Tekniker för navigering i urbana och störda GNSS-miljöer

Slutrapport

JOUNI RANTAKOKKO, ERIK AXELL, JONAS NYGÅRDS,
JOAKIM RYDELL, NIKLAS STENBERG

FOI-R--4907--SE
ISSN 1650-1942 December 2019

Jouni Rantakokko, Erik Axell, Jonas Nygårds,
Joakim Rydell, Niklas Stenberg

Tekniker för navigering i urbana och störda GNSS-miljöer

Slutrapport

Titel	Tekniker för navigering i urbana och störda GNSS-miljöer– Slutrapport
Title	Navigation technologies for urban and GNSS-challenged environments – Final report
Rapportnr/Report no	FOI-R--4907--SE
Månad/Month	December
Utgivningsår/Year	2019
Antal sidor/Pages	52
ISSN	1650-1942
Kund/Customer	Försvarsmakten
Forskningsområde	Ledningsteknologi
FoT-område	Ledning och MSI
Projektnr/Project no	E72784
Godkänd av/Approved by	Christian Jönsson
Ansvarig avdelning	Ledningssystem

Sammanfattning

Positionerings- och navigeringssystem utgör viktiga delsystem för praktiskt taget alla militära plattformar. GNSS-mottagare ger i många situationer noggranna estimat av plattformens position, hastighet och tid. I urbana scenarion, där GNSS-signalerna utsätts för flervägsutbredning, dämpning och diffraktion, är dock den noggrannhet och tillgänglighet som kan erhållas med GNSS-mottagare otillräcklig samtidigt som mottagarna relativt enkelt kan störas ut. I framtida konfliktsituationer förväntas GNSS-mottagarna att utsättas för avancerade stör- och vilseledningsattacker.

I rapporten beskrivs hur GNSS-mottagarna kan ges en högre robusthet, dels genom detektion av störning och vilseledning och dels med hjälp av signaler från flera konstellationer. Samverkande navigering kan ge betydande fördelar för mindre plattformar som opererar i GNSS-störda miljöer. Plattformar som har avancerade PNT-system kan ge betydande förbättringar för mindre plattformar som använder enklare sensorer.

Nyckelord: PNT, GNSS, störning, vilseledning, detektion, multikonstellationsmottagare, samverkande navigering

Summary

Positioning and navigation systems constitutes important systems of most military platforms. GNSS-receivers provides accurate position, velocity and time estimates in many scenarios. However, in urban environments, where the satellite signals are subjected to radio wave propagation effects such as multipath propagation, attenuation from buildings and diffraction, the accuracy and availability may be insufficient. Furthermore, GNSS-receivers are susceptible towards jamming and spoofing attacks, which are expected to occur in future conflicts.

The report describes how GNSS-receivers can achieve a higher robustness, through detection of jamming and spoofing attacks and through the use of multi-constellation receivers. Collaborative navigation can also provide substantial benefits for smaller platforms that operate in GNSS-challenged environments. Platforms that are equipped with advanced PNT-systems can yield substantial improvements in particular for smaller platforms that utilize less advanced PNT-systems.

Keywords: PNT, GNSS, jamming, spoofing, detection, MFMC-receivers, collaborative navigation

Innehållsförteckning

1 Inledning

Positionerings- och navigeringssystem utgör viktiga delsystem för praktiskt taget alla militära plattformar. Satellitnavigeringssystem (eng. *Global Navigation Satellite System, GNSS*) utgör normalt grunden för dessa system. GNSS-mottagare ger i många situationer noggranna estimat av plattformens position, hastighet och tid (eng. *Position, Velocity, Time - PVT*). I urbana scenarion, där GNSS-signalerna utsätts för flervägsutbredning, dämpning och diffraktion, är dock den noggrannhet och tillgänglighet som kan erhållas med GNSS-mottagare otillräcklig. GNSS-signalerna kan dessutom enkelt störas ut.

På större plattformar kan avancerade tröghetsnavigeringssystem (TNS) och störskyddssystem i form av gruppantenner (eng. *Controlled Radiation Pattern Antenna, CRPA*) integreras vilket ger en kraftigt ökad robusthet mot avsiktlig störning. Dessa tekniker kan dock vara för dyra, stora eller tunga för att integreras på små och medelstora plattformar såsom arméfordon, mindre fartyg och på exempelvis mindre taktiska och stridstekniska obemannade plattformar. Störsäkra navigeringssystem är en kritisk möjliggörande teknik för utvecklingen av höggradigt automatiserade obemannade system, samtidigt som det är kritiskt att förbättra robustheten mot avsiktlig störning även i dagens RPAS (eng. *Remotely Piloted Aircraft System*) [1]. Obemannade system som inte har en god uppfattning om sin position och orientering, och där kommunikationssystemet samtidigt blir utstört, kan inte längre utföra sin uppgift.

Det finns därmed ett tydligt behov av att utveckla positionerings- och navigeringssystem med en högre grad av robusthet, i form av förbättrat störskydd och ökad tillgänglighet samt integritet. Detta kan åstadkommas genom att: (*i*) komplettera GPS-signalerna med signaler från det europeiska Galileosystemet, (*ii*) detektera (och undertrycka) störning och vilseledning och (*iii*) integrera stöttande sensorer som kan överbrygga kortare eller längre GNSS-bortfall.

Exempel på stöttande sensorer som förväntas användas i de flesta framtida navigeringssystem innefattar lågkostnadssensorer som treaxliga accelerometrar, gyron, magnetometrar, barometer och passiva bildalstrande sensorer. Noggrannheten och tillförlitligheten kan vid navigering med bildalstrande sensorer förbättras avsevärt genom att använda digitala kartdatabaser. Samverkande navigeringstekniker förväntas på sikt möjliggöra en förbättrad prestanda för framförallt mindre plattformar som har stringenta krav på storlek, vikt, strömförbrukning och kostnad.

1.1 Syfte

Rapporten utgör slutrapportering av FoT-projektet *Tekniker för navigering i urbana och störda GNSS-miljöer* som genomförts inom FoT-området *Ledning och MSI* under perioden 2017 till 2019. Rapporten innehåller delvis sammanfattningar av tidigare rapporter som tagits fram i projektet.

1.2 Projektbeskrivning

Följande fyra övergripande frågeställningar har studerats inom ramen för projektet:

- Hur ska navigeringssystemen utformas för små och medelstora plattformar så att tillräcklig robusthet uppnås samtidigt som dessa plattformars stringenta krav på vikt, storlek, strömförbrukning och kostnad kan uppfyllas?
- Hur bör satellitnavigeringssystemet Galileo integreras i framtida militära (multi-) GNSS-mottagare?
- Vilken förmåga till robusthet mot, och detektion av, störning och vilseledning av GNSS-signaler bör införas i militära navigeringssystem?
- Kan samverkande navigering utgöra ett kostnadseffektivt komplement till plattformsbundna navigeringssystem?

Projektets mål var att ge rekommendationer för navigeringssystem-lösningar för små och medelstora plattformar.

1.2.1 Aktiviteter

De tekniker som studerats i projektet är generella och kan användas på ett flertal olika typer av plattformar. Ett flertal aktiviteter har genomförts under projektets gång, bland annat följande tre kunskapsuppbyggande aktiviteter där algoritmer har utvecklats och utvärderats inom följande delområden:

- Utveckling och utvärdering av algoritmer för detektion av störnings- och vilseledningsattacker mot GNSS-mottagare.
- Analyser av potentiella fördelar med multifrekvens- och multikonstellationsmottagare för GNSS.
- Utveckling och utvärdering av algoritmer och strategier för samverkande navigering mellan plattformar med multisensorsystem.

Projektet har utvecklat experiment- och demonstrationssystem i syfte att underlätta för kunskapsöverföringen till Försvarsmakten och FMV. Dessa

demonstrationssystem kommer fortsatt att användas i syfte att öka kunskapen om sårbarheter hos befintliga positionerings- och navigeringssystem och möjliga tekniska lösningar. Projektet deltog i den multinationella demonstration som genomfördes i Sennybridge, Wales, inom NATO SET-229 (*Cooperative Navigation in GNSS Degraded and Denied Environments*).

Finansieringen av FoT-relaterad forskning inom navigeringsområdet har under perioden varit fragmenterad, uppdelad i ett flertal projekt som genomfört olika mindre forskningsaktiviteter. Interna workshops har arrangerats inom ramen för projektet i syfte att sprida information om pågående verksamheter och möjliggöra en koordinering av forsknings-insatserna.

1.2.2 Publikationslista

I projektet har följande FOI-publikationer tagits fram ([2]-[7]):

- E. Axell och T. Lindgren, *Multiantenntekniker för detektion av vilseledningsattack mot GNSS*, Totalförsvarets Forskningsinstitut, FOI-R--4500--SE, 2017.
- T. Lindgren och F. M. Eklöf, *Multi-GNSS - översikt, implementationsaspekter och utmaningar*, Totalförsvarets Forskningsinstitut, FOI-D--0782--SE, 2017.
- J. Rantakokko och F. Marsten-Eklöf, *En beskrivning av två fall av störning och vilseledning som genomförts mot GPS under 2017*, Totalförsvarets Forskningsinstitut, FOI MEMO 6260, december 2017.
- T. Lindgren, P. Eliardsson, E. Axell och P. Johansson, *Rekommendationer avseende detektion av störning och vilseledning av GNSS*, Totalförsvarets Forskningsinstitut, FOI-R--4694--SE, december 2018.
- J. Rantakokko, J. Nygårds, J. Rydell, M. Alexandersson och P. Andersson, *Tekniker för navigering i urbana och störda GNSS miljöer - redovisning av genomförd demonstration och beskrivningar av utvecklade demonstrationssystem*, Totalförsvarets Forskningsinstitut, FOI Memo 6958, december 2019.
- N. Stenberg, E. Axell och T. Lindgren, *Analys av multi-GNSS med GPS och Galileo under påverkan av flervägsutbredning*, Totalförsvarets Forskningsinstitut, FOI-R--4892--SE-0.0, januari 2020. (under tryckning)

Arbetet inom aktiviteten samverkande navigering kommer även att avrapporteras vid vetenskaplig konferens och i NATO-publikationer under 2020.

2 GNSS

Det sker en snabb utveckling inom GNSS-området, både när det gäller införandet av nya GNSS och i form av omfattande moderniseringar av GPS. Fler signaler, vissa med en större bandbredd, kommer att sändas från satelliterna på delvis nya frekvenser. Fler krypterade tjänster är även under utveckling, även riktat mot kommersiella användare, där autentisering av signalerna för detektion av vilseledningsattacker är en viktig komponent. Stora resurser satsas även internationellt på olika förbättringar inom mottagarsegmentet.

GNSS har på kort tid utvecklats till en närmast oumbärlig teknik inom många civila sektorer men det används även i ett stort antal militära plattformar och system. Den ökande användningen av GNSS-mottagare i militära konfliktområden, där både militära krypterade signaler och öppna civila GNSS-signaler används av olika aktörer, har även lett till en kraftig ökning av incidenter med störning och vilseledning av GNSS-mottagare.

I detta kapitel beskrivs först kortfattat principerna för hur ett GNSS fungerar. Därefter ges en beskrivning av typiska stör- och vilseledningsattacker mot GNSS som genomförts de senaste åren. Denna översikt baseras på öppet publicerad information (exempelvis [3],[8]-[11]). Slutligen beskrivs nuläget rörande metoder för detektion av störning och vilseledning, samt en metod för hur vilseledningssignaler kan undertryckas i framtida GNSS-mottagare genom att utbyta information mellan mottagarna.

2.1 Användningen av GNSS i det civila samhället och dess sårbarheter

Det civila samhällets beroende av satellitbaserade system för tids- och positionsangivelser ökar i snabb takt och idag är många samhällskritiska infrastruktursystem beroende av GNSS-mottagare [12]. Deras popularitet härstammar från GNSS-mottagarnas förmåga att ge en noggrann och tillförlitlig position och tid med små och billiga mottagare. De utgör idag en vital komponent som levererar tidsestimat i ett stort antal tillämpningar såsom inom finanssektorn, elförsörjning och kommunikation. GNSS-mottagare används som ett navigeringsstöd av stora delar av befolkningen men de är även viktiga hjälpmedel inom transport- och logistiksektorerna samt för räddningstjänst, polis och ambulans. De är även en integrerad,

kritisk del av navigeringssystemen i autonoma fordon[1] och UAV:er. Även bygg- och anläggningsbranscherna är beroende av GNSS-mottagare med hög positionsnoggrannhet för att öka effektiviteten och säkerheten[2]. Marknaden för GNSS-produkter och stödtjänster överstiger numera 150 miljarder euro per år och under 2019 levererades över 1.8 miljarder GNSS-mottagarchip (främst massmarknadsmottagare med ett pris under 5 euro till exempelvis mobiltelefoner)[3].

Storbritannien genomförde 2018 en omfattande analys av beroendet av noggrann tid från GNSS i samhällskritisk infrastruktur samt för navigering [13]. Ett stort antal kritiska beroenden identifierades och farhågan var även att beroendet kommer att fortsätta öka då samhället blir än mer automatiserat. I USA genomfördes en studie finansierad av NIST (eng. *National Institute of Standards and Technology*) som estimerade att kostnaden för en dag med ett nationellt GPS-bortfall skulle vara omkring en miljard dollar [14]. Även om detta är en grov uppskattning så är det klarlagt att kostnaden för ett bortfall skulle vara substantiellt.

GNSS-mottagare har ett antal kritiska sårbarheter vilket gör det olämpligt att använda dessa som den enda sensorn för tids- eller positionsangivelser i samhällskritiska system. De allvarligaste hoten mot GNSS-mottagare bedöms idag utgöras av avsiktliga stör- och vilseledningsattacker (figur 2.1).

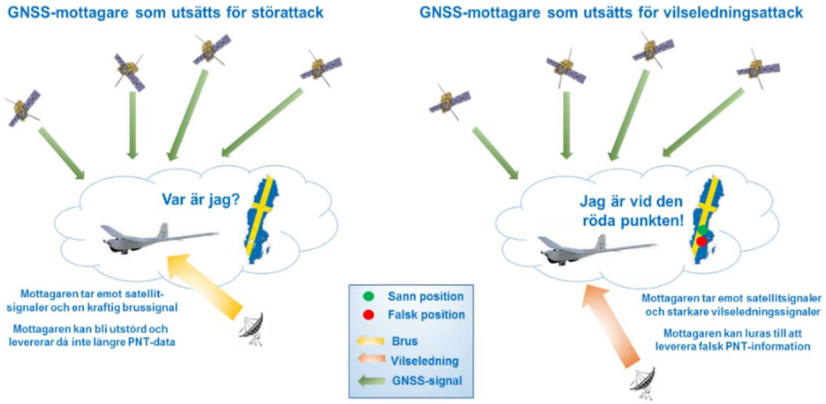
Inom ramen för projektet STRIKE3[4] genomfördes mätningar på ett 50-tal olika positioner och vid en halv miljon tillfällen detekterades interferenser i dessa mätstationer. Drygt 70 000 av dessa bedömdes härröra från avsiktlig störning. I [3] gavs en sammanfattning, baserad på öppna källor, av olika incidenter där avsiktlig störning (Finnmarken, Norge) och vilseledning (Svarta havet) genomfördes mot GPS-mottagare under 2017. Sedan dess har mer information publicerats i öppna källor som visar att förekomsten av vilseledning inom, och i närheten av, ryskt territorium fortsatt pågår i en omfattning som är större än vad som tidigare varit allmänt känt [8]. Samtidigt misstänks Ryssland numera även ha genomfört störattacker direkt riktat mot exempelvis NATO-övningar som

[1] www.septentrio.com/en/insights/role-gnss-localization-safe-assisted-driving

[2] www.septentrio.com/en/insights/what-spoofing-and-how-ensure-gps-security

[3] www.gsa.europa.eu/system/files/reports/market_report_issue_6.pdf

[4] www.gnss-strike3.eu/, ett EU H2020 projekt som delfinansierades genom GSA (*European GNSS Agency*).



Figur 2.1: Effekterna av framgångsrik störning (vänster) och vilseledning (höger) mot en GNSS-mottagare.

Trident Juncture[5]. Dessa stör- och vilseledningsattacker fortsätter trots det faktum att navigationssystemen på civila fartyg och passagerarflyg även utanför ryskt territorium blivit utstörda eller vilseledda[6].

2.2 Principerna för GNSS

Det finns fyra globala GNSS som är (eller som under 2020 eller 2021 förväntas bli) fullt operativa:

- USA: *NAVSTAR Global Positioning System* (GPS).
- Ryssland: *Global'naya Navigatsionnaya Sputnikovaya Sistema* (Glonass).
- Kina: *Beidou Navigation Satellite System* (BDS-2).
- EU: Galileo.

Galileo är det enda systemet som står under civil kontroll. De olika GNSS sänder signaler på flera frekvenser och med olika bandbredd, effekt och modulation[7]. Utöver de globala satellitnavigeringssystemen finns även flera regionala system som förbättrar GNSS-mottagarnas prestanda, bland annat det indiska NavIC (eng. *Navigation Indian Constellation*) och det japanska QZSS (eng. *Quasi-Zenith Satellite System*). Storbritannien

[5] www.aftenposten.no/norge/i/P3bAG6/Sa-ofte-slar-Russland-ut-GPS-nettet-i-Norge-Na-er-russerne-blitt-en-trussel-mot-sivile-fly

[6] thebarentsobserver.com/en/security/2018/11/warning-possible-gps-jamming-northern-finland

[7] gssc.esa.int/navipedia/images/1/1c/Galileo_Signals_in_Space.png

genomför nu omfattande förstudier som förberedelse för att efter Brexit snabbt kunna realisera ett eget GNSS med både öppna och krypterade signaler.

De olika GNSS fungerar i stort sätt enligt samma grundprinciper. GPS och Galileo är uppbyggda av tre olika segment: rymd-, kontroll- och användarsegmenten (figur 2.2). Rymdsegmentet för GPS består i dag av drygt 30 satelliter, medan Galileo har 22 aktiva satelliter, som rör sig i förutbestämda banor (figur 2.2). Satelliterna befinner sig mellan 20 000 och 26 000 km från mottagarna vilket leder till att signalstyrkan vid jordytan är mycket låg. Satellitsignalerna innehåller information som gör att mottagarna kan bestämma satelliternas positioner noggrant.

Satelliterna är utrustade med atomur vilket gör att de kan synkronisera sändningarna noggrant. Mottagarna kan då jämföra den mottagna signalen med en lagrad kopia för att avgöra hur lång tid det tog för signalen att nå mottagaren och på så sätt mäta avståndet till de olika satelliterna. Varje satellit använder en unik kod vilket gör att mottagarna kan separera signalerna, och även identifiera satelliterna, vid avståndsmätningarna.

En GNSS-mottagare estimerar sin position, hastighet och tid (PVT) genom att mäta avståndet till minst fyra satelliter. Under goda förhållanden, där mottagarna har fri sikt till satelliterna, ser en mottagare mellan åtta och tolv GPS-satelliter samtidigt. Om både GPS- och Galileosignaler används kan antalet synliga satelliter fördubblas. Ju fler satelliter som mottagaren kan mäta avståndet till, desto högre noggrannhet kan normalt fås.

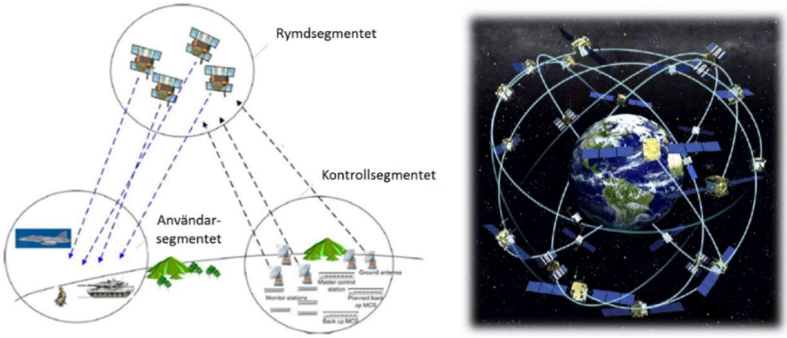
2.2.1 GPS

GPS-satelliterna sänder idag ut en öppen C/A-signal (eng. *Coarse-Acquisition*) och en militär (krypterad) P(Y)-signal. Den senare signalen har en större bandbredd och den sänds även på två frekvenser vilket medför att atmosfärspåverkan på signalen kan estimeras och kompenseras bort.

GPS genomgår en omfattande modernisering där flera nya signaler introduceras. GPS kommer att sända även öppna signaler på flera frekvenser och några av signalerna sänds ut med en högre effekt och större bandbredd (se t.ex. [6] och dess referenser).

2.2.2 Galileo

Galileosystemet är under uppbyggnad och det kommer bestå av 24 satelliter i tre cirkulära plan drygt 23 000 km ovanför jorden. Sex aktiva



Figur 2.2: Vänster: GPS och Galileo består av tre segment: rymdsegment (satelliter), kontrollsegment (övervakning och styrning) samt ett användarsegment (GPS-mottagarna). Höger: Illustration av GPS satellitkonstellation (Illustration: NOAA / Public Domain)

reservsatelliter kommer även finnas tillgängliga. Galileosatelliterna kunde börja användas, tillsammans med GPS-satelliter, för att ge en förbättrad positionslösning redan i december 2016 och systemet deklarerades då ha nått IOC (eng. *Initial Operative Capability*). Galileo förväntas bli fullt operativt senast under 2021.

Fyra tjänster utvecklas inom Galileo (bestående av sex signaler som sänds på fyra frekvensband):

- Open Service (OS): Fritt tillgänglig tjänst för positionering, navigering och tid.
- High Accuracy Service (HAS): En tjänst som kompletterar OS och möjliggör en högre noggrannhet genom användningen av ytterligare en navigationssignal i ett annat frekvensband. Signalen kan bli krypterad för att möjliggöra ökad kontroll av användningen av tjänsten.
- Public Regulated Service (PRS): En robustare, krypterad tjänst avsedd för auktoriserade användare. Nationerna beslutar individuellt vilka användare som tillåts använda PRS.
- Search-and-Rescue (SAR): SAR-tjänsten förväntas när den är fullt utbyggd bestå av två delar: (*i*) en automatisk nödsignal på 406 MHz som detekteras (inom 10 minuter) och lokaliseras (med en noggrannhet på ca 5 km) från Galileosatelliterna och (*ii*) en returlänk som informerar den nödställde om att nödsignalen tagits emot och att räddningsresurser är på väg. SAR-tjänsten integreras i det internationella systemet COSPAS-SARSAT.

2.2.3 Multifrekvens- och multikonstellationsmottagare

Ett sätt att öka noggrannheten och tillgängligheten för en GNSS-mottagare, speciellt i urbana miljöer, är att använda signaler från flera olika konstellationer (t.ex. GPS och Galileo) och även från olika frekvenser. Högprestandamottagare har länge använt signaler från två frekvenser och satelliter från flera GNSS. Även kommersiella lågkostnadsmottagare använder idag ofta satelliter från flera GNSS och vissa tillverkare har under 2019 även utvecklat mottagarkort som kan hantera signaler på två frekvenser.

2.3 Militär användning

Rekommendationen är idag att Försvarsmakten ska använda militära GPS-mottagare som använder den krypterade P(Y)-signalen då de har en förbättrad integritetsmonitorering och har en högre robusthet mot stör- och vilseledningsattacker. Moderniseringen av GPS och utvecklingen av nya GNSS, framförallt Galileo, och de nya bredbandiga signalerna öppnar dock upp för möjligheten att nå en ökad tillgänglighet, noggrannhet och ett förbättrat störskydd genom att komplettera de krypterade signalerna med öppna signaler.

2.3.1 Militär GPS

Försvarsmakten är idag en ackrediterad användare av militära GPS-mottagare, som använder P(Y)-signalerna. De används både i form av handhållna system och även som plattformsburna mottagare.

En ny krypterad GPS-signal, benämnd M-kod, avsedd för militär användning är under införande. Den har flera viktiga förbättringar gentemot den befintliga P(Y)-signalen, exempelvis[8]:

- Möjlighet att sända med högre effekt i utvalda regioner, i syfte att öka motståndskraften mot fientlig störning, utan att orsaka interferenser med de civila signalerna.
- Möjlighet att störa ut civil användning av GNSS på samma frekvensområde, utan att M-kodssignalen störs ut (eng. *Blue-Force Electronic Attack, BFEA*).

[8] GNSS Solutions: New GNSS frequencies, advantages of M-Code, and the benefits of a solitary Galileo satellite, *InsideGNSS*, maj/juni 2006. (insidegnss.com/wp-content/uploads/2018/01/MayJune06GNSSSolutions.pdf)

- Viss ökad robusthet mot störning och ökad positions-noggrannhet.
- Snabbare första positionslåsning jämfört med P(Y)-mottagare.
- Förbättrad säkerhetsarkitektur.

Prestanda för GPS M-kodsmottagare kommer att utvärderas inom ramen för internationella samarbeten de närmaste två åren. Dylika mottagare bedöms kunna finnas tillgängliga för införande på Försvarsmaktens plattformar under 2023 eller 2024.

2.3.2 Galileo Public Regulated Service (PRS)

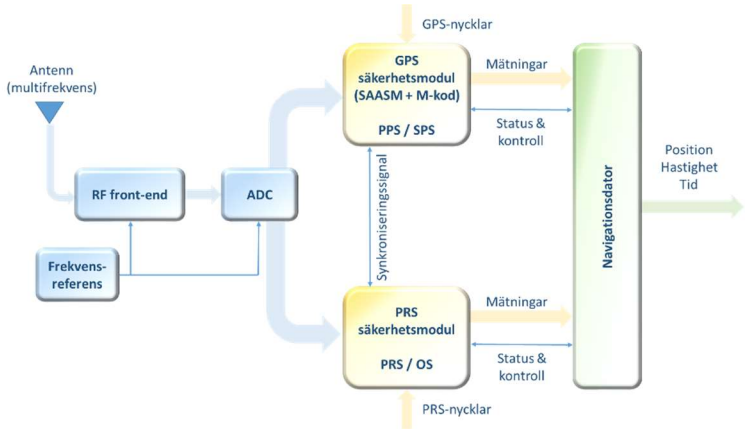
Galileo utvecklar en krypterad tjänst, benämnd PRS (eng. *Public Regulated Service*), som har delvis liknande egenskaper som M-kodssignalen. PRS kommer endast kunna användas av statligt auktoriserade användare, såsom blåljusmyndigheter och militär. De olika nationerna avgör själva vilka som ska få använda PRS och de kan ge exempelvis leverantörer av kritisk infrastruktur (elnät, telekomnät, finans m.m.) tillåtelse att använda denna tjänst.

PRS är avsedd att ge en ökad robusthet och tillgänglighet under exempelvis störning och vilseledning[9], samtidigt som den medger att civila GNSS-mottagare kan störas ut lokalt inom ett operationsområde utan att PRS påverkas (BFEA). En öppen översikt av Galileo PRS ges i [14].

2.3.3 Diskussion

Vid en militär konflikt mot en kvalificerad motståndare kan det vara riskabelt att helt förlita sig på ett enskilt GNSS då detta kan degraderas eller slås ut helt [6]. Att kombinera signaler från flera GNSS har fördelar ur ett robusthetsperspektiv både p.g.a. att flera olika system används (t.ex. GPS och Galileo) men även då användningen av flera signaler på olika frekvensband försvårar för den som vill störa signalen. Att nyttja signaler på olika frekvenser medför att motståndaren tvingas sprida ut störeffekten på ett större frekvensband. Det har en begränsad påverkan på markbundna avancerade störsystem (som primärt inte är effektbegränsade) men det kan ge fördelar mot exempelvis störsystem som placeras på mindre UAV:er.

[9] www.gsa.europa.eu/security/prs



Figur 2.3: Möjlig mottagararkitektur där GPS M-kod och Galileo PRS kompletterar varandra (baserad på [16]). Separata säkerhetsmoduler kommer sannolikt att vara en förutsättning för att realisera en dylik mottagare.

2.3.3.1 En kombinerad militär GNSS-mottagare

En kombinerad PRS och M-kodsmottagare är ett intressant framtida alternativ för militära plattformar. Ett exempel på en möjlig mottagararkitektur visas i figur 2.3, baserat på arbete genomfört av QinetiQ och Rockwell Collins UK [16]. Att använda en kombination av Galileos PRS-signaler och GPS P(Y)- och M-kodssignalerna förväntas ge en avsevärt ökad robusthet mot vilseledningattacker men ytterligare skydd i form av metoder för detektion av vilseledning och störskyddssystem (gruppantenner) bör även införas.

Detaljerad information rörande prestanda för GPS M-kod och Galileo PRS omgärdas av sekretess. Genom internationella samarbeten är målet att delta i utvärderingar av prestanda för dessa tjänster, exempelvis via projektet 3PfD (*PRS Pilot Project for Demonstration*). Resultaten förväntas dock inte vara tillgängliga förrän tidigast i slutet av 2020. Därför diskuteras i denna rapport endast möjligheterna med de öppna Galileosignalerna.

2.4 Sårbarheter

Hoten mot satellitsegmentet utgörs främst av rymdväderfenomen (solstormar) och rymdskrot, men flera länder (USA, Ryssland, Kina och Indien) har visat förmågan att bekämpa fientliga satelliter med antisatellitmissiler. Kontrollsegmentet behöver kunna hantera cyberattacker och cybersäkerheten uppdateras i samband med moderniseringen av marksegmentet för GPS. I en krigssituation utgör även kinetisk bekämpning ett potentiellt hot mot markstationerna och

deras kommunikationssystem. Den mänskliga faktorn och fel vid uppdateringar av mjukvaran i satelliterna har även orsakat fel som påverkat noggrannheten och tillgängligheten. När det gäller användar-segmentet (mottagarna) så är tillgängligheten och noggrannheten fortfarande otillfredsställande i urbana miljöer, framförallt inomhus. Dessa potentiella sårbarheter är svåra att bedöma men en rimlig slutsats är att det är svårt att garantera att ett specifikt GNSS kommer att fungera utan avbrott i en potentiell militär konflikt. En multikonstellations-mottagare har en ökad robusthet mot ovanstående sårbarheter.

De allvarligaste hoten mot GNSS-mottagare idag bedöms dock utgöras av interferenser, avsiktlig störning och vilseledning. Avsiktlig störning och vilseledning av civila GNSS-mottagare pågår kontinuerligt, i en omfattning som är avsevärt större än vad som tidigare har sammanställts i öppna källor [8].

2.4.1 Störning mot GNSS

På grund av de låga signalnivåerna för GNSS-signalerna på jordytan kan även en enkel störsändare störa ut en GNSS-mottagare inom ett relativt stort område. Moderna mottagare kan hantera låga störnivåer utan att dess positionsestimat påverkas. När störnivåerna ökar, men innan mottagaren blivit helt utstörd, ger den utsatta mottagaren normalt ett positionsestimat med ett kraftigt ökande positionsfel och osäkerhet. Effekten av kraftig störning är att den utsatta mottagaren inte längre kan ge ett positions- eller tidsestimat.

Störning mot GNSS-mottagare är vanligt förekommande, även riktat mot civil användning (exempelvis vid stölder av lyxbilar och båtmotorer, riktat mot s.k. *fleet management systems* för lastbilschaufförer, eller vid GPS-baserade biltullar [3]). Störning och vilseledning genomförs numera även regelbundet i militära sammanhang.

Förekomsten av interferenser och lågeffektsstörsändare har karaktäriserats inom det europeiska forskningsprojektet STRIKE3. Störning och vilseledning som utförts av statliga aktörer med avancerade telekrigssystem i närheten av ryskt territorium, och i Syrien, har analyserats och rapporterats i [8]. Dessa öppna källor ger en tydlig bild av att störning och vilseledning mot civila GNSS-mottagare alltjämt pågår i en mycket hög omfattning. Ett stort antal civila GNSS-användare påverkas regelbundet i form av att mottagarna blir utstörda, eller att de levererar falska positionsangivelser.

2.4.1.1 Interferenser och lågeffektstörsändare

I STRIKE3-projektet placerades detektionssystem avsedda att upptäcka interferenser och störning i det civila GNSS-frekvensbandet (L1/E1) på mer än 50 olika utvalda platser, exempelvis vid motorvägar och i hamnar. Närmare en halv miljon incidenter har detekterats varav 70 000 bedöms härröra från avsiktlig störutrustning. I 15 000 fall stördes mottagaren ut helt och kunde inte längre leverera position eller tid. Dessa markbaserade detektionssystem fångar främst upp förekomsten av lågeffektstörsändare som passerar i närheten av detektorsystemet.

2.4.1.2 Störning utförd av statliga aktörer

Flera statliga aktörer har de senaste åren regelbundet genomfört störning av både de civila och militära frekvensbanden. GNSS-mottagare har störts ut bland annat i och omkring militära konfliktområden som Syrien och Ukraina ([8],[10],[16]).

Under de senaste tre åren har ett stort antal varningar till civil flyg- och sjöfart gått ut som varnar för GNSS-störning[10]. De senaste aktiva varningarna rör medelhavet och Persiska Viken och Hormuzsundet[11,12]. Civila passagerarflygplan har även under juni och juli 2019 utsatts för GPS-störning i luftrummet ovanför Ben Gurion flygplatsen i Tel Aviv[13]. Markbaserade mottagare påverkades inte. En trolig källa till störningarna i Israel var ryska telekrigssystem som är aktiva i Syrien, eventuellt ända från den ryska militära basen i Khmeimim som är 350 km bort. I Sydkorea rapporterades att GPS-störning, som genomfördes av Nordkorea under våren 2016, påverkade mottagarna i över 100 pasagerarflygplan och omkring 70 fiskebåtar[14,15].

---

[10] MSCI advisory, som ges ut av MARAD (*US Maritime Advisory*) som är en del av DoT (*US Department Of Transportation*), samt NOTAM (*Notice to Airmen*).

[11] www.maritime.dot.gov/msci-advisories, ”2019-013-Eastern/Central Mediterranean and Suez Canal – GPS Interference” varnar sjöfart för kraftig GPS-interferens vid Libyen och nordväst om Malta, vid Egypten nära Port Said och Suezkanalen samt i närheten av Cypern. Se även https://edition.cnn.com/2019/08/07/politics/us-warns-of-iranian-threats-to-shipping/

[12] www.maritime.dot.gov/msci-advisories, “2019-012-Persian Gulf, Strait of Hormuz, Gulf of Oman, Arabian Sea – Threats to commersial vessels by Iran”.

[13] www.timesofisrael.com/disruption-of-gps-systems-at-ben-gurion-airport-resolved-after-two-months/

[14] www.bbc.com/news/world-asia-35940542

[15] www.reuters.com/article/us-northkorea-southkorea-gps/south-korea-tells-u-n-that-north-korea-gps-jamming-threatens-boats-planes-idUSKCN0X81SN

I [3] gavs en sammanfattning av de incidenter av GPS-bortfall som rapporterades under 2017 i norra delarna av Norge och Finland. Från att tidigare ha bedömts vara ett led i egna övningar (exempelvis under Zapad17), med syftet att träna den ryska militären att agera under GPS-bortfall, bedöms de senaste incidenterna istället ha varit riktade direkt mot främmande makts övningar. GPS-störningen som genomfördes riktat mot Trident Juncture påstås av den norska civila och militära underrättelsetjänsten (Etteretningstjenesten) ha utförts med ett avancerat telekrigssystem inifrån ryskt territorium[16]. Inför övningen detekterades först kortare störningar som lokaliserades till Luotsari flygbas. Enligt Etteretningstjenesten flyttades därefter störsystemet till Sjar övningsområde där det placerades på en högre höjd. Antalet detekterade störningar ökade därefter kraftigt i förekomst, längd och effekt under hela övningen. Vid tre tillfällen under 2018 pågick störning av GPS-signalerna i Norge och vid varje tillfälle pågick dessa under en period av två till tre veckor[17].

I Syrien genomförs störning med avancerade telekrigssystem närmast regelmässigt. Forskare vid *University of Austin*, *Texas*, använde under våren 2018 data från en GNSS-mottagare placerad på Internationella rymdstationen (ISS) och lyckades detektera störning mot både L1- och L2-frekvensbanden och även lokalisera störningen (baserat på Doppleranalyser) till den ryska Khmeimimbasen [16]. Störningen genomförs, åtminstone till del, med autentiska GPS-signaler, men utan ett navigeringsmeddelande, vilket medför att mottagaren trackar satelliterna men inte kan ge ett positionsestimat [16]. Denna typ av störning benämns ibland för *Denial-of-Service (DoS) spoofing*. Dessa störsystem sänder med en mycket hög effekt och kan helt slå ut, eller kraftigt försämra noggrannheten för, en GNSS-mottagare på stora avstånd.

Syftet med denna störning är sannolikt att skydda baser mot attacker från UAV:er och precisionsvapen [8],[16]. Ryska baser i Syrien, i Khmeimim och Tartus, attackerades i början av januari 2018 med svärmar av hemmabyggda, GPS-styrda UAV:er som bar IED:er (*Improvised Explosive Devices*)[18].

[16] www.tv2.no/a/10406767/

[17] www.aftenposten.no/norge/i/P3bAG6/Sa-ofte-slar-Russland-ut-GPS-nettet-i-Norge-Na-er-russerne-blitt-en-trussel-mot-sivile-fly

[18] jamestown.org/program/swarm-attack-russias-military-facilities-syria/

2.4.2 Vilseledning

Vilseledning definieras som utsändningen av falska GNSS-signaler med syftet att få en utsatt mottagare att tro att dessa är autentiska signaler vilket medför att mottagaren estimerar en felaktig position och tid [17] (figur 2.1). Vilseledning kan utföras på ett flertal sätt, som har olika effekt på en mottagare. En utsatt mottagare kan även komma att ange att dess positionsestimat har en låg osäkerhet vilket ökar risken för att användaren (eller sensorfusionsalgoritmen i ett multisensorsystem) tror att den angivna positionen är korrekt.

Antalet incidenter där GNSS-mottagare har utsatts för vilseledning är högre än vad som tidigare har rapporterats. I [8] anges att över 1 300 fall av vilseledning av olika GNSS-mottagare, vid över 10 000 olika tillfällen, som drabbat civil sjöfart har upptäckts sedan februari 2016. Dessa fall av vilseledning har verifierats främst genom analyser av fartygens positioner som rapporteras av AIS (eng. *Automatic Identification System*) och de har utförts i och utanför ryskt territorium. Vilseledning har upptäckts på tio olika platser i hamnar runt om i Ryssland. Eftersom analyserna främst är baserade på AIS-data, vilket endast ger information om kustnära vilseledningsfall, så är bedömningen att betydligt fler fall kan antas ha förekommit. Antalet detekterade fall av vilseledning minskade efter de rapporter i utländsk media som vilseledningsattackerna i Svarta havet ledde till under 2017 men de pågår fortfarande i hög omfattning [8]. Vilseledning sker även regelbundet i centrala Moskva[19] sedan 2016, senare även i S:t Petersburg[20], vilket rapporterats i media (exempelvis [9]). Dessa har senare även bekräftats av analyser av data från motionsappar som Strava som visar att personerna ska ha befunnit sig på landningsbanorna på flygplatserna Vnukovo och Sheremetyevo [8]. I alla dessa fall har mottagaren vilseletts till att rapportera en position som varit på en rysk flygplats.

Syftet med vilseledningen bedöms i många fall ha varit att skydda platser där president Putin har befunnit sig eller skydd av viktiga internationella möten, officiella byggnader (t.ex. Kreml, och i Krim och Sochi) och även privata residens [8],[9]. Vilseledning har detekterats på avlägsna platser i samband med besök av presidenten vilket indikerar tillgången till, och användningen av, mobila vilseledningssystem [8].

[19] www.themoscowtimes.com/2016/10/21/the-kremlin-eats-gps-for-breakfast-a55823

[20] www.themoscowtimes.com/2016/12/27/drivers-in-st-petersburg-report-gps-problems-in-city-center-a56653

Fram tills för ett par år sedan var bedömning att det varit relativt komplext att utföra vilseledningsattacker då det krävde en hög kunskapsnivå samt förhållandevis avancerad och dyr utrustning. Den snabba utvecklingen av mjukvaruradio har dock medfört att kostnaden för hårdvaran numera ligger på enstaka tusen kronor, samtidigt som mjukvara för att realisera detta finns tillgänglig gratis på nätet ([3],[9]).

Vilseledningsattacker som de som beskrivs i [17] är ett allvarligt hot mot de öppna, okrypterade GNSS-signalerna. De krypterade militära signalerna har ett bättre skydd mot många typer av vilseledning.

3 Detektion av störning och vilseledning

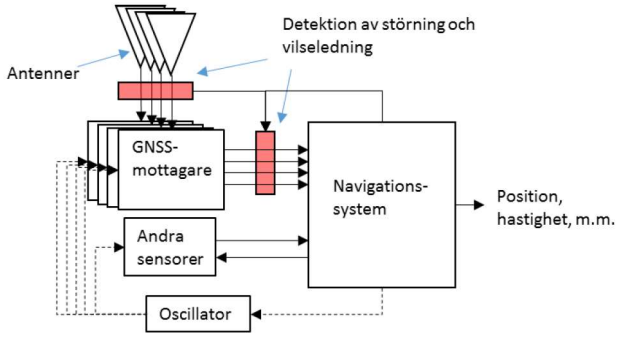
För att nå en hög integritetsnivå behöver en GNSS-mottagare ha förmågan att detektera stör- och vilseledningsattacker. I [5] gavs rekommendationer avseende vilka detektionsmetoder som bör integreras i militära PNT-system.

Det finns ett flertal olika metoder för att detektera störning och vilseledning, som fungerar olika bra beroende på hur störningen eller vilseledningen genomförs. En schematisk skiss av ett generiskt multisensornavigationssystem bestående av en eller flera GNSS-antenner och -mottagare, stöttande sensorer och en oscillator visas i figur 3.1 [5]. GNSS-mottagarna skickar data (exempelvis pseudoavståndsmätningar, fasmätningar och satellitpositioner) till navigationsdatorn som fusionerar denna information med annan sensorinformation. Detektionsalgoritmerna kan antingen använda data som skickas från GNSS-mottagarna, eller använda data direkt från antennerna. I det senare fallet förutsätts en dedikerad hårdvara för detektionssystemet, medan det eventuellt kan vara möjligt att kravställa önskad detektionsförmåga för det första fallet då tillverkarna även kan utföra detta direkt i mottagaren.

3.1 Detektionsalgoritmer

Ett stort antal detektionsalgoritmer för att upptäcka störning av GNSS-signalerna har föreslagits i den vetenskapliga litteraturen (se exempelvis sammanställningen som ges i [7]). En kombination av olika detektions-algoritmer kan behöva implementeras för att kunna detektera de olika typerna av oavsiktliga interferenser och avsiktliga störsignaler som kan användas vid en attack. Vissa av algoritmerna kan även användas som stöd vid detektion av vilseledningsattacker.

Målet är att detektionsalgoritmerna ska detektera störning tidigt, vid låga störnivåer, innan de påverkar positionsnoggrannheten hos GNSS-mottagaren. På så sätt kan ett multisensornavigationssystem sluta använda informationen från GNSS-mottagaren innan noggrannheten hos det integrerade navigationssystemet har hunnit degraderas. Detta är viktigt eftersom positioner från GNSS-mottagaren ofta används för att estimera olika biasfel i tröghetssensorerna. Felaktigt estimerade biasfel kan orsaka en avsevärt snabbare degradering av positionsnoggrannheten vid ren tröghetsnavigering när GNSS-mottagaren är utstörd.



Figur 3.1: Illustration av ett generiskt navigationssystem med multipla GNSS-mottagare/antenner och stöttande sensorer.

3.1.1 Detektion av störning

Energidetektion är ett effektivt verktyg för att detektera störning vid nivåer som är lägre än vad som krävs för att mottagarens positionsnoggrannhet ska påverkas. Även starka vilseledningssignaler kan detekteras. Utmaningen vid energidetektion är att anpassa tröskelnivån så att även svaga störsignaler kan detekteras med en låg falsklarmssannolikhet i miljöer där bakgrundsbrusnivån kan variera (exempelvis i urbana miljöer).

Energidetektion kan implementeras av mottagartillverkarna direkt men då detta inte är gjort så förutsätter energidetektion idag att en separat hård- och mjukvara integreras i navigeringssystemet. Detta är inte önskvärt i alla situationer och då kan detektionsalgoritmer med sämre möjlighet att tidigt detektera störsignaler appliceras. Vissa mottagare kan idag leverera information om värdet från dess AGC (eng. *Automatic Gain Control*). AGC-värdet kan ses som en enkel, kraftigt kvantiserad, version av energidetektion.

GNSS-mottagarna levererar även data, exempelvis position, hastighet, tid och C/N_0, som ger vissa möjligheter att detektera störning. Analyser av C/N_0-estimaten för de olika satelliterna kan användas för att detektera störning då störningen syftar till att försämra signal-till-brusförhållandet. En utmaning är att ett lågt C/N_0 kan orsakas även av andra orsaker, exempelvis av att signalerna dämpas på grund av byggnader eller vegetation. Detta mått fungerar normalt inte längre när mottagaren är helt utstörd eller av någon annan anledning inte längre kan ge ett positionsestimat.

Analyser av frekvensspektrumet kan även utföras i syfte att upptäcka framförallt smalbandiga interferenser. Detta ger möjlighet att filtrera bort dessa signaler innan energin når själva mottagaren.

3.1.2 Detektion av vilseledning

Vilseledningsattacker kan genomföras på ett antal olika sätt som delvis ger olika påverkan på en mottagare (se exempelvis [17] och [18]). De olika typerna av vilseledning kan inte detekteras med en enkel detektionsmetod utan flera algoritmer behöver kombineras för att ge ett bra skydd mot vilseledning.

Genom att kombinera följande algoritmer (där urvalet påverkas av GNSS-mottagaren och navigationssystemet [5]) med energidetektion kan dock en tillförlitlig detektion av vilseledning av GNSS-signalerna erhållas i många relevanta scenarion.

- Rimlighetskontroll av data från mottagaren, exempelvis hastighet (mot rörelsemodell för plattformen), tid (monotont ökande) och orimligt höga värden på C/N_0.
- Detektionsalgoritmer där positioner för de olika konstellationerna eller frekvenserna (tjänster) beräknas och jämförs sinsemellan. De öppna tjänsterna kan även valideras mot någon av de mer robusta krypterade tjänsterna, antingen kontinuerligt eller vid behov då en annan algoritm indikerar att vilseledning kan pågå.
- Jämförelser med position och/eller hastighet från stöttande sensorer såsom tröghetsnavigeringssystem eller från odometri.
- Distribuerade mottagare som utbyter information, såsom pseudoavståndsmätningar eller NMEA-data, och kombinerar denna information från flera positioner.
- Implementera multipla korrelatorer i mottagarkedjan så den kan estimera om flera versioner av samma signal anländer till mottagarantennen. Detta kan orsakas av en vilseledningsattack (men även flervägsutbredning ger liknande effekt).

Detektionsalgoritmerna ovan är sorterade i bedömd komplexitetsordning.

Avancerade militära gruppantennsystem (CRPA) innehåller en energidetektor och de ger även ofta ett tillförlitligt estimat av stör-till-brusförhållandet (J/N). Det kan även vara möjligt att med gruppantennen estimera riktningarna för varje satellitsignal, och på så sätt detektera om de har en orealistisk geometrisk spridning. Denna metod förutsätter dock en tät integration mellan gruppantennen och mottagaren.

Nya tjänster är under utveckling inom Galileoprogrammet som även omfattar autentisering av signalerna, dvs en kontroll genomförs för att säkerställa att mottagarna inte är utsatta för vilseledning (eng. *Navigation*

Message Authentication, NMA[21]).

3.2 Undertryckning

Störsignaler kan undertryckas med olika tekniker. Smalbandig filtrering genomförs redan i mottagare. Deterministiska (förutsägbara) signaler som kan estimeras kan även filtreras bort på olika sätt. Bredbandig brusstörning kan dock endast undertryckas med hjälp av en gruppantenn (CRPA) som utför spatiell (rumslig) filtrering. Även de flesta typerna av vilseledning som utgör ett hot idag kan undertryckas med en gruppantenn.

En intressant metod för att undertrycka de vanligaste formerna av vilseledning, som använder en ensam sändarantenn, är algoritmer som utnyttjar information från flera samverkande mottagare [24]. Genom att i de olika mottagarna implementera möjligheten att följa flera samtidiga signaler kan de estimera pseudoavstånden till både de autentiska satelliterna och till vilseledningssignalerna. Genom att kombinera denna information är det möjligt att detektera vilka korrelationstoppar (pseudoavstånd) som härrör från de autentiska signalerna och använda dessa vid positionsbestämningen. Mottagarna kan då, under vissa begränsningar, estimera den sanna positionen även då vilseledningssignalerna är starkare än de autentiska satellitsignalerna [24].

3.3 Diskussion

Stora forskningsresurser har lagts på att upptäcka, karaktärisera och även undertrycka interferenser och störning och kunskapen är god gällande hur störattacker bör detekteras. Motsvarande forskningsinsatser gällande algoritmer för detektion av vilseledningsattacker har dock varit mer begränsade men de senaste åren har även metoder för vilseledningsdetektion föreslagits och utvärderats även i öppen litteratur. Det är idag möjligt att implementera tillförlitliga detektionsalgoritmer för störning men vissa typer av vilseledningsattacker kan fortsatt vara svåra att upptäcka i tid. Störskyddssystem i form av gruppantennsystem är effektiva i att både detektera och undertrycka stör- och vilseledningsattacker.

[21] www.gsa.europa.eu/news/assuring-authentication-all

4 Multikonstellationsmottagare som kombinerar signaler från Galileo och GPS

I detta kapitel beskrivs fördelarna med att använda GNSS-mottagare som utnyttjar de öppna signalerna från både GPS och Galileo, samt signaler på flera frekvenser (eng. *Multi-Frequency and Multi-Constellation, MFMC, receiver*). Analysen fokuserar på de möjliga fördelar som kan nås i urbana miljöer där signalerna blockeras av byggnader och där multipla versioner når mottagaren efter att de reflekterats på olika objekt (flervägsutbredning).

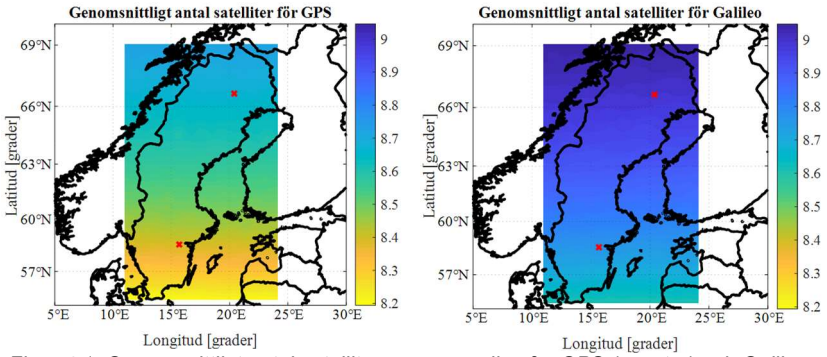
En mottagare som kan använda fler satelliter kan förväntas få en ökad tillgänglighet och noggrannhet i framförallt urbana miljöer. De nya moderniserade öppna GPS-signalerna (L1C och L5) ger en viss ökad noggrannhet i urbana miljöer, delvis på grund av större bandbredd, högre effekt eller en ny modulationstyp.

De teoretiska fördelarna som kan nås genom att nyttja nya typer av signaler och satelliter från både GPS och Galileo innebär dock inte automatiskt att dessa vinster realiseras i befintliga mottagare. I praktiken har framförallt dagens massmarknadsmottagare begränsningar i implementationerna för hur de väljer ut och kombinerar de satellitsignaler som följs och används i positionslösningen. Dessa begränsningar kan idag reducera de fördelar som uppnås med MFMC-mottagare.

4.1 Satellittäckning i Sveriges närområde

I detta avsnitt jämförs antalet satelliter som är synliga på olika positioner i Sverige och över Östersjön för GPS och Galileo. Ett medelvärde beräknades för varje position över en tidsperiod på 24 timmar.

Figur 4.1 visar det genomsnittliga antalet synliga satelliter för grundkonstellationerna av GPS och Galileo, vilka består av 24 satelliter vardera. Det är i genomsnitt fler synliga satelliter över Sverige med Galileo än med GPS. Satellitbanorna för Galileo är planerade för att ge en förbättrad täckning för nordliga breddgrader jämfört med GPS. Detta medför också att GDOP (eng. *Geometric Dilution of Precision*) är lägre för Galileo jämfört med GPS (tabell 4.1). GDOP anger hur satellitgeometrin påverkar noggrannheten i positionsestimering. Ett stort



Figur 4.1: Genomsnittligt antal satelliter som är synliga för GPS (vänster) och Galileo (höger) utvärderat över 24 timmar.

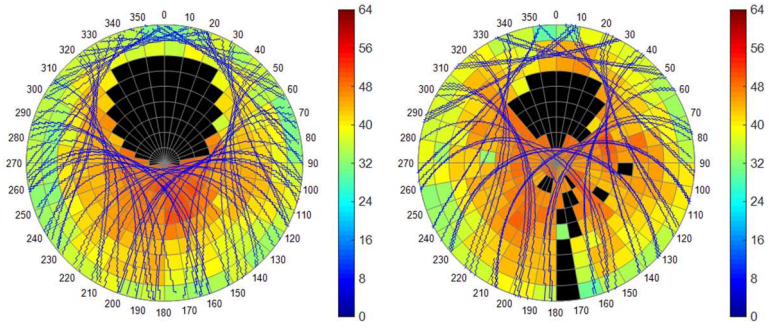
GDOP indikerar en ogynnsam geometri på satelliterna vilket leder till ett ökat positionsfel. Om GPS och Galileo kombineras kommer antalet synliga satelliter närmast dubbleras vilket också gör att GDOP förbättras signifikant (tabell 4.1). En sammanfattning av resultaten visas i tabell 4.1 för två utvalda positioner i Sverige (Linköping och Jokkmokk).

Grundkonstellationen för GPS består av 24 satelliter, men GPS har för närvarande 32 aktiva satelliter i konstellationen. GDOP är lägre för den befintliga konstellationen med 32 satelliter (tabell 4.1). Även Galileo planerar att inom ett par år ha 30 aktiva satelliter men positionerna för dessa extra satelliter är ännu inte kända.

I figur 4.2 illustreras, för GPS (vänster) och Glonass (höger), medelvärdet av uppmätt C/N_0 (i Linköping) från satelliter för olika sektorer av himlen samt spåren av satellitbanorna. Glonass har 23 satelliter och de täcker inte alla sektorer söderut över ett dygn (svartmarkerade sektorer).

Tabell 4.1: Genomsnittligt GDOP och genomsnittligt antal satelliter över 24 timmar för två positioner utvärderat för GPS med 24 respektive 32 satelliter i konstellationen, samt för Galileo med 24 satelliter i konstellationen. Antal satelliter i konstellationerna anges inom parentes.

Konstellation	N 58,5659° E 15,6751° (nära Linköping)		N 66,6383° E 20,3926° (nära Jokkmokk)	
	Genomsnittligt GDOP	Genomsnittligt antal satelliter	Genomsnittligt GDOP	Genomsnittligt antal satelliter
GPS (24)	2,00	8,39	2,19	8,67
Galileo (24)	1,93	8,76	2,02	8,99
GPS (24) + Galileo (24)	1,46	17,15	1,56	17,66
GPS (32)	1,75	11,24	1,87	11,57



Figur 4.2: Färgkodade medelvärden av C/No i varje sektor i dB samt spåren av satellitbanorna (endast hela grader) för GPS (vänster) och Glonass (höger). Uppmätt under ett dygn i Linköping.

Figur 4.2 visar även att GPS-banorna vänder några grader söder om Linköping medan Glonass vänder ca 10 grader norrut. GPS ger en delvis sämre satellitgeometri över delar av Sverige då det finns delar av himlen som satellitbanorna inte täcker. Resultatet från satellitgeometrin för GPS blir dels en något sämre positionsnoggrannhet men det ger även en ökad risk för att fler satelliter blockeras av byggnader om mottagaren befinner sig norr om en byggnad jämfört med om mottagaren är söder om denna.

4.2 Prestanda för olika GNSS-signaler

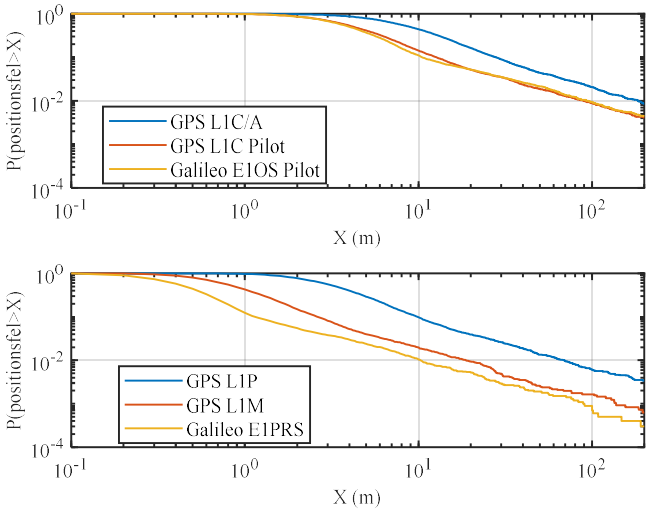
I detta avsnitt beskrivs resultatet från simuleringar av hur en GNSS-mottagare påverkas av flervägsutbredning för ett antal olika signaler från GPS- och Galileo-satelliter. Syftet med simuleringarna är att jämföra prestanda med avseende på val av signaler och kombination av konstellationer för en multi-GNSS-mottagare i ett scenario med flervägsutbredning. Resultaten redovisas mer utförligt i [4].

De nominella grundkonstellationerna (med 24 satelliter) för GPS- och Galileo-systemen har antagits och beräkningen av satellitpositionerna har gjorts för en slumpmässig tid. GNSS-mottagaren har antagits befinna sig på en slumpmässig position inom ett rektangulärt område som täcker Sverige och Östersjön (figur 4.1). På denna position har det antagits att det finns en oändligt lång gata i en slumpmässig riktning flankerad av byggnader på båda sidor (*urban canyon*). Mottagaren antas befinna sig mitt i gatan som är 30 meter bred och byggnaderna antas vara 10 meter höga. Byggnaderna blockerar satelliter med låg elevation i vissa riktningar och dessa inkluderas inte i positionslösningen. Dessutom tas satelliter med elevationsvinkel under fem grader inte med i positions-lösningen. Pseudoavstånden till de återstående satelliterna får en

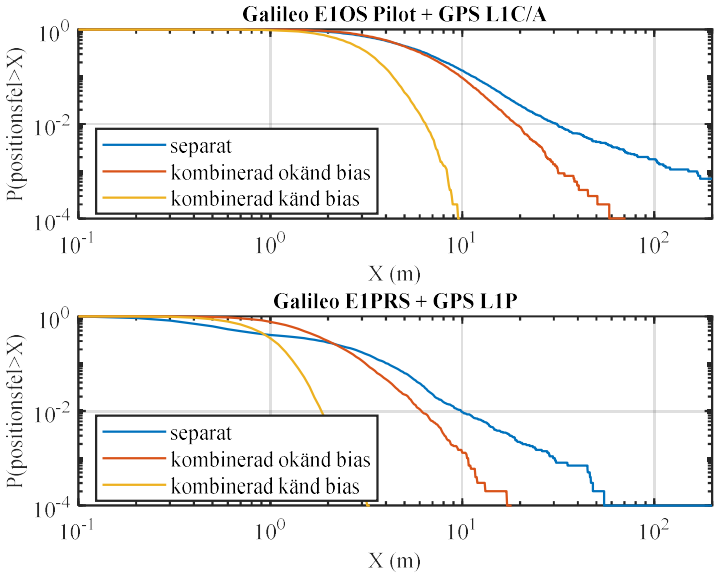
flervägsutbredningskomponent med slumpmässig fördröjning (motsvarande upp till 30 m), med 6 dB lägre effekt än direktkomponenten.

Det positionsfel som orsakas av flervägsutbredning beror både på hur många satelliter som är tillgängliga och hur dessa är utspridda geometriskt på himlen. Om fler än en GNSS-konstellation används finns olika sätt att kombinera dessa. Den enklaste lösningen innebär att en position beräknas *separat* för de två systemen och sedan kombineras. I de resultat som visas nedan väljs den lösning som har mest fördelaktig satellitgeometri (lägst GDOP) [4]. De uppmätta pseudoavstånden för GPS- och Galileosatelliterna kan även *kombineras* i en gemensam lösning, där den relativa klockdriften mellan de två systemen antingen är okänd eller känd.

I figur 4.3 visas sannolikheten att positionsfelet orsakat av flervägsutbredning överstiger ett givet värde för olika GPS- och Galileosignaler. De moderniserade GPS-signalerna, och de nya Galileosignalerna, ger högre noggrannhet i jämförelse med de äldre signalerna. I figur 4.4 jämförs positionsfelet för de tre olika kombinationsmetoderna, för den civila GPS L1 C/A-signalen och Galileo E1 OS (eng. *Open Service*) signalen. En signifikant minskning av positionsfelet kan teoretiskt sett uppnås genom att kombinera signalerna från GPS och Galileo. Figur 4.4 visar att risken för stora positionsfel är lägre då GPS L1C/A och Galileo E1OS



Figur 4.3: Sannolikheten för att positionsfelet orsakat av flervägsutbredning överstiger ett givet värde för olika GPS- och Galileosignaler. Den nedre figuren jämför prestanda för de krypterade signalerna.



Figur 4.4: Sannolikheten för att positionsfelet orsakat av flervägsutbredning överstiger ett givet värde för olika sätt att kombinera GPS- och Galileosignalerna.

signalerna kombineras jämfört med de positionsfel som erhålls för den signal som enskilt ger bäst prestanda (Galileo E1 PRS i figur 4.3). Genom att i en mottagare använda pseudoavståndsmätningar från både Galileo PRS och GPS M-kod kan teoretiskt en hög robusthet mot flervägsutbredning erhållas. En sådan kombinerad mottagare kan troligen realiseras i framtiden men den förutsätter sannolikt att två separata säkerhetsmoduler och krypton används [18].

5 Samverkande navigering

Samverkande navigering kan genomföras på ett stort antal sätt, men grunden är att flera samverkande plattformar utbyter information sinsemellan i syfte att förbättra sin egen och de andras navigeringssystem (position och orientering). Samverkande navigering är ett viktigt komplement för framförallt mindre plattformar som under en lång tid framöver förväntas ha problem att med plattformens eget navigerings-system kunna vidmakthålla en hög positionsnoggrannhet över en längre tid i GNSS-störda operationer.

Exempel på hur samverkan kan genomföras inkluderar:

- Uppbyggnad av gemensamma databaser av exempelvis landmärken eller kartor.
- Radiobaserad avståndsmätning mellan soldater eller plattformar och utbyte av respektive navigationssystems positions- och orienteringsestimat.
- UAV-baserad (eng. *Unmanned Aerial Vehicle*) lokalisering av markplattformar och efterföljande uppdateringar av de enskilda markplattformarnas navigeringslösningar.

5.1 Samverkan mellan luft- och markplattformar

Flygande och markplattformar kan samverka för att förbättra markplattformarnas positionsestimat. Markplattformarna antas vara utrustade med plattformsbundna navigeringssystem (exempelvis tröghetsnavigering stöttad med odometri) som estimerar plattformarnas position och orientering, samt de tillhörande osäkerheterna. I GNSS-störda miljöer växer positionsfelet för dessa system med tiden. De flygande plattformarna estimerar sin egen position och orientering med bildalstrande sensorer (exempelvis genom matchning av bilder mot en referenskarta) och de har även förmåga att detektera, följa och lokalisera markplattformarna (med tillhörande osäkerhetsmått). Genom att skicka dessa positionsestimat till markplattformarna kan deras positions-noggrannhet förbättras.

5.1.1 UAV-positionering

Som komplement till GNSS-baserad positionering utvecklar FOI ett kamerabaserat system för positionsbestämning av UAV. UAV:n är försedd med en kamera som hålls stabiliserad i lodtittande riktning med hjälp av en gimbal. Bilder från kameran jämförs kontinuerligt med en

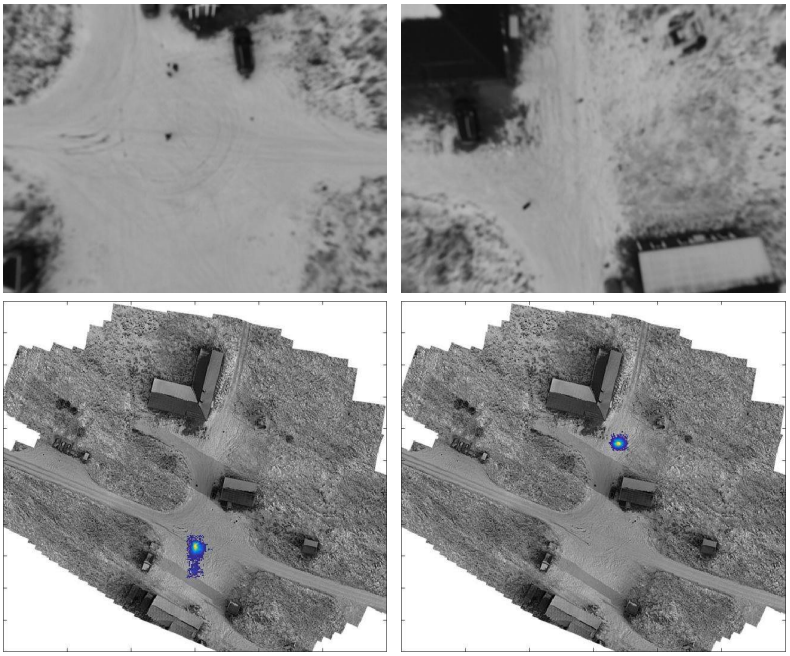
georefererad karta av operationsområdet. De delar av kartan, som liknar den aktuella bilden, utgör möjliga hypoteser om UAV:ns position. I många miljöer ger detta dock ingen entydig positionslösning för en lågflygande UAV då flera delar av referensbilden kan likna varandra.

För att erhålla en entydig lösning mäts även UAV:ns hastighet genom analys av bildströmmen från kameran. För varje bild beräknas pixlarnas förflyttning jämfört med föregående bild (s.k. optiskt flöde). Efter korrigering för höjd (som estimeras med hjälp av en barometer) och riktning (som estimeras med hjälp av en elektronisk kompass) kan UAV:ns hastighet estimeras. Hastighetsestimatet kombineras med resultat från bildmatchningen i ett partikelfilter, där varje partikel representerar en hypotes om UAV:ns position. Genom att väga samman de olika partiklarna fås ett estimat av UAV:ns position och ett mått på estimatets osäkerhet. Algoritmen beskrivs mer detaljerat i [19].

Metoden har utvärderats i olika miljöer och visat sig fungera bra under två förutsättningar: att det finns tillräckligt mycket variation i miljön, och att referensbilden är tillräckligt lik verkligheten. Det första villkoret innebär att metoden oftast fungerar bra i exempelvis urbana miljöer med byggnader eller vägar, men att positionering över skog, fält och framför allt vatten fungerar betydligt sämre. Det andra villkoret innebär att referensbilden måste uppdateras om det skett betydande förändringar sedan den samlades in. Sådana förändringar kan till exempel vara nybyggda hus eller vägar, eller snötäcke som tillkommit eller försvunnit.

Figur 5.1 visar två exempel från ett försök med flygning på ganska låg höjd (ca 20 - 25 meter) med en multirotor-UAV över gles bebyggelse. På grund av den låga flyghöjden syns endast en liten del av marken i kamerabilderna. I det första exemplet saknar en stor del av bilden i stort sett visuell struktur och osäkerheten i positionsestimatet blir därför stor. I det andra exemplet, några sekunder senare under samma försök, ser kameran tydliga strukturer i form av en byggnad. Positionsosäkerheten blir då låg. Det är därför viktigt att även andra kompletterande sensorer, exempelvis tröghetssensorer, integreras för att hantera tillfällen där det kamerabaserade systemet ger begränsad information. Ett annat alternativ är att dess flygrutt (även höjd) planeras i förväg utifrån kartinformationen så att den undviker att flyga över områden med begränsad visuell struktur.

Positioneringsalgoritmen fungerar i realtid på en Nvidia Jetson, som är en liten dator som med lätthet kan bäras av även en liten UAV. I nuläget förutsätts att en uppdaterad referensbild finns tillgänglig. I de försök som genomförts har bilder från Google Earth eller motsvarande tjänster använts, alternativt så har egna referensbilder genererats genom att samla



Figur 5.1: Övre raden: bilder från kameran. Undre raden: referensbild med överlagrad fördelning av positionshypoteser. Till vänster visas ett fall då bilden har lite struktur och osäkerheten därför är stor. Till höger visas ett fall då tydliga strukturer i bilden medför en lägre osäkerhet.

in flygbilder vartefter ortografiska foton har genererats med hjälp av fotogrammetri.

5.1.2 Detektion och följning av rörliga objekt

Under 2018 påbörjades utveckling av en metod för att, med samma kamera som används för positionering, även detektera och följa rörliga mål [20]. Därefter har algoritmen förenklats och gjorts mer robust och beräkningseffektiv[22].

Algoritmen detekterar och följer mål enligt följande:

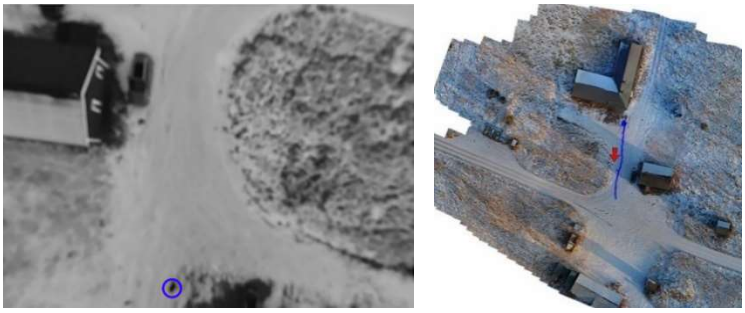
[22] Metoderna för bildbaserad UAV-positionering samt detektion och följning av rörliga objekt har utvecklats i samarbete med FoT-projektet *Autonom övervakning med samverkande sensorer* (FoT-område Sensorer & signaturanpassning).

1) Beräkna det optiska flödet mellan föregående och aktuell bild från kameran. Det optiska flödet beskriver hur de enskilda pixlarna förflyttats mellan två bilder.
2) Hitta områden där det optiska flödet skiljer sig från omgivningen. Avvikelserna i optiskt flöde orsakas av rörliga plattformar på marken men även av stationära objekt som master, träd, tak på byggnader, etc.
3) Bland de områden där villkoret i (2) uppfylls, hitta områden där även bildens intensitet avviker från omgivningen. Välj ut de områden där intensitetsavvikelsens storlek matchar den förväntade storleken hos de objekt som ska detekteras. Detta steg sorterar bort många av de falska detektioner som fås i steg (2).
4) Använd den estimerade positionen och orienteringen för UAV:n, samt markplattformarnas positioner i bilden, till att lokalisera markplattformarna. Detta ger objektens positioner i världskoordinater. Detektionerna från en sekvens av bilder associeras därefter till varandra så att målspår, som beskriver hur respektive objekt rör sig, kan genereras.
5) Filtrera bort målspår som inte förflyttat sig tillräckligt långt från sina startpunkter. Därmed kan kvarvarande falska rörelsedetektioner som orsakas av uppstickande stationära objekt elimineras.

En begränsning med denna metod är att den endast detekterar objekt som rör sig tillräckligt långt. Vid en flyghöjd på ca 50 meter över typisk bebyggelse behöver ett objekt förflytta sig ungefär tre meter för att med god marginal kunna skiljas från en falsk detektion. En fördel med metoden är att även små objekt (som bara täcker några pixlar i kamerabilderna) kan detekteras och följas.

Figur 5.2 visar ett exempel på följningsresultat, från samma fältförsök som beskrivs i det föregående avsnittet. Till vänster visas en bild från kameran. En person har markerats manuellt för ökad tydlighet. Till höger visas UAV:ns estimerade position och riktning (röd pil) samt ett målspår (blå linje med en cirkel vid målets aktuella position), överlagrade på referensbilden över området. Även detektion och följning kan utföras i realtid på en Nvidia Jetson som kan bäras ombord på UAV:n.

För att underlätta utveckling och utvärdering av metoden, har en simuleringsmiljö tagits fram. Simuleringen använder *Microsoft AirSim*, ett verktyg för simulering av UAV-flygning och generering av sensordata från UAV-burna avbildande sensorer. *AirSim* använder sig i sin tur av spelmotorn *Unreal Engine* för generering av realistisk grafik. I simulatorn har en modell av strid i bebyggelse (SIB) anläggningen Spång, i Kvarn, lagts in. Fasta rörelsebanor för obemannade markfordon (UGV) har



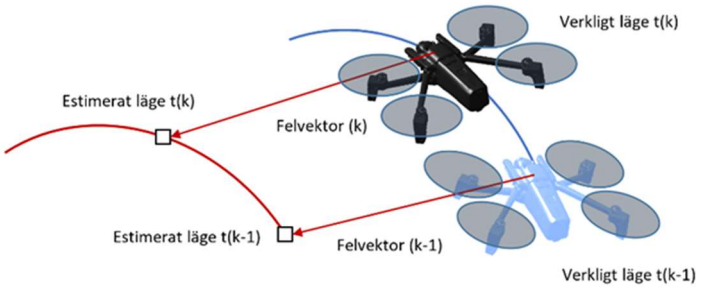
Figur 5.2: Vänster: Bild från kameran med en person markerad. Höger: Målspår som visar personens rörelse.

Figur 5.3: Simulerad bild från en UAV-monterad kamera, med markering för detekterad UGV.

definierats, och flygning över området simulerats. Figur 5.3 visar en simulerad kamerabild där en detekterad UGV markerats med cirklar.

5.1.3 Samverkande navigering

När en markplattform får ett estimat av sitt målspår från UAV:n behöver därefter positioneringssystemet uppdateras via sensorfusion med navigeringslösningen från det plattformsburna navigeringssystemet. Ett problem som behöver hanteras i denna sensorfusion är bias i felet på informationen från UAV:n. I figur 5.4 illustreras hur ett fel i dödräkning kvarstår mellan två mätpositioner. Detta fel är inte, i statistisk mening, vitt brus och om det hanteras som vitt brus kommer noggrannheten i lösningen överskattas. I nuläget rapporteras position, identitet och osäkerhet i mätning respektive egen positionsosäkerhet från UAV:n. Markfarkosten har ett eget navigeringssystem bestående av dödräkning (t.ex. baserat på tröghetsnavigering med enkla accelerometrar och gyron kombinerat med odometri) samt i förekommande fall stöttning från lokala landmärken via en algoritm benämnd SAM (eng. S*moothing and Mapping*) där mjukvarupaketet GTSAM används (som utvecklats av Georgia Tech [21]).

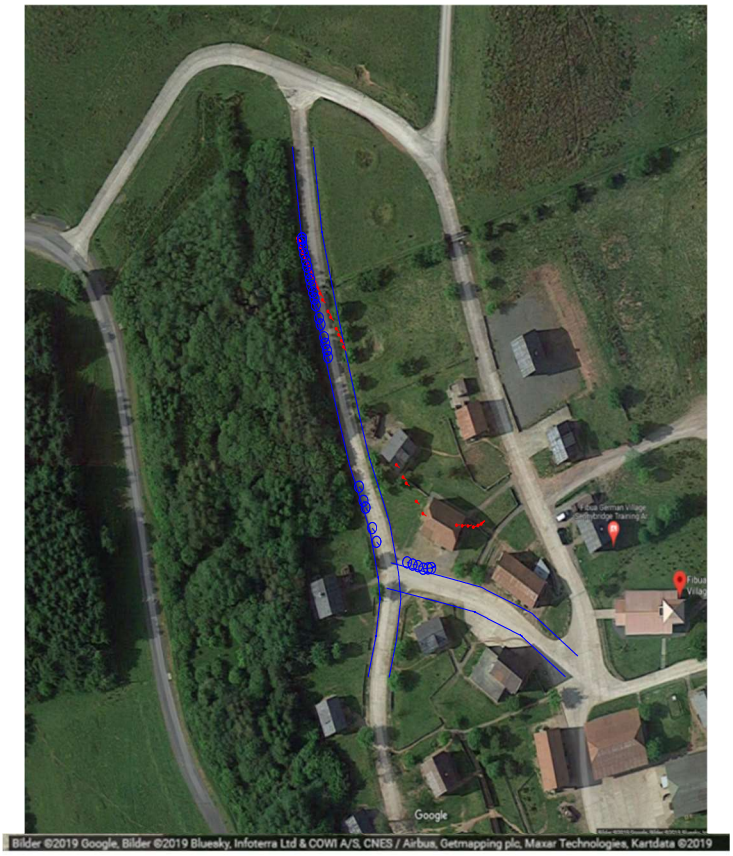


Figur 5.4: Illustration över hur fel i navigering kan kvarstå över tid. Felvektorn vid tid t(k) är mycket lik den vid tid t(k-1).

De två positionerna kan nu fusioneras. I nuläget används en metod som är robust mot okända korrelationer, benämnd ICI-algoritmen (eng. *Inverse Covariance Intersection*). Algoritmen genererar en överskattning av den korrelerade informationen mellan mätningarna och kompenserar för densamma [22]. Genom att en överskattning används kommer algoritmen inte att underskatta sin osäkerhet till kostnaden av ett konservativt estimat. I figur 5.5 illustreras resultat från försök i NATO gruppen SET-229 [2] där ett fotmonterat tröghetsnavigeringssystem [23] använts med stöttning från UAV. Personen har rört sig på höger sida av vägen för att sedan i korsningen gå över på vänster sida framför huset. Personens position (representerad av röda punkter) hade i dessa tester ett ovanligt stort fel men detta har till stor del kompenserats av informationen som tillhandahålls från UAV:n.

5.2 Värdering av samverkande navigering

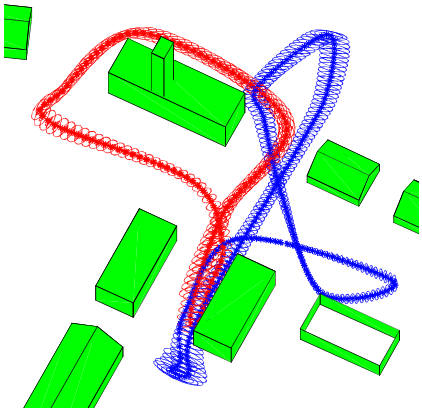
I de föregående avsnitten visades exempel från fältförsök med samverkande navigering utifrån målföljningsdata från en UAV med kartstöttad navigering. Ett simulerat scenario har även använts för att analysera vilka fördelar som olika samverkande navigeringstekniker kan förväntas ge. Scenariot avser demonstrera de grundläggande principerna för samverkande navigering snarare än att demonstrera ett specifikt system. Grundförutsättningen i scenariot, som beskrivs i figur 5.6, är att två fordon navigerar med dödräkning där vinkeldriften är den dominerande felkällan. Driften i vinkelestimatet har överdrivits i analyserna av visualiseringsskäl.



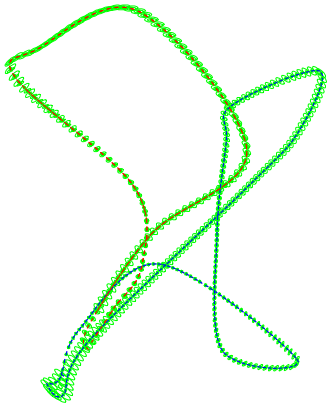
Figur 5.5: Stöttning av navigering med målspårsestimat från UAV. Experiment genomfört vid data insamling/generalrepetition inför demonstration i NATO SET-229. De röda prickarna representerar fotmonterad tröghetsnavigering utan stöttning. Blå cirklar representerar resultat efter stöttning. (ortofoto bakgrund © Google & Bluesky)

GTSAM användes först till att analysera osäkerheten då plattformarna samverkade och genomförde avståndsmätningar då plattformarna hade fri sikt till varandra (figur 5.7). Denna analys simulerar samverkan genom avståndsmätningar som utförs med tidsmätande impulsradio (eng. *Ultra-Wideband, UWB*) [23]. I figur 5.8 jämförs den största osäkerheten (största axeln i osäkerhetsellipsen) med och utan samverkan. Trots att noggrannheten i avståndsmätningarna är hög (5cm) så ger samverkan endast ungefär en halvering av positionsosäkerheten.

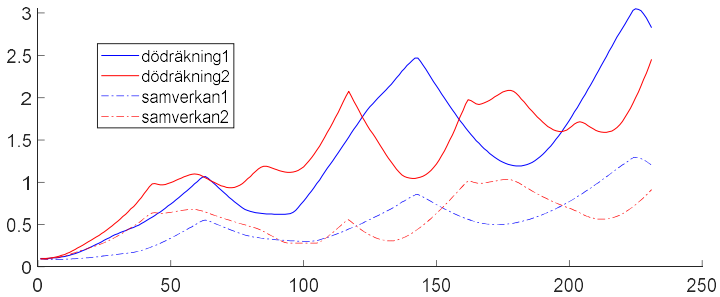
I samma scenario, men där den ena plattformen istället har en avsevärt högre positionsosäkerhet, kan den plattform som har en hög osäkerhet nästan uppnå den bättre plattformens prestanda (figur 5.9). Den relativa prestandaförbättringen blir avsevärt högre för denna plattform.



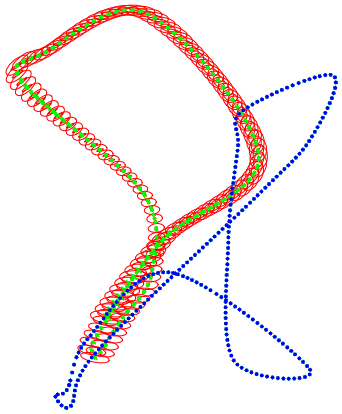
Figur 5.6: Simulerade banor med dödräkningsfelets osäkerhet illustrerat som ellipser motsvarande 68% sannolikhet (vilket innebär att de estimerade positionerna befinner sig innanför ellipsen ungefär två gånger av tre). Den röda banan hinner mer än ett varv under scenariot så det finns dubbla ellipser på en del av banan.



Figur 5.7: Osäkerhet efter samverkan via inbördes avståndsmätningar.

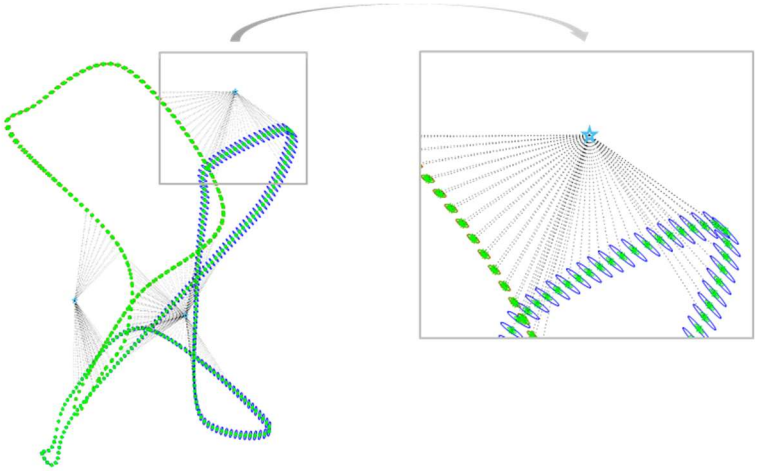


Figur 5.8: Simulerad osäkerhet för de två dödräknande navigationssystemen före och efter samverkan (avståndsmätningar och utbyte av positioner och osäkerhetsestimat) i ett scenario där de två plattformarna har ungefär lika stor positionsosäkerhet.

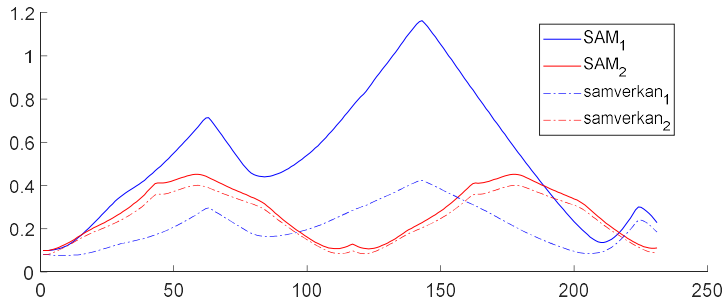


Figur 5.9: Samverkande navigering genom avståndsestimering där plattform 2 har en betydligt lägre osäkerhet (blå ellipser). Osäkerheten efter samverkande navigering visas i grönt medan den ursprungliga osäkerheten utan samverkan visas i rött.

Samverkande navigering kan även genomföras genom att utbyta information om stationära landmärken som kan estimeras av båda plattformarna. Sensorerna antas i denna analys ha en begränsad räckvidd så att landmärkena endast kan ses under kortare delar av trajektorian, vilket illustreras i figur 5.10 med prickade linjer till landmärket, men där avstånds- och riktningsnoggrannheten är hög. Ett exempel på en sensor med sådana egenskaper är en LiDAR (eng. *Light Detection and Ranging*). I denna analys användes SAM på mätningar av punktlandmärken (simulerade träd) för att förbättra dödräkningssystemets noggrannhet.



Figur 5.10: Scenario med delning av landmärken (markerade med blå stjärnor). Till höger visas en uppförstorad bild av osäkerheterna i den del av trajektorian där osäkerheterna är som störst. De gröna ellipserna visar osäkerheterna vid samverkan.



Figur 5.11: Största osäkerheten i position för enskild SAM på inmätta landmärken samt efter samverkande navigering med delade landmärken.

Plattformarna navigerar antingen enskilt eller gemensamt där allt data samlas i en helhetslösning. Med enbart tre träd erhålls dels en lägre positionsosäkerhet för de enskilda plattformarna, men framförallt en väsentlig förbättring för den plattform som har den sämsta mätgeometrin (figur 5.10 och figur 5.11).

5.3 Diskussion

Ovanstående exempel visar på typiska resultat för samverkande navigeringsalgoritmer. Vid användningen av inbördes avståndsmätningar, och utbyte av positioner och tillhörande positionsosäkerheter, i scenarion där plattformarna har ungefär lika hög positionsosäkerhet kan samverkande navigeringstekniker leda till en halvering av positionsosäkerheten. Vinsten vid samverkande navigering är högst när en av plattformarna har en hög positionsnoggrannhet och den andra plattformen har ett sämre positionsestimat.

Genom att utbyta information mellan fler än två plattformar kan positionsnoggrannheten förbättras ytterligare. Samverkande navigering bedöms vara en potentiellt viktig teknik för främst mindre plattformar i GNSS-störda miljöer, framförallt om de även har möjlighet att (åtminstone sporadiskt) utbyta information med en plattform som har en hög positionsnoggrannhet. Ett exempelscenario kan vara att ett fordon är utrustat med avancerade störundertryckningssystem (gruppantenner) som medger att den har tillgång till GNSS-positionsestimat. Andra plattformar, vars GNSS-mottagare är utstörda, kan då fortsatt erhålla en hög positionsnoggrannhet genom samverkande navigeringstekniker som beskrevs ovan. En specifik positionsnoggrannhet kan dock inte garanteras vid samverkande navigering då det förväntas ske på opportunistisk basis. Samverkan genomförs när möjligheten uppenbarar sig, exempelvis vid frisiktsförhållande till en annan plattform då en noggrann avståndsestimering kan genomföras.

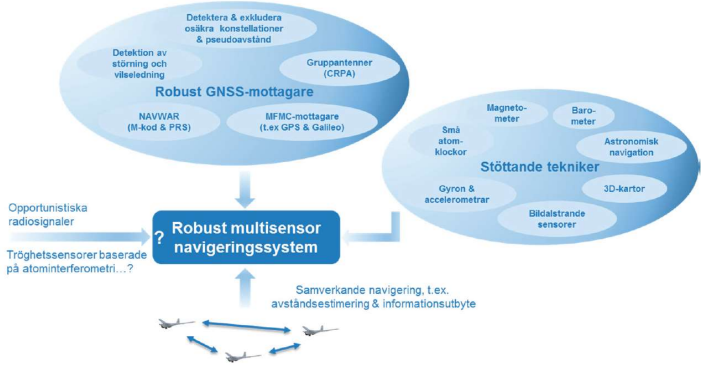
6 Rekommendationer

I detta kapitel ges generella rekommendationer för hur framtida militära PNT-system bör implementeras. Fokus i arbetet har varit mot små och medelstora plattformar, både bemannade och obemannade, som ofta har begränsningar i storlek, vikt, effektförbrukning och kostnad.

6.1 Multisensorsystem

Sensorutvecklingen har det senaste årtiondet varit snabb och sensorernas prestanda har förbättrats samtidigt som kostnad och storlek för dessa har reducerats kraftigt. Även små plattformar kan utrustas med multisensorsystem för att ge en högre noggrannhet men framförallt ger de en viss förmåga att operera i GNSS-störda miljöer.

I [25] rekommenderas att utvecklingen av framtida militära navigeringssystem för obemannade plattformar fokuseras mot multisensorsystem bestående av en robust GNSS-mottagare som kompletteras med stöttande sensorer och samverkande navigering för att nå en hög tillförlitlighet i GNSS-störda miljöer (figur 7.1).



Figur 7.1: Illustration av multisensornavigeringssystem baserat på en robust GNSS-mottagare som stöttas med ytterligare sensor för att nå en hög tillförlitlighet och noggrannhet.

6.2 GNSS-mottagare

En robust GNSS-mottagare bör i militära system använda sig av:

- Krypterade signaler, såsom M-kod och/eller PRS.
- Störskyddssystem i form av adaptiva gruppantenner (typ CRPA).

- Öppna signaler från flera GNSS-konstellationer och frekvenser.
- Algoritmer för detektion av störning och vilseledning, samt detektion av otillförlitliga pseudoavståndsmätningar eller konstellationer.

6.2.1 Gruppantenner

Gruppantenner är en mogen teknik som ger en markant förbättring av robustheten för en GNSS-mottagare. De bör integreras på alla plattformar där det är praktiskt möjligt. Små gruppantenner har de senaste åren utvecklats avsedda bland annat för integration på markfordon och taktiska UAV:er.

6.2.2 Detektion av störning och vilseledning

Algoritmer för detektion av störning och vilseledning bör inkluderas i alla framtida mottagare [5]. Dessa algoritmer kan vara implementerade direkt i mottagaren, eller implementeras separat i PNT-systemet. Algoritmer som implementerats direkt i en mottagare, såsom i kommande M-kods- eller PRS-mottagare, behöver utvärderas av oberoende part inför en upphandling för att förstå begränsningarna med de algoritmer som leverantörerna valt att implementera.

I de fall en gruppantenn integreras i PNT-systemet är det viktigt att även information från denna inkluderas vid detektion då den kan ge tillförlitliga estimat av störning och vilseledning.

6.2.3 Kombinationer av GPS och Galileo

Försvarsmakten bör i framtida PNT-system använda GNSS-mottagare som använder signaler från både Galileo och GPS. Glonass och Beidou bör anses som mindre säkra då betydligt mindre är känt om hur dessa styrs [6]. Detta innebär däremot inte att användningen av Glonass och Beidou helt ska uteslutas. Det viktiga vid designen av en GNSS-mottagare är att ha kontroll över vilka signaler som mottagaren använder i positionsberäkningen och att endast använda signaler som mottagaren eller PNT-systemet bedömer vara tillförlitliga. En integritetskontroll måste alltså finnas, av olika GNSS men även av individuella pseudoavståndsmätningar. Sammanfattningsvis kan följande rekommendationer ges:

- Både Galileo och GPS bör användas.
- Glonass och Beidou kan användas om tillförlitlig integritets-kontroll finns för att avgöra rimligheten i pseudoavstånds-mätningarna.

- I situationer där GPS och Galileo är utstört men Glonass fortsatt fungerar bör mottagarna ha möjlighet att använda Glonass som ett reservalternativ.

6.3 Samverkande navigering

Samverkande navigeringsmetoder har en stor potential och de är intressanta för framtida militära PNT-system. Fortsatta FoU-aktiviteter behöver dock genomföras i syfte att utveckla och utvärdera konkreta förslag till hur samverkande navigering bör införas i framtida militära PNT-system, kopplat till vilka möjligheter som olika plattformars PNT-system medger. Det är även viktigt att studera möjligheterna att utveckla strategier för, och implementera, samverkansstrategier mellan heterogena PNT-system då det förväntas medge lägre kostnader för de enskilda plattformarnas PNT-system.

7 Slutsatser

GNSS-området är under snabb utveckling där nya konstellationer och tjänster införs. GNSS-mottagare kommer fortsatt att utgöra en viktig del av framtida PNT-system. De har dock fortsatt ett antal sårbarheter, främst gentemot avsiktlig störning och vilseledning, som medför att nya kompletterande algoritmer och sensorer bör integreras. I framtida konfliktsituationer kommer GNSS-signalerna att utsättas för avancerade stör- och vilseledningsattacker. Liknande incidenter kan även komma att genomföras i fredstid för att störa Försvarsmaktens övningsverksamhet.

Grundkonstellationen för Galileo har en något bättre täckning över Sverige än motsvarande konstellation för GPS. När Galileo är fullt utbyggt förväntas även den reella konstellationen för Galileo ge en något bättre satellitgeometri. Skillnaden är dock mycket liten i normala fall men i urbana miljöer kan det eventuellt få en viss påverkan. Den stora vinsten fås istället genom att använda satelliter från både GPS och Galileo i mottagaren. De nya GNSS-signalerna är mindre känsliga mot flervägsutbredning. Genom att använda satelliter från både GPS och Galileo blir fler satelliter tillgängliga. Det har störst påverkan i urbana miljöer med kraftig flervägsutbredning, där ett enskilt GNSS inte alltid kan ge en tillförlitlig positionsmätning. Till de fördelar som har noterats med en multikonstellations- och multifrekvensmottagare jämfört med en traditionell GPS-mottagare hör framförallt bättre tillgänglighet i stadsmiljö då antalet tillgängliga satelliter är betydligt högre. I en militär tillämpning där robusthetskravet är drivande är systemdiversiteten och till viss del ökad tålighet mot stör- och vilseledningsattacker (som uppnås främst genom fler signaler på olika frekvenser) tilltalande. Komplexiteten och därmed kostnaden för en MFMC-mottagare kommer att vara högre, främst p.g.a. det ökade antalet tillgängliga frekvensband, men fördelarna som kan uppnås är betydande.

Energidetektion är en effektiv metod för att tidigt detektera störning av GNSS-signalerna. Olika typer av vilseledning kan inte detekteras med en enkel detektionsmetod utan flera algoritmer behöver kombineras för att ge ett bra skydd mot vilseledning. Ju högre skyddsnivå som krävs, desto högre komplexitet får detektionsmetoderna [17]. För att erhålla högsta skyddsnivå behöver GNSS-mottagaren utrustas med en gruppantenn eller flera distribuerade antenner. Vilseledningsattacker kan även undertryckas om flera mottagare, som alla har möjlighet att följa multipla versioner av satellitsignalerna, kan utbyta information sinsemellan [24].

De studier och experimentella utvärderingar som genomförts indikerar att samverkande navigering har potential att ge betydande fördelar för framförallt PNT-system på mindre plattformar som opererar i GNSS-

störda miljöer. Samverkande navigering är ett intressant framtidsområde och det finns ett stort antal metoder som kan användas för att åstadkomma samverkan mellan plattformar. Möjligheterna beror även på vilka sensorer som plattformarnas PNT-system använder. Avancerade plattformar med bra PNT-system kan genom samverkande navigering ge betydande förbättringar för mindre plattformar som har mer begränsade sensorsystem.

Referenser

[1] J. Rantakokko, F. Näsström, J. Nygårds, R. Woltjer och K. Bengtsson, *Tekniköversikt autonoma och obemannade system - Del 2: Markstriden*, Totalförsvarets Forskningsinstitut, FOI-R--4901--SE, december 2019.

[2] J. Rantakokko, J. Nygårds, J. Rydell, M. Alexandersson och P. Andersson, *Tekniker för navigering i urbana och störda GNSS miljöer - redovisning av genomförd demonstration och beskrivningar av utvecklade demonstrationssystem*, FOI Memo 6958, december 2019.

[3] J. Rantakokko och F. Marsten-Eklöf, *En beskrivning av två fall av störning och vilseledning som genomförts mot GPS under 2017*, FOI MEMO 6260, december 2017.

[4] N. Stenberg, E. Axell och T. Lindgren, *Analys av multi-GNSS med GPS och Galileo under påverkan av flervägsutbredning*, Totalförsvarets Forskningsinstitut, FOI-R--4892--SE-0.0, januari 2020.

[5] T. Lindgren, P. Eliardsson, E. Axell och P. Johansson, *Rekommendationer avseende detektion av störning och vilseledning av GNSS*, Totalförsvarets Forskningsinstitut, FOI-R--4694--SE, december 2018.

[6] T. Lindgren och F. M. Eklöf, *Multi-GNSS - översikt, implementationsaspekter och utmaningar*, FOI-D--0782--SE, 2017.

[7] E. Axell och T. Lindgren, *Multiantenntekniker för detektion av vilseledningsattack mot GNSS*, FOI-R--4500--SE, 2017.

[8] *Above us only stars – Exposing GPS spoofing in Russia and Syria*, C4ADS rapport, 2019.

[9] H. Lied, *GPS freaking out? Maybe you're too close to Putin*. NRKbeta, 2017-09-18. (https://nrkbeta.no/2017/09/18/gps-freaking-out-maybe-youre-too-close-to-putin/)

[10] S. Linder och M. Alexandersson, *Användning av störsändning i konflikten i Ukraina - en sammanställning från öppna källor*, FOI MEMO 5625, januari 2016.

[11] M.J. Murrian, L. Narula och T.E. Humphreys, "Characterizing Terrestrial GNSS Interference from Low Earth Orbit", *ION GNSS+*, Miami, FL, september 2019.

[12] *Vikten av var och när – Samhället beroende av korrekt tids- och positionsangivelse*, MSB778, november 2014.

[13] *Satellite-derived time and position: A study of critical dependencies*, Government Office for Science, UK, 2018.

[14] A. C. O´Connor et al. *Economic benefits of the Global Positioning System (GPS) – Final report*, RTI International, June 2019. (www.rti.org/sites/default/files/gps_finalreport.pdf)

[15] M. Alexandersson, F. Marsten Eklöf och B. Gabrielsson, *Framtida nationell användning av Galileo/PRS*, MSB & FOI, MSB1290, oktober 2018.

[16] N. Davies, A. Evans, M. Jones, M. Macleod, R. Bowden, D. Hagan, H. Mayoh, D. Mathews, ”Towards Dual Mode Secure Navigation Using the Galileo Public Regulated Service (PRS) and PGS Precise Positioning Service (PPS)”, *ION GNSS+,* Portland, OR, september 2016.

[17] M. L. Psiaki och T. E. Humphreys, ”GNSS spoofing and detection”, *Proceedings of the IEEE*, juni 2016.

[18] J. Rantakokko, F. Marsten-Eklöf, T. Lindgren och J. Nygårds, *Robusta positioneringssystem – Slutrapport*. FOI-RH--1792--SE, april 2017.

[19] J. Rydell, E. Bilock och M. Tulldahl, ”Computationally Efficient Vision-based UAV Positioning”, *ION International Technical Meeting (ITM)*, Reston, Virginia, januari 2019.

[20] J. Rantakokko och J. Rydell, *Robust navigering för obemannade farkoster – statusuppdatering*, Totalförsvarets forskningsinstitut, FOI Memo 6593, december 2018.

[21] F. Dellaert, *Factor graphs and GTSAM: A hands-on introduction*, 2012. (https://gtsam.org/tutorials/intro.html)

[22] B. Noack, J. Sijs, M. Reinhardt och U. D. Hanebeck, ”Decentralized data fusion with inverse covariance intersection”, *Automatica*, vol. 79, pp. 35-41, 2017.

[23] J. O. Nilsson, J. Rantakokko, P. Händel, I. Skog, M. Ohlsson och K. V. S. Hari, ”Accurate indoor positioning of firefighters using dual foot-mounted inertial sensors and inter-agent ranging”, *IEEE/ION Position, Location and Navigation Symposium (PLANS)*, april 2014.

[24] N. Stenberg, *Spoofing Mitigation Using Multiple GNSS-Receivers*, Examensarbete, Linköpings Universitet, juni 2019.

[25] J. Rantakokko, J. Rydell, P. Strömbäck, F. Marsten-Eklöf, A. Lennartsson och M. Hagström, *Autonomi och obemannade system – Förslag till inriktning av delområdet Robust Navigering*, Totalförsvarets forskningsinstitut, FOI-R--4523--SE, december 2017.

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