems 1*, pp. 289-311, 2015.
- [31] Chen Zhu, Michael Meurer, Christoph Günther, "Integrity of visual navigation - Developments, challenges, and prospects", *NAVIGATION: Journal of the Institute of Navigation*, 69 (2), juni 2022.
- [32] S. Yi, S. Worrall och E. Nebot, "Metrics for the evaluation of localisation robustness," i *2019 IEEE Intelligent Vehicles Symposium (IV)*, 2019.
- [33] M. Gelin, *Terrain Referenced Navigation with Path Optimization: Optimizing Navigation Accuracy by Path Planning*, M.Sc. Thesis, Kungliga Tekniska Högskolan, TRITA-EECS-EX; 2022:41, 2022.
- [34] J. Rydell, E. Bilock och M. Tulldahl, "Computationally efficient vision-based UAV positioning," i *International Technical Meeting of The Institute of Navigation*, Reston, Virginia, 2019.
- [35] G. Conte och P. Doherty, "Vision-based unmanned aerial vehicle navigation using geo-referenced information," *EURASIP Journal of Advances in Signal Processing*, 2009.
- [36] F. Lindsten, J. Callmer, H. Ohlsson, D. Törnqvist, T. B. Schön och F. Gustafsson, "Geo-referencing for UAV navigation using environmental classification," i *2010 IEEE International Conference on Robotics and Automation*, 2010.
- [37] D.-Y. Gu, C.-F. Zhu, J. Guo, S.-X. Li och H.-X. Chang, "Vision-aided UAV navigation using GIS data," i *Proceedings of 2010 IEEE International Conference on Vehicular Electronics and Safety*, 2010.
- [38] A. Mueller, M. Himmelsbach, T. Luettel, F. V. Hundelshausen och H.-J. Wuensche, "GIS-based topological robot localization through LIDAR crossroad detection," i *2011 14th International IEEE Conference on Intelligent Transportation Systems (ITSC)*, 2011.
- [39] J. Rydell och E. Bilock, "MONST3R: Miniature optical navigation system through 3D recognition", i *Unmanned Systems Technology XXIV*, SPIE, Orlando, USA, 2022.
- [40] B. C. Matei, N. Vander Valk, Z. Zhu, H. Cheng och H. S. Sawhney, "Image to LIDAR matching for geotagging in urban environments," i *IEEE Workshop on Applications of Computer Vision (WACV)*, 2013.
- [41] Y. Xu, V. John, S. Mita, H. Tehrani, K. Ishimaru och S. Nishino, "3D point cloud map based vehicle localization using stereo camera," i *2017 IEEE Intelligent Vehicles Symposium (IV)*, 2017.

- [42] A. Taneja, L. Ballan och M. Pollefeys, "City-scale change detection in cadastral 3D models using images," i *2013 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 2013.
- [43] R. Dubé, A. Gawel, H. Sommer, J. Nieto, R. Siegwart och C. Cadena, "An online multi-robot SLAM system for 3D LiDARs," i *IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*, 2017.
- [44] NATO Science and Technology Organization, *Cooperative Navigation in GNSS Degraded / Denied Environments - Final Report*, Technical Report, STO-TR-SET-229, 2020.
- [45] J. Nygård och J. Rydell, "Cooperative navigation for UAV and ground units," *Proceedings of SET-275 Symposium on Cooperative Navigation in GNSS Degraded and Denied Environments*, STO-RSY-SET-275, Split, Kroatien, september 2021.

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