



Undertryckning av GNSS-vilseledning med stöd av tröghetsnavigering

ALBIN WESTLUND, ERIK AXELL

Albin Westlund, Erik Axell

Undertryckning av GNSS- vilseledning med stöd av tröghetsnavigering

Titel	Undertryckning av GNSS-vilseledning med stöd av tröghetsnavigering
Title	GNSS Spoofing Suppression Supported by Inertial Navigation
Rapportnr/Report no	FOI-R--5687--SE
Månad/Month	December
Utgivningsår/Year	2024
Antal sidor/Pages	32
ISSN	1650-1942
Uppdragsgivare/Client	Försvarsmakten
Forskningsområde	Ledningsteknologi
FoT-område	Ledning och MSI
Projektnr/Project no	E51564
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

För att realisera önskad robusthet i system för positionering, navigering och tid (PNT) förutsätts ett multisensorsystem som integrerar en kombination av GNSS (eng. global navigation satellite system) och andra sensorer. En trend i internationell utveckling av PNT är modulära system med öppna standardiserade gränssnitt. För att möjliggöra sådana modulära system krävs möjlighet att övervaka osäkerheter och integritet för varje modul (sensor eller delsystem) i systemet. Målet med denna rapport är att redovisa resultat från en studie av undertryckning av GNSS-vilseledning med stöd av INS (eng. inertial navigation system).

I studien implementerades och utvärderades flera algoritmer i FOI:s egenutvecklade NavToolbox, vilket är ett mjukvarubibliotek för multisensorfusion i PNT-system. Resultaten visar att GNSS-vilseledning kan upptäckas med de utvärderade detektionsalgoritmerna, med stöd av INS. Att upptäcka starten på vilseledning fungerar bra med alla utvärderade detektionsmetoder. Att upptäcka när vilseledningen upphör, så att korrekt GNSS-signal återigen kan användas, är mer utmanande speciellt för de utvärderade detektorerna baserat på jämförelse av relativ rörelse mellan GNSS- och INS-positioner. Innovationsbaserad detektion fungerar ofta bättre i de utvärderade scenarierna än metoden som baseras på relativ rörelse. Den innovationsbaserade detektorn återtar inte vilseledning efter detektion men har en viss fördröjning, på grund av observationsfönstret längd, innan GNSS återtas igen efter attackens slut.

Vilseledning med positioner som avviker kraftigt under kort tid från den sanna positionen är relativt lätta att upptäcka och därmed att exkludera ur filterlösningen. Mer sofistikerade attacker, då vilseledningspositionen avviker gradvis under längre tid är svårare att hantera och upptäcks först en tid efter att de påbörjas. Mottagarpositionen bör därför exkluderas ur navigeringsfilterlösningen redan innan attacken upptäcks. Hur långt tillbaka filtret bör räknas om beror på flera faktorer, bl.a. längden på observationsfönstret, vilseledningens karaktär och kvalitet på tröghetssensorer. Detta utvärderas till viss del i denna rapport men bör studeras vidare.

Utvärderingen visar också att filterlösningen kan få ett stort och snabbt växande fel om filtret börjar dödräkna från en tidpunkt som har stor osäkerhet i hastighet och orientering, exempelvis när hastigheten ändras kraftigt. För att minska risken för initialiseringsfel när GNSS exkluderas och endast INS används bör tidpunkten då död räkning påbörjas väljas med varsamhet, exempelvis genom att identifiera tidigare tidsintervall då hastigheten är konstant.

Nyckelord: GNSS, INS, vilseledning, integritetsövervakning

Summary

A multi-sensor system that integrates a combination of GNSS (global navigation satellite system) and other sensors is required to realize the desired robustness of future positioning, navigation and time (PNT) systems. A clear trend in the international development of PNT is modular systems with open and standardized interfaces. To enable such modular systems, the ability to monitor uncertainties and integrity of each module (sensor or subsystem) in the system is required. The goal of this report is to present results from a study of GNSS spoofing suppression with INS (inertial navigation system) support.

In the study, several algorithms were implemented and evaluated in the NavToolbox, developed by FOI, which is a software library for multi-sensor fusion in PNT systems. The results show that GNSS spoofing can be detected with the evaluated detection algorithms, supported by INS. Detecting the start of spoofing works well with all evaluated detection methods. Detecting when the spoofing ends, so that the correct GNSS position can be used again, is more challenging especially for the evaluated detectors based on comparison of relative motion between GNSS and INS positions. Innovation-based detection often performs better in the evaluated scenarios than the relative motion-based approach. The innovation-based detector does not use spoofed positions after detection but has a certain delay, due to the length of the observation window, before GNSS is used again after the end of the attack.

Spoofed positions that deviate significantly from the true position over a short period of time are relatively easy to detect and thus to exclude from the filter solution. More sophisticated attacks, where the spoofed position deviates gradually over a longer period of time, are more difficult to handle and are only detected some time after the start of the attack. The GNSS position should therefore be excluded from the navigation filter solution even before the attack is detected. How far back the filter should be recalculated depends on several factors, such as the length of the observation window, the nature of the spoofing attack and the quality of the inertial sensors. This is evaluated to some extent in this report, but should be studied further.

The evaluation also shows that the filter solution can have a large and rapidly growing error if the filter starts dead reckoning from a point in time that has large uncertainty in speed and orientation, for example when the speed changes. To reduce the risk of initialization errors when GNSS is excluded and only INS is used, the time when the dead reckoning starts should be chosen carefully, for example by identifying previous time intervals when the speed is constant.

Keywords: GNSS, INS, spoofing, integrity monitoring

Innehållsförteckning

1	Inledning	7
2	Bakgrund.....	8
3	Utvärderade algoritmer	10
	3.1 Test baserat på relativ rörelse	10
	3.2 Innovationsbaserat test.....	11
4	Genomförande.....	13
5	Resultat	17
	5.1 Test baserat på relativ rörelse	17
	5.2 Innovationsbaserat test.....	21
6	Diskussion	28
	6.1 Test baserat på relativ rörelse	28
	6.2 Innovationsbaserat test.....	28
	6.3 Framtida arbete	29
7	Slutsatser.....	30
8	Referenser.....	31

1 Inledning

För att realisera den önskade robustheten i system för positionering, navigering och tid (PNT) förutsätts ett multisensorsystem som integrerar en kombination av GNSS (eng. global navigation satellite system) och andra sensorer. En tydlig trend i den internationella utvecklingen av PNT är modulära system med öppna standardiserade gränssnitt. Idén med ett sådant koncept är att en kärna av sensorfusionsalgoritmer, delsystem och sensorer är lika för ett stort antal plattformar, men andra delsystem eller sensorer kan bytas ut relativt enkelt genom plug-and-play-funktionalitet för att anpassas till olika plattformar. För att möjliggöra sådana modulära system krävs möjlighet att övervaka osäkerheter och integritet för varje modul (sensor eller delsystem) i systemet. Denna rapport redovisar resultat för undertryckning av GNSS-vilseledning med stöd av INS (eng. inertial navigation system).

Syftet med denna rapport är att öka kunskapen om hur robustheten hos multisensorsystem för PNT kan ökas genom integritetsövervakning av ingående sensorer och delsystem. Ett ytterligare syfte med arbetet är att sprida användningen och öka kunskapen om FOI:s egenutvecklade NavToolbox, vilket är ett mjukvarubibliotek för multisensorfusion i PNT-system. Målet med rapporten är att redovisa resultat från en studie av vilseledningsundertryckning i ett integrerat GNSS- och INS-system.

Rapporten inleds med en sammanfattning av kända algoritmer för undertryckning av GNSS-vilseledning med stöd av INS i kapitel 2. Kapitel 3 beskriver de testade och delvis egenutvecklade algoritmerna för undertryckning av GNSS-vilseledning med stöd av INS som har implementerats och utvärderats i NavToolbox. Kapitel 4 beskriver genomförandet av testerna, dvs. dels hur vilseledningen har skapats men också hur data som går in i navigeringsfiltret har skapats. Kapitel 5 redovisar resultaten i form av prestanda för de utvärderade algoritmerna. Kapitel 6 diskuterar lärdomarna från de testade algoritmerna samt beskriver framtida arbete för ytterligare utvärdering och utveckling av algoritmerna. Slutligen presenteras rapportens slutsatser i Kapitel 7.

2 Bakgrund

Alla metoder för att upptäcka störning eller vilseledning av GNSS-mottagare eller fel hos tröghetssensorer är baserade på att jämföra observationer med vad som är förväntat och rimligt. Observationerna kan vara direkta mätningar eller data som har efterbehandlats i varierande grad, t.ex. estimerade pseudoavstånd eller position alternativt rörelser i form av hastighet, acceleration eller innovationer i ett navigeringsfilter. Att utföra en jämförelse för att upptäcka en orimlig avvikelse kan innebära olika saker, från att direkt jämföra en position eller rörelse med en känd rörelsemodell eller ett annat pålitligt PNT-system (t.ex. en annan GNSS-mottagare eller INS), till statistisk detektionsteori eller maskininlärningsbaserade klassificeringsalgoritmer.

För att detektera vilseledning och störning mot GNSS med stöttning av INS finns det flera vägar att gå, exempelvis att använda pseudoavstånd från varje satellit som mätningar eller att beräkna positionen genom iterativ minsta-kvadrat-lösning över pseudoavstånden. För samtliga typer av mätningar finns det metoder för att upptäcka vilseledning och störning som har stora likheter. Konceptuellt baseras alla metoder på att detektera avvikelser mellan beräknad och förväntad acceleration, hastighet eller position för GNSS, INS eller kombinationen av GNSS och INS.

Ett vanligt sätt att beräkna position (och hastighet) genom att utnyttja mätningar från GNSS och INS är med ett utökat Kalmanfilter (eng. extended Kalman filter, EKF), i vilket GNSS-mätningar är filtrets observationer och INS-uppdateringar är insignal i prediktionssteget. Ett sätt att upptäcka avvikelser i ett Kalmanfilter är att skapa ett hypotestest baserat på filtrets så kallade innovation. Innovationen är skillnaden mellan det förväntade mätvärdet, som beräknas genom mätmodellen, och det mätta sensorvärdet. Innovationsbaserad feldetektion bygger på att det finns ett förväntat sensorvärde. Det förväntade sensorvärdet kan exempelvis beräknas genom Kalmanfiltrets sensormodell. Skillnaden mellan det förväntade värdet och den nya mätningen av sensorvärdet bildar filtrets innovation i den aktuella tidpunkten.

En vanlig detektionsmetod är att skapa ett så kallat χ^2 -test med en teststatistik som baseras på innovationen och dess kovarians i varje tidssteg [1]. För detta test kan en beslutströskel beräknas via inversen av fördelningsfunktionen för χ^2 -fördelningen för en önskad signifikansnivå. Om mätningen ger ett värde på teststatistiken som överstiger beslutströskeln kommer mätningen anses felaktig. Dessa tester kan vara av olika fönsterlängder beroende på önskade detektoregenskaper. Längre fönsterlängder detekterar långsamt växande fel lättare medan kortare fönster detekterar snabbt växande fel lättare [1]. Flera parallella detektorer med olika fönsterlängder kan därför krävas för att detektera olika typer av attacker [2], [3]. En beslutströskel kan beräknas från testet genom att välja en önskad signifikansnivå och beräkna tröskeln teoretiskt baserat på modellantaganden eller empiriskt genom att utvärdera hur teststatistiken varierar i olika vilseledningsscenarier.

När en mätning genererar ett testvärde över beslutströskeln så är det vanligaste sättet att inte genomföra mätuppdatering i filtret med den nya mätningen. Ett annat sätt är att dämpa eller förstärka mätkovariansen eller mätmodellens kovarians och i vissa fall direkt tillståndets kovarians beroende på om mätningen anses felaktig [4], [5], [6].

Det finns också arbete som utnyttjar pseudoavstånden och exkluderar satelliter ur positionsberäkningen baserat på variansen av satelliternas innovation [7], [8], [9]. Genom

en förberäknad tröskel som är baserad på motsvarande varians under gynnsamma villkor så exkluderas en satellit i taget tills variansen är lägre än tröskeln med de kvarvarande satelliterna. En exkluderad satellit börjar användas igen först när den är nära det förväntade pseudoavståndet igen. Denna metod förutsätter att minst fyra satelliter anses tillförlitliga, annars sker ingen mätuppdatering. I [8] dras slutsatsen att vilseledning kan upptäckas med denna metod i en flygplanstillämpning, om inte anfallaren kan estimeras och följa offrets rörelse med orealistiskt hög noggrannhet och liten fördröjning.

Ett alternativ till att använda pseudoavstånd är att istället använda bärvågsfasen som mätning. I [10] så spåras bärvågsfasen i ett tätt kopplat system och vilseledningsdetektion sker över de tio senaste mätepokerna för GNSS-mottagaren genom ett χ^2 -test som beror på den förväntade bärvågsfasen med hjälp av IMU¹-mätningar och den mätta bärvågsfasen.

Ett annat sätt att upptäcka avvikelser, utan att använda kalmanfilter, är att ha två oberoende positionslösningar, t.ex. en INS- och en GNSS-lösning. Ett test kan då skapas som jämför position, hastighet eller acceleration mellan GNSS och INS. Position kan utnyttjas genom jämförelse av mottagarposition och INS-position beräknad genom död räkning. Hastighet kan jämföras genom att beräkna den numeriskt genom att derivera mottagarpositionslösning [1]. På liknande sätt kan acceleration beräknas genom att numeriskt beräkna dubbelderivata av mottagarpositioner, vilken kan direkt jämföras med IMU:ns acceleration [11], [12], [13], [14].

I [15] utnyttjas rörelser hos ett fartyg (pitch och roll), som är okända för anfallaren, tillsammans med IMU-data för att detektera vilseledning. Ett hypotestest baserat på rörelseavvikelser i position mellan GNSS och INS används för att skapa en detektor baserat på ett så kallat GLRT (eng. generalized likelihood-ratio test). GLRT är en generell metod inom detektionsteori, med vilken teststatistiken skapas genom att beräkna kvoten mellan sannolikheterna för två hypoteser och beräkna okända parametrar med maximum likelihood-metoden.

En svårighet med att göra jämförelser med INS är att felet i denna lösning ackumuleras över tid p.g.a. sensorfel. Om GNSS-mottagaren har varit utsatt för vilseledning under lång tid är det därför svårt att göra en rimlig jämförelse med lösningen från enbart INS. En åtgärd för att minska denna svårighet är att integrera ytterligare sensorer för att stötta INS-lösningen. Exempelvis föreslår [16] vilseledningsdetektion som jämför mottagarpositioner med positioner från ett system som kombinerar IMU och odometer (hastighetsmätningar) i en fordonstillämpning.

I [17] föreslås ett GLRT för att upptäcka vilseledning av GNSS med stöd av INS och magnetometer. I [17] används GLRT genom att skatta (a) orientering med magnetometer och gyrometer, (b) position, acceleration och hastighet genom maximum likelihood-metoden och (c) beräkna sannolikhetskvoten för de två hypoteserna att GNSS-mottagaren är utsatt för en vilseledningsattack eller att den inte är utsatt för en attack. Under hypotesen att mottagaren inte är utsatt för någon attack används acceleration, position och initial hastighet som parametrar som ska motsvara den sanna trajektorian, medan för den andra hypotesen används samma parametrar plus motsvarande parametrar för en vilseledd körbana.

¹ Inertial measurement unit

3 Utvärderade algoritmer

Utvärderingen av algoritmerna har baserats på navigeringsfilter som nyttjar mätningar från en GNSS-mottagare. Undertryckning av vilseledning gjordes genom att mottagarens positionslösning utesluts ur filtret om den bedöms vara vilseledd. I uppdateringssteget användes accelerometer- och gyrometermätningar för att prediktera rörelse mellan mottagaruppdateringarna.

Ett alternativ till att använda positioner är att använda pseudoavstånd som mätningar i filtret, för att avgöra om varje individuell satellitsignal ska inkluderas i filtret. Detta kan förbättra prestanda i vissa fall, eftersom det ger möjlighet att inkludera vissa satellitsignaler och utesluta andra.

I löst integrerade modulära PNT-system förväntas GNSS-mottagare leverera positionslösningar, men inte alltid pseudoavstånd. För många fall av vilseledning bedömer vi att vilseledningsdetektion baserat på positionsmätningar är tillräckligt och presterar ungefär lika bra som detektion baserat på pseudoavstånd. Dessutom är nyttjande av pseudoavstånd istället för position mer komplext att utveckla, implementera och utvärdera. Det är exempelvis enkelt att i en mjukvarusimulering generera egna positioner givet en sann bana och därmed också svåra fall av vilseledning utan långa simuleringar i en fullständig GNSS-simulator. Att generera pseudoavstånd som mätningar kräver kontroll av fler parametrar såsom satellitpositioner och tid. Dessutom krävs ett navigeringsfilter som kan utnyttja pseudoavstånd fullt ut, i kombination med INS. Denna studie har utgått från NavToolbox-biblioteket och där har filtren som nyttjar pseudoavstånd ännu inte validerats att de fungerar som förväntat. Filtret har varit ett utökat Kalmanfilter med tillstånd för position, hastighet och orientering.

För att detektera vilseledning har vi fokuserat på två typer av tester. Dels innovationsbaserade tester, där innovationen är felet i positionsprediktionen jämfört med nya mätningar från en GNSS-mottagare. Dels tester där vi jämför rörelse som beräknas från mottagarpositioner respektive INS oberoende av varandra. En viktig aspekt i studien har varit att inte bara detektera när GNSS-mottagaren börjar bli vilseledd, utan också att bestämma när vilseledningsattacken är slut. Därför har vi valt att utforma tester och filter därefter.

Gemensamt för alla tester är att när vilseledning bedöms vara aktiv så räknas filterlösningen om från ett tidigare tidssteg och därifrån används enbart IMU-uppdateringar tills mottagarpositionen inte anses vara vilseledd. Genom att beräkna filterlösningen från en tidigare tidpunkt blir avvikelserna från den sanna trajektorian betydligt mindre jämfört med en beräkning som görs då vilseledning upptäcks. Detta beror på att det kan ta flera tidssteg i navigeringsfiltret innan vilseledning upptäcks, speciellt vid långsamt avvikande attacker, vilket innebär att vilseledda positioner riskerar att inkluderas i filtret redan innan attacken upptäcks. Att räkna filtrets tillstånd en tid tillbaka från upptäckt av vilseledningen innebär t.ex. att den initiala hastigheten och orienteringen i filtret är närmare de sanna då mottagarpositioner exkluderas ur lösningen.

I vissa fall bör attacken kunna detekteras snabbt, exempelvis när vilseledningsattacken ger ett stort positionshopp direkt, och därmed behöver omräkningen bara göras från föregående tidssteg och inte flera tidssteg tillbaka. Hur långt tillbaka omräkningen bör göras beror på bl.a. hur vilseledningen avviker från den sanna banan, hur långt observationsfönster som används för detektion och kvalitet på IMU.

3.1 Test baserat på relativ rörelse

En typ av test vi har undersökt är att jämföra mottagarens positionslösning med en INS-lösning under ett observationsfönster. INS-lösningen antas ha blivit initialiserad någon gång då hastighet och orientering är kända, och därefter har endast uppdateringar från

IMU skett genom död räkning utan några korrigeringar av hastighet eller stöttning med GNSS.

Skillnaden i rörelse mellan GNSS-mottagaren och INS har beräknats inom varje observationsfönster på två sätt:

1. Genom att ta första positionen jämfört med den sista positionen

$$T_i = \|(GNSS_i - GNSS_{i-k}) - (INS_i - INS_{i-k})\|. \quad (1)$$
2. Genom att summera parvisa skillnaden mellan varje mottagaruppdatering och motsvarande positionsskattning för INS

$$T_i = \sum_{j=i-k+1}^i \|(GNSS_j - GNSS_{j-1}) - (INS_j - INS_{j-1})\|. \quad (2)$$

I ekvationerna (1) och (2) är $GNSS_i$ positionsmätning från mottagaren i tidssteg i och INS_i är positionslösning i samma tidpunkt för lösningen med enbart IMU.

Ett problem med detta är att INS-lösningen driver i hastighet och därmed även i position. Med tiden kommer dess rörelse därmed inte kunna jämföras med GNSS-mottagarens rörelse eftersom den har drivit för mycket i hastighet. Därför behövs en uppdatering av hastighet och orientering under långa tester. En vanlig lösning av den typen av problem är att till exempel ha en stöttande odometrer som uppdaterar och korregerar hastigheten.

Beslutströskeln för testerna har valts som konstant i kombination med att test (1) och (2) har justerats, genom att skatta en linjär tillväxt från fallet utan vilseledning. Testet har sedan modifierats genom att subtrahera den modellerade tillväxten.

För att användas i en verklig implementation bör IMU-driften hanteras av navigeringsfiltret genom att kontinuerligt estimeras och kompenseras. Driften är beroende på bl.a. hur länge sedan INS-lösningen uppdaterades med data från annan sensor, IMU-fel och manövrerar. Detta bör hanteras i framtida studier.

3.2 Innovationsbaserat test

För denna typ av test har Mahalanobis-avståndet i kvadrat, för varje mätuppdatering, sparats. Mahalanobis-avståndet betar sig olika beroende på när filtret detekterar eller säger att vilseledning är aktivt. Ju tidigare en attack upptäcks, desto lättare är det att upptäcka att attacken är slut. Detta på grund av att prediktionen från filtret kommer vara närmre de sanna GNSS-signalerna vid attackens slut.

Genom att summera avståndet över flera tidssteg fås en teststatistik, q_i , som är χ^2 -fördelad med $3k$ frihetsgrader om felet antas vara normalfördelat [1]

$$q_i = \sum_{j=i-k}^i \gamma_j^T S_j^{-1} \gamma_j, \quad (3)$$

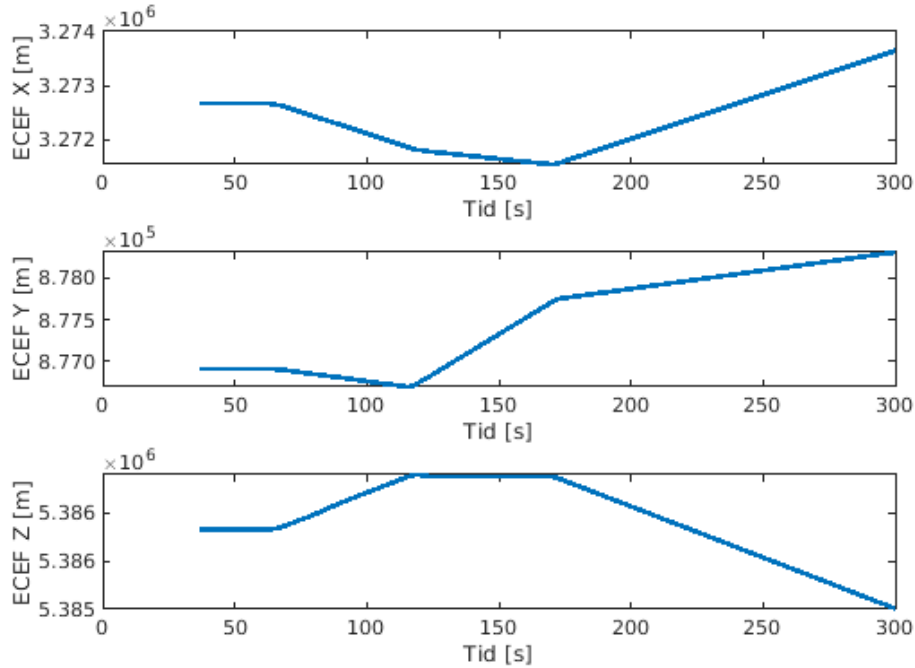
där γ_j är innovationen i tidpunkt j , S_j är kovariansmatrisen och k är längden på observationsfönstret inom vilket testet beräknas. Då teststatistiken har en sannolikhetsfördelning som åtminstone approximativt överensstämmer med teorin kan en beslutströskel beräknas teoretiskt för ett givet val av falsklarmssannolikhet.

Ett kort observationsfönster (litet k) gör att teststatistiken varierar mer och snabbare än med ett långt observationsfönster (stort k). Då vilseledning aktiveras kommer en teststatistik baserat på ett kortare fönster alltså att få ett större hopp jämfört med ett längre fönster. Det finns både för- och nackdelar med detta. Fönsterlängden påverkar även hur lång tid teststatistiken minskar när en attack har stängts av, på så sätt att teststatistiken minskar i värde lika länge som fönsterlängden. Därmed fås en fördröjning till att vilseledning bedöms ha upphört, som beror på fönstrets längd. Med ett långt fönster och till exempel två vilseledningsattacker som är tätt inpå varandra kommer sannolikheten för att hinna få in en sann GNSS-signal till filtret vara liten. Sannolikheten för att hinna

uppdatera med en sann GNSS-signal kan dock bli större genom att välja en högre beslutströskel, men på bekostnad av högre sannolikhet att använda vilseledda mottagarpositioner. Däremot kan ett litet fönster ha större sannolikhet för att ta in vilseledning för snabbt eller i fel tidpunkt p.g.a. teststatistikens snabbare variationer. Ett exempel är om vilseledaren korsar den positionslösning filtret har.

4 Genomförande

Simuleringar har gjorts i FOI:s GNSS-simulator för att generera GNSS- och IMU-data enligt en modell av ett objekts körbana. Trajektorian har två svängar, se Figur 1, och objektet körde i konstant hastighet med 20 m/s.



Figur 1: Trajektorian för varje koordinat i ECEF².

För att bearbeta GNSS-data från simulatören användes en U-blox-mottagare (modell ZED-F9P). På grund av att simuleringar i realtid tar lång tid har denna utvärdering valt att simulera vilseledning genom att digitalt skapa vilseledningspositioner under olika långa perioder och skeden. Detta har gjorts i Matlab med hjälp av mottagarmätningar från ett simulatortest utan vilseledning. Positionerna och deras osäkerhet, som beräknas av mottagaren, används som mätningar och mätmodellens kovarians i navigeringsfiltret. Under vilseledning används samma kovarians som mätningarna och samma hastighetsskattningar som mottagaren.

För att injicera en vilseledningsattack har därefter ett växande fel för azimuth lagts på, alltså kommer objektet sakta avvika från den sanna trajektorian. Azimut har beräknats i horisontalplanet med hjälp av de beräknade hastighetsmätningarna i horisontalplanet, $\hat{v}_{ECEF,y_i}$ och $\hat{v}_{ECEF,x_i}$, enligt

$$\widehat{Azimut}_i = \tan^{-1} \left(\frac{\hat{v}_{ECEF,y_i}}{\hat{v}_{ECEF,x_i}} \right).$$

Det adderade felet som simulerar vilseledningen har en tillväxtperiod, en avtagande period och en period där objektet kör i samma riktning som den sanna trajektorian, men en bit ifrån som följd av det tidigare tillagda felet. Under tillväxtfasen så växer felet exponentiellt tills det når den felstorlek som ska testas. Azimutfelet växer enligt följande, där N är det sista tidsteget i tillväxtfasen:

² Earth-centered, Earth-fixed coordinate system

$$Azimut_{vilseledning,i} = \widehat{Azimut}_i + \exp\left(\log(Azimut_{fel} + 1) \cdot \frac{i}{N}\right) - 1, \\ i = 0, 1, 2, \dots, N.$$

Felet avtar sedan på följande sätt där M är det sista tidssteget då felet avtar

$$Azimut = \widehat{Azimut}_i + \exp\left(\log(Azimut_{fel} + 1) \cdot \frac{M-i}{M-N}\right) - 1, \\ i = N, N+1, N+2, \dots, M.$$

Sedan är azimutfelet noll tills attacken upphör. Hastigheten beräknas enligt följande under vilseledningsattacken

$$v_{vilseledning,i} = \left[\begin{array}{c} \cos(Azimut_{vilseledning,i}) \\ \sin(Azimut_{vilseledning,i}) \\ \frac{\hat{v}_{ECEF,z_i}}{\|\hat{v}_{ECEF}\|} \end{array} \right] \|\hat{v}_{ECEF}\|.$$

Vilseledningspositionerna beräknas därefter på följande sätt under vilseledningsattacken

$$p_{vilseledning,i+1} = p_{vilseledning,i} + v_{vilseledning,i+1}.$$

Tabell 1 visar parametrarna för de fyra vilseledningsscenario som används för utvärdering. Figur 2, Figur 3 och Figur 4 visar felet i azimut, hastighet respektive position för dessa scenarier. Positionsfelet är beräknat som

$$\|\hat{p}_{ECEF,i} - p_{ECEF,i}\|,$$

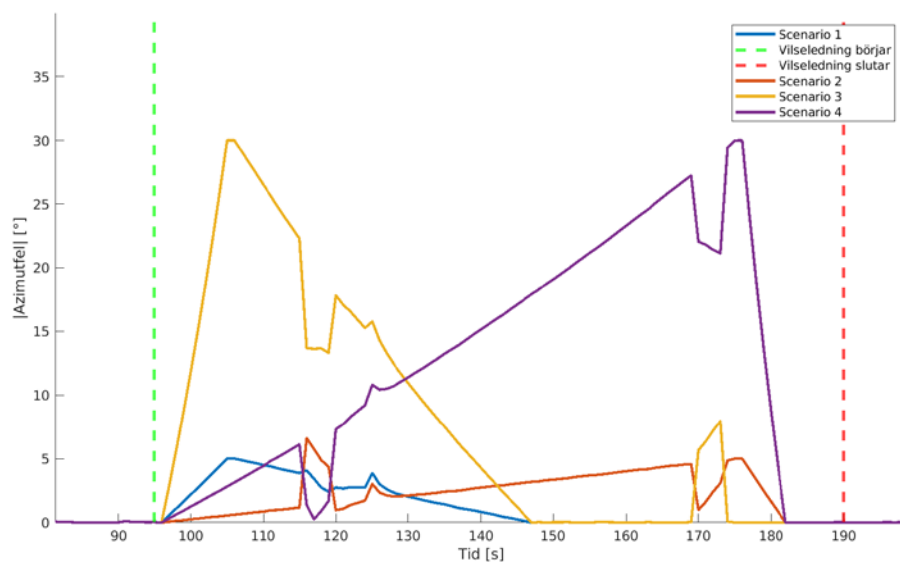
för varje tidssteg i och hastighetsfelet är beräknat på liknande sätt, enligt

$$\|\hat{v}_{ECEF,i} - v_{ECEF,i}\|.$$

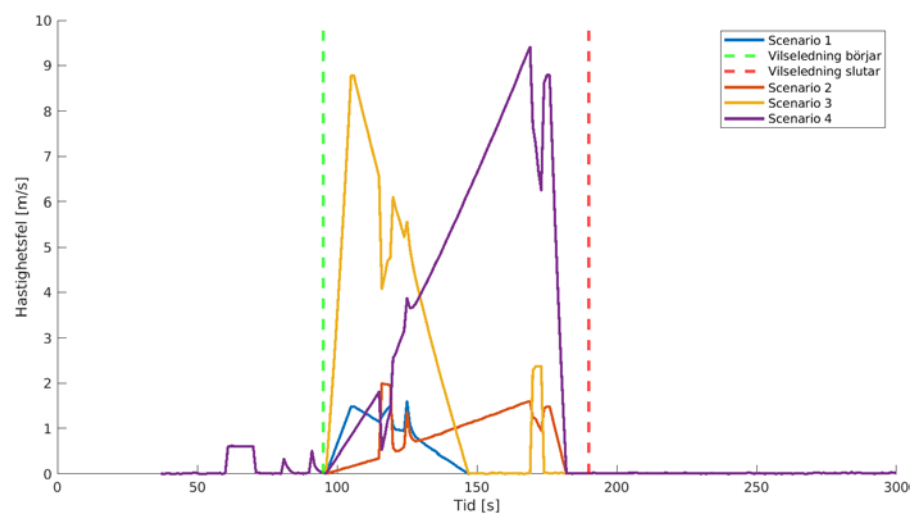
Detta gäller i hela rapporten då felet i hastighet och position nämns.

Tabell 1: Fyra scenarion som används för utvärdering.

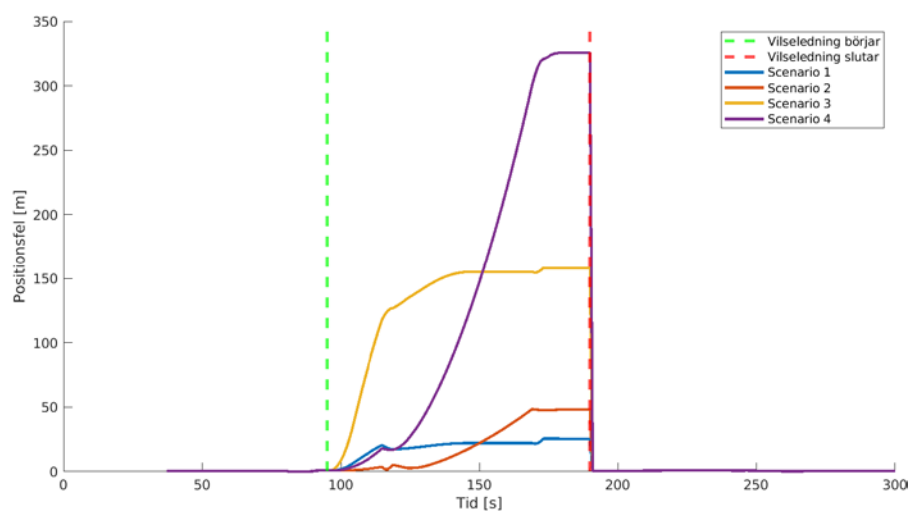
Scenario	Start [s]	Slut [s]	Tillväxtperiod [s]	Azimutfel [°]
1	95	190	10	5
2	95	190	80	5
3	95	190	10	30
4	95	190	80	30



Figur 2: Azimutfelet till följd av fyra olika vilseledningsattacker.



Figur 3: Hastighetsfelet till följd av fyra olika vilseledningsattacker.



Figur 4: Positionsfelet till följd av fyra olika vilseledningsattacker.

Eftersom azimuthfelet är baserat på den skattade hastigheten växer inte det beräknade azimuthfelet på exakt samma sätt som det adderade felet. Det beror på att mottagaren har perioder där den skattar hastigheten sämre, till exempel i kurvor. Detta ses i Figur 2, då objektet ändrar riktning omkring 115 s och 170 s samtidigt som azimuthfelet avviker från tillväxten enligt det adderade felets modell.

Ofta har GNSS-mottagare ett eget navigeringsfilter som motverkar alltför snabba variationer i deras positionsskattningar. Vi har valt att inte filtrera de skattade vilseledningspositionerna genom till exempel ett Kalmanfilter, eftersom det krävs trimning av filtret och val av lämplig rörelsemodell för att efterlikna övergångarna mellan då vilseledningen sätts på respektive av.

Förutom data från U-blox-mottagaren, som endast nyttjar GPS³ L1, och data om hur objekt rör sig på riktigt genererar GNSS-simulatorens även emulerade IMU-data. Dessa data är simulerade med fel enligt en felmodell för den aktuella IMU:n, vilket är KVH 1775. Eftersom IMU-data skapas enligt en stokastisk felmodell ger olika simuleringar olika realiseringar av IMU-data vilket ger varierande avvikelser. För att göra rättvisa jämförelser mellan olika vilseledningsscenarion (även utan vilseledning) har samma IMU-data använts för alla scenarion.

³ Global Positioning System

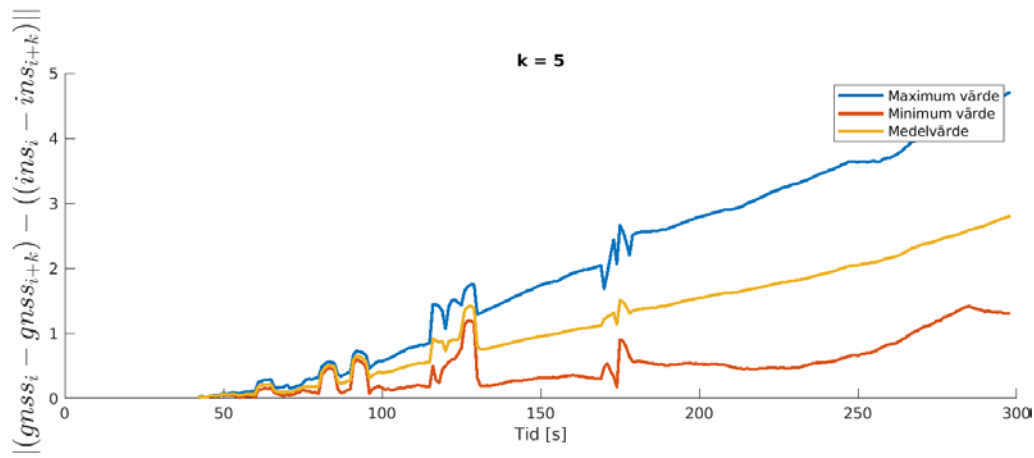
5 Resultat

I detta avsnitt presenteras resultatet av studien avseende prestanda för undertryckning av vilseledning med olika val av detektionsalgoritmer och för olika vilseledningsscenarion.

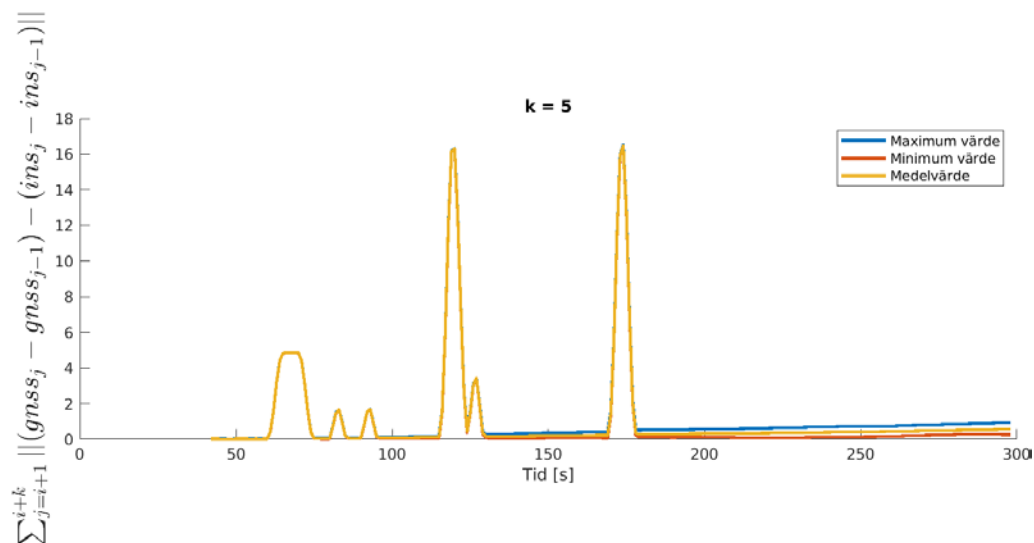
5.1 Test baserat på relativ rörelse

I Figur 5 och Figur 6 visas testvärden för test (1) respektive test (2), där INS-lösningen initialiseras och inte får stöttande mätningar från andra sensorer efter initialisering. Som förväntat är feltillväxten hos INS-lösningen ett problem om mottagarmätningar jämförs med en INS-lösning som initialiserades långt innan attacken. Värdena som visas är medel-, maximum- och minimivärdet i varje tidssteg från sex olika realiseringar av samma körbanan samt samma IMU och felmodell.

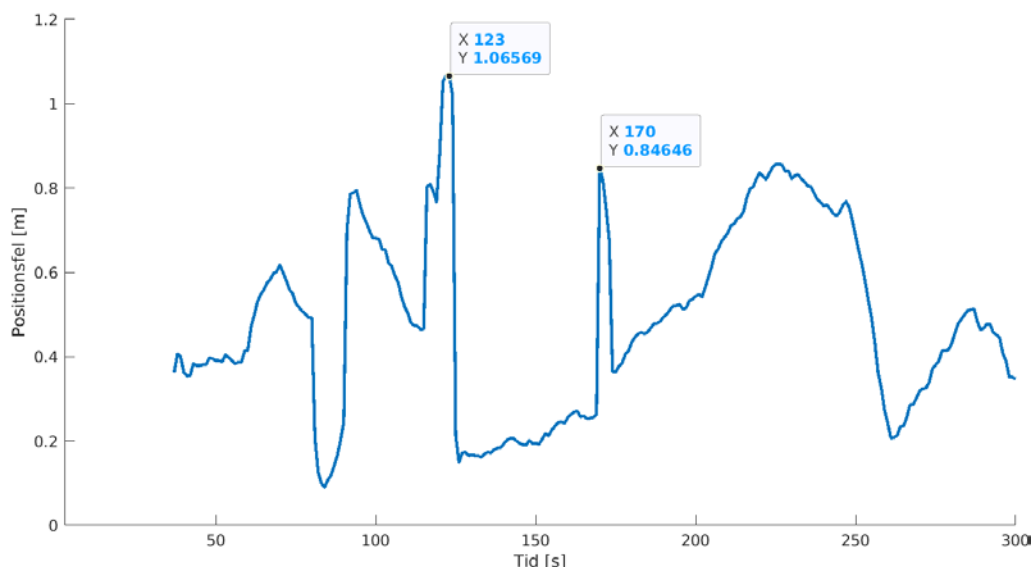
Det är tydligt för test av typen (2) att risken för falsklarm är högre när objektet ändrar riktning i svängar, eftersom teststatistiken får ökat värde där. Mottagaren får också ett större fel i svängar, se t.ex. Figur 7 där svängarna befinner sig vid de markerade topparna.



Figur 5: Test enligt (1) med fönsterlängd på fem sampel.



Figur 6: Test enligt (2) med fönsterlängd på fem sampel.



Figur 7: Mottagarfelet under ett fall utan vilseledning, med markerade toppar i felet.

Tröskeln för test (1) och (2) väljs från den sämsta realiseringen, se exempelvis Figur 5 och Figur 6, och blir

$$T_r = \max_i (T_i - k \cdot (t_i - t_o)),$$

där k i detta fall är den skattade lutningen, t_o är tiden för initialiseringen, T_i är teststatistikens värde innan justering, i är index för det aktuella tidssteget och T_r är tröskeln. Teststatistiken blir efter justering följande

$$T_i = T_i - k \cdot (t_i - t_o).$$

Med kompensation ger testerna färre falsklarm, men samtidigt växer sannolikheten för missad detektion med tiden. Genom att istället börja dödräkna från ett så sent tidssteg som möjligt minskar sannolikheten för missad detektion jämfört med död räkning från början av simuleringen.

Enda gången död räkning med INS kan initialiseras med säkerhet är när objektet har en känd rörelse, exempelvis när det står stilla. Alternativa initialiseringsformer för ett rörligt objekt är att till exempel nyttja hastighetsskattningen från antingen ett navigeringsfilter, mätningar från mottagaren eller att vrida objektets orientering med hjälp av flera mätpunkter efter varandra. Dessa alternativ kommer att vara sämre än initialisering vid stillastående, men tröskelvärden för dessa tester borde kunna anpassas efter resultat och ändå ge bra detektionssannolikhet.

Ett av mått för prestanda som används i denna studie är RMSE (root mean square error) som har beräknats enligt

$$RMSE = \sqrt{\frac{1}{N} \sum_{i=1}^N \|\hat{p}_i - p_i\|^2}.$$

I Tabell 2 visas detektorinställningar för utvärdering av test (1). Filterlösningen räknas om 20 sampel bakåt i tiden då den snabbaste detektionen var 3 s, och den långsammaste 23 s, efter vilseledningens start (Tabell 3). Att långsammast upptäckt sker efter 23 s beror på att

positionsfelet hos mottagaren endast har växt till fyra meter vid den tidpunkten, då ett fönster med 20 sampel används.

I Tabell 3 visas resultat med test (1), och det syns att bättre lösningar fås med vilseledningsexkludering. Eftersom detektionen inte beror på filtrets lösning är perioderna då vilseledning exkluderas samma när filtret räknar om med död räkning från ett antal sampel bakåt som när det inte görs.

Tabell 2: Detektorinställningar för utvärdering av test (1).

Detektorinställning	Metod	Fönsterlängd	Antal sampel bakåt från detektion som död räkning börjar
1	(1)	20	20
2	(1)	5	20
3	(1)	20	0
4	(1)	5	0

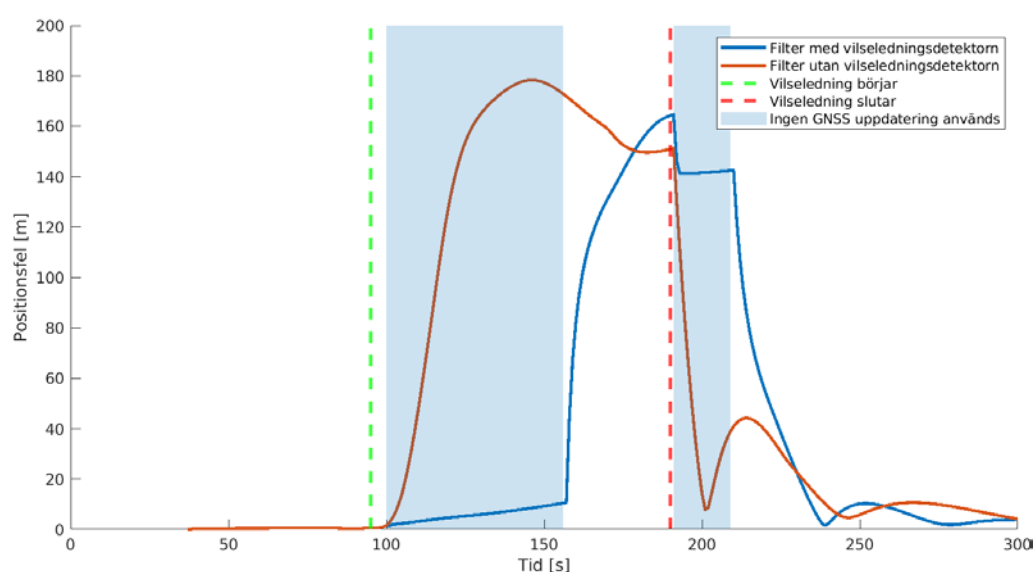
Tabell 3: Observerade resultat med test enligt (1) och där filtrets tillstånd räknas om 20 sampel tillbaka i tiden från detektion av vilseledning.

Scenario se Tabell 1	Detektorinställning se Tabell 2	Första larm [s]	Mottagarfel vid detektion [m]	RMSE [m]	Tid från attack är slut tills GNSS används oavbrutet [s]	Största positionsfel [m]
1	-	-	-	13	-	26
2	-	-	-	19	-	55
3	-	-	-	89	-	178
4	-	-	-	127	-	369
1	1	106	9	12	20	28
2	1	118	4	8	20	25
3	1	100	9	65	20	165
4	1	110	10	8	20	22
1	2	101	3	11	5	26
2	2	116	2	7	5	33
3	2	98	3	59	5	152
4	2	104	3	28	5	219
1	3	106	9	13	20	30
2	3	118	4	7	20	20
3	3	100	9	69	20	173
4	3	110	10	9	20	23
1	4	101	3	11	5	26
2	4	116	2	8	5	25
3	4	98	3	60	5	155
4	4	104	3	40	5	169

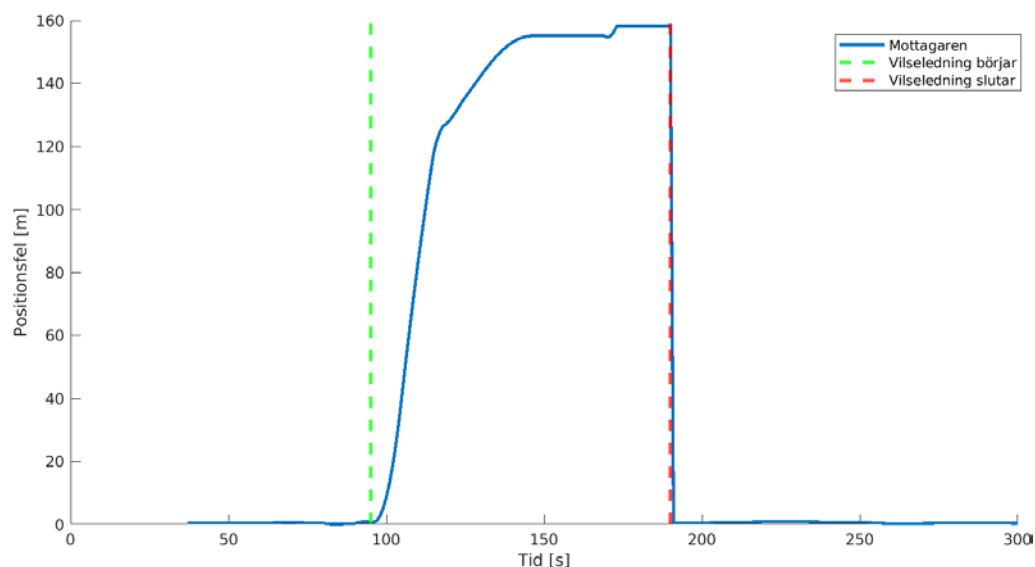
För fallet då azimutfelet är 30 grader och har en tillväxtperiod på 10 s, fås ett relativt stort fel även med en detektor (Figur 8). Detta beror på att attacken är utformad så att vilseledningspositionerna rör sig på liknande sätt som objektet i slutet av attacken. Detta ses i Figur 9, där positionsfelet är nästan konstant i slutet. Perioden för då vilseledningspositionerna rör sig i samma rörelse som den sanna trajektorien är ca 40 s. Detta test jämför inte den förväntade positionen från tidpunkten för vilseledningsdetektionen, utan endast lika många sampel bakåt i tiden som motsvarar

fönsterlängden. Därmed kan den förväntade positionen i detta test vara nära vilseledningspositionerna i perioder då de rör sig likt den sanna trajektorian. Istället kan fönstret vid detektion vara adaptivt och t.ex. lika långt som tidsskillnaden mellan nu och vilseledningsdetektionen, vilket bör testas i framtida arbete. Dock som tidigare har beskrivits, växer testen med tiden p.g.a. feltillväxt från IMU och därför behöver en noggrann analys göras för hur fönsterlängd påverkar testvärde.

Testet som har en fönsterlängd på 20 sampel får också ett lägre RMSE överlag och speciellt för de aggressivare attackerna i scenarier 1 och 3. Detta beror på att testet med fönsterlängd på 20 sampel tar in mottagarpositionen 15 sampel senare jämfört med fem sampels fönsterlängd, för de attacker som under en period rör sig likt objektets sanna rörelse. Däremot detekterar testen med kortare fönsterlängd vilseledningen snabbare, men det spelar mindre roll då mottagarfelet är ungefär lika stort vid detektion för fönsterlängderna 5 respektive 20 sampel.



Figur 8: Positionsfelet med och utan den beskrivna vilseledningsdetektor enligt test (1) i scenario 3 (maximalt azimuthfel på 30 grader och tillväxtperiod på 10 s).



Figur 9: Positionsfelet hos mottagaren under vilseledningsattacken i scenario 3 (maximalt azimuthfel på 30 grader och tillväxtperiod på 10 s).

Test (1) jämför sista och första positionen över ett fönster, men inte positionerna däremellan. Det innebär att vilseledning inte kan upptäckas om första och sista positionerna i båda lösningarna stämmer överens, oavsett hur rörelsen har skett mellan dessa positioner. Ett alternativt test som inte har undersökts i denna studie är att ha ett glidande test över ett fönster där varje sampel jämförs med l sampel bakåt i tiden. Ekvationen för ett sådant test kan uttryckas som

$$T_i = \sum_{j=i-k+l}^i \|(GNSS_j - GNSS_{j-l}) - (INS_j - INS_{j-l})\|.$$

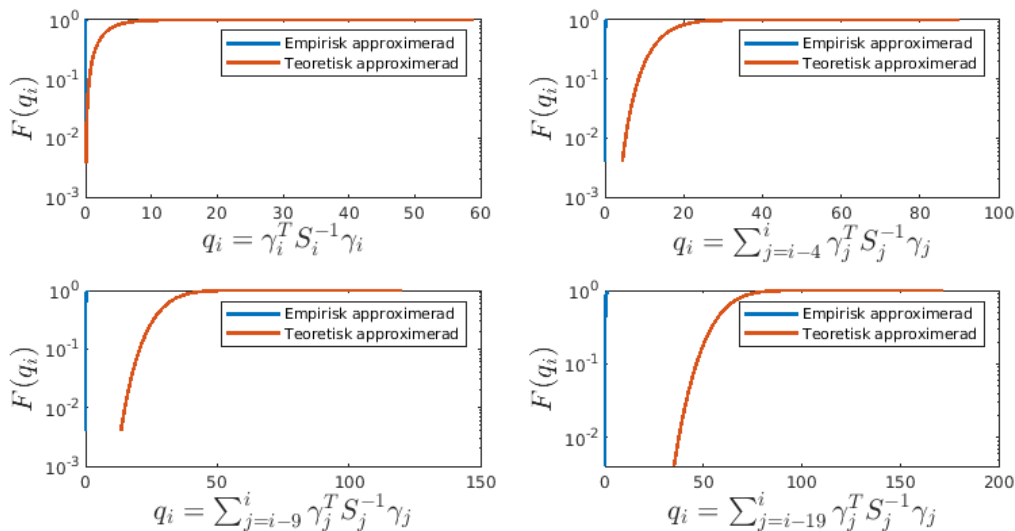
Viktigt i ett sådant test är att ha ett väl valt stort l , då om l är 1 blir det samma som test (2), som hade ökad sannolikheten för falsklarm i kurvor, och om $l = k$ blir det samma som test (1). Detta är något som bör studeras i framtida arbete.

5.2 Innovationsbaserat test

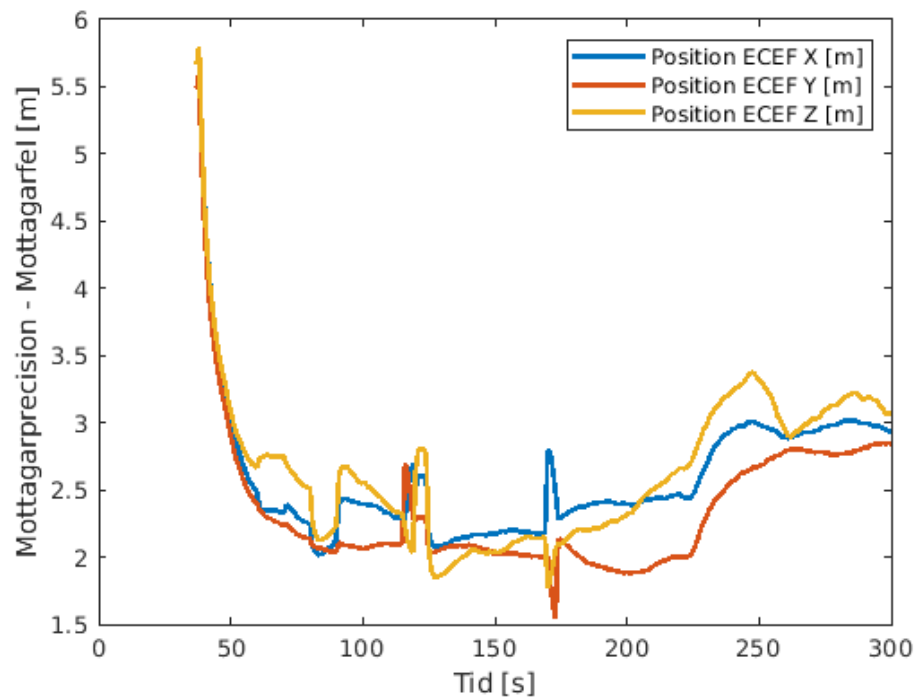
I detta avsnitt presenteras resultat för innovationsbaserade tester. I Figur 10 visas den empiriskt beräknade kumulativa fördelningsfunktionen av teststatistiken (3) under ett fall utan vilseledning. Den teoretiska approximationen ses också för samma teststatistik och det är tydligt att kurvorna inte matchar varandra. Detta innebär att de antaganden som ligger till grund för den teoretiska approximationen inte stämmer särskilt bra med data från testerna, dvs. att innovationsvektorn i testerna inte är normalfördelad och oberoende i tid. En förklaring till detta är att en jämförelse mellan empirisk och teoretisk approximation bör ske på betydligt fler scenarion, fler simuleringar samt över en längre tid, för att den ska efterlikna teorin. En annan faktor är osäkerheten hos positionerna. När mottagarfelet jämförs med mottagarens egna skattade precision är det tydligt att precisionen är grovt underskattad (Figur 11). Med en bättre skattad precision blir också teststatistiken högre, eftersom innovationen multipliceras med inversen av innovationens kovarians, vilken består av bl.a. mätningarnas kovarians, enligt

$$S_i = H_i P_{i|i-1} H_i^T + R_i,$$

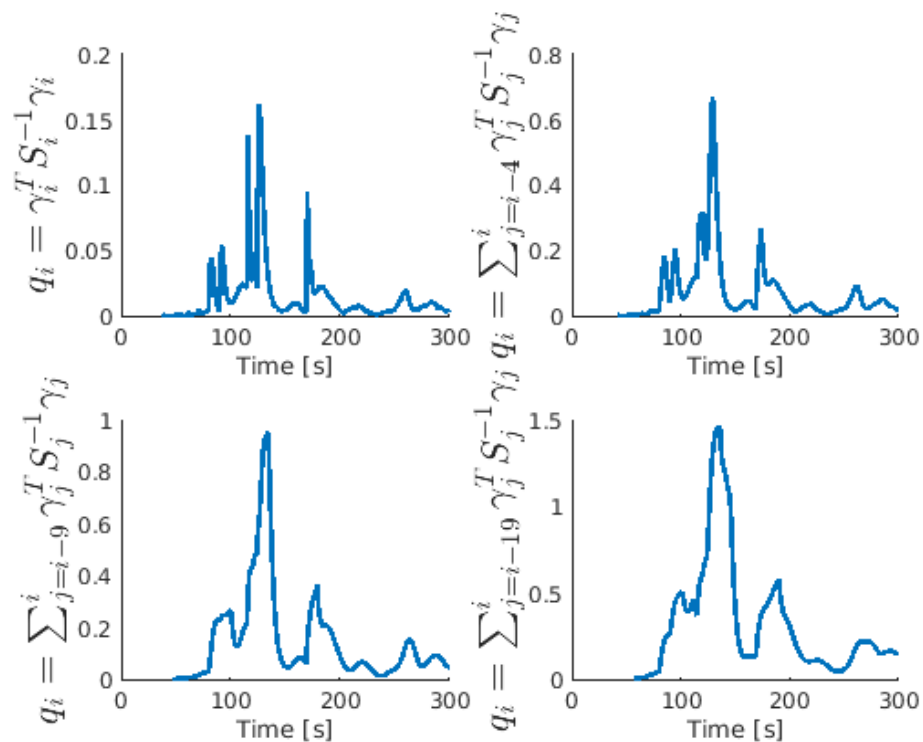
där R_i är kovariansen hos mätningen, $P_{i|i-1}$ är osäkerheten kring tillståndet innan mätningen och $H_i = \frac{\partial h}{\partial x}|_{x_{i|i-1}}$ är partiella derivatan av mätmodellen givet tillståndets skattning innan mätningen. En felaktig skattning av kovariansen blir således en faktor till att den empiriska datan och den teoretiska approximationen inte stämmer helt överens.



Figur 10: Den empiriska och teoretiska approximationen av kumulativ fördelning av teststatistiken (3) under ett fall utan vilseledning.



Figur 11: Mottagarens fel jämfört med mottagarens skattade precision.



Figur 12: Teststatistiken utan vilseledning.

Beslutströskeln väljs som max-värdet för teststatistiken under fallet utan vilseledning, se Figur 12 för hur teststatistiken varierar över simuleringstiden. Tröskeln avrundas uppåt till närmsta heltal för att ytterligare ta höjd mot falsklarm.

I Tabell 4 visas detektorinställningar för utvärdering av test (3) och i Tabell 5 visas resultaten för inställningar med scenarion från Tabell 1.

Tabell 4. Detektorinställningar för utvärdering av test (3) för scenario 1-4 i Tabell 1.

Detektor-inställning	Metod	Fönsterlängd	Antal sampel bakåt död räkning börjar vid detektion	Tröskel
5	(3)	20	20	2
6	(3)	5	20	1
7	(3)	20	0	2
8	(3)	5	0	1

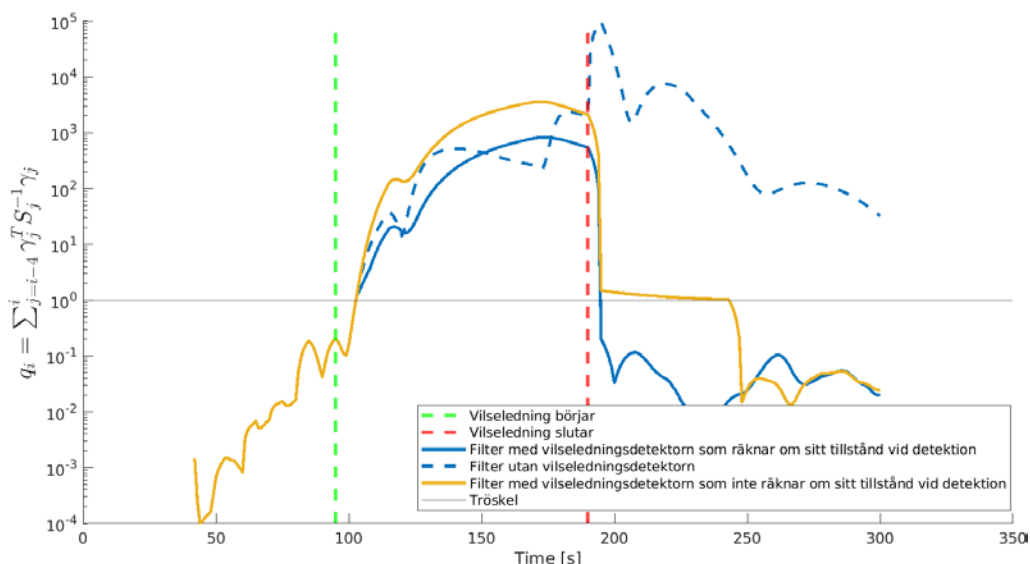
Tabell 5: Resultat med vilseledningsdetektorn enligt test (3).

Scenario se Tabell 1	Detektor-inställning se Tabell 4	Första larm [s]	Mottagarfel vid larm [m]	RMSE [m]	Tid från att attack är slut till att GNSS används oavbrutet [s]	Största positionsfelet [m]
1	-	-	-	13	-	26
2	-	-	-	18	-	55
3	-	-	-	89	-	178
4	-	-	-	127	-	369
1	5	102	4	4	20	12
2	5	117	2	2	20	6
3	5	99	5	5	20	14
4	5	104	3	4	20	11
1	6	101	3	4	5	11
2	6	116	2	2	5	5
3	6	98	3	4	5	12
4	6	103	3	4	5	10
1	7	102	4	17	Aldrig	41
2	7	117	2	20	Aldrig	49
3	7	99	5	15	Aldrig	36
4	7	104	3	19	Aldrig	45
1	8	101	3	4	5	10
2	8	116	2	23	Aldrig	55
3	8	98	3	2	5	6
4	8	103	3	7	53	19

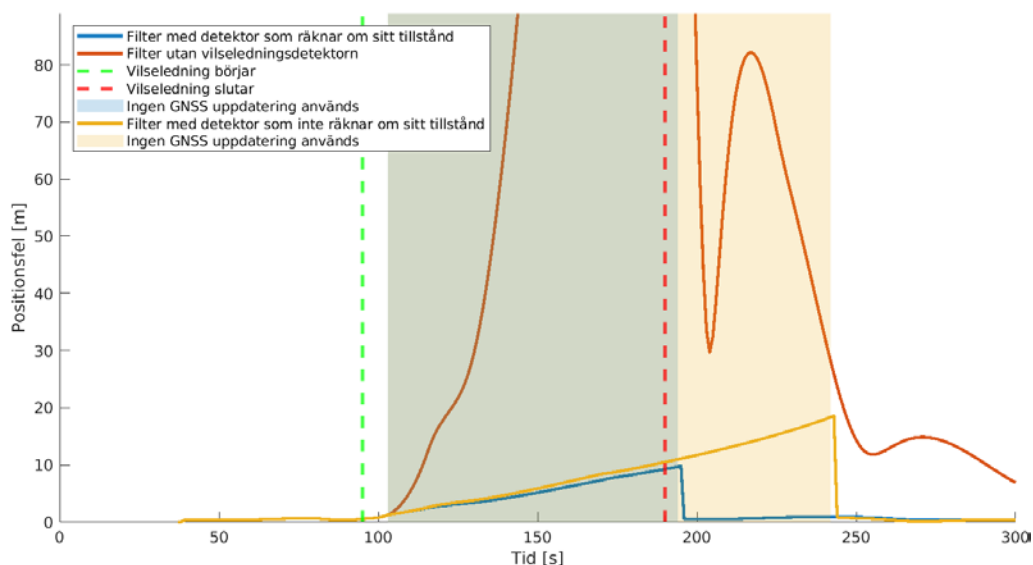
Den innovationsbaserade detektorn upptäcker vilseledningen ungefär lika snabbt som den detektor som beskrevs i föregående kapitel (Tabell 3). Till skillnad från detektorn baserad på relativ rörelse så tar den innovationsbaserade detektorn inte in vilseledda positioner i dessa scenarion efter att den har detekterat vilseledning (Figur 14). Resultaten visar också att lösningen blir bättre av att räkna om filtrets tillstånd med död räkning 20 sampel bakåt i tiden från detektion, när fönsterlängden är 20 sampel. Det framkommer också att teststatistiken, utan att räkna om filtrets tillstånd med död räkning 20 sampel bakåt från detektion, inte går under beslutströskeln när vilseledningen är avslutad. Detta gäller i samtliga gjorda tester/scenarion för test (3) med vissa undantag för när fönsterlängd är fem sampel och scenarion har ett kraftigt växande fel (scenario 1 och 3), vilket troligen beror på att felet detekteras tidigt. Scenario 4 lyckas också använda GNSS-signaler igen men med en längre fördröjning.

I Figur 13 visas teststatistiken enligt test (3) med en fönsterlängd på fem sampel för scenario 4 där den blåa linjen räknar om filtrets tillstånd vid detektion och den gula gör inte det. Det är tydligt att teststatistiken blir lägre då filtret räknas om vilket delvis beror på

större osäkerhet i filtret då det var 20 s längre sedan en mätuppdatering skedde. Lösningen som inte räknar om filtertillståndet har blivit korrupt av att det har tagit in vilseledda mottagarpositioner och kan därmed ha en sämre skattning av sitt tillstånd, men med högre (falsk) säkerhet. I Figur 14 visas positionsfelet för filtret, där ses det att lösningen som räknar om filtertillståndet från 20 sampel bakåt med död räkning också får bättre positionslösningar med tiden.



Figur 13: Teststatistiken (3) med fönsterlängd på fem sampel för scenario 4.



Figur 14: Positionsfel enligt test (3) med fönsterlängd på fem sampel för scenario 4.

För att undersöka hur snabbt felet växer optimerades felet mot funktionen

$$\hat{p}_{fel,i} = b \cdot (t_i - t_0)^a + p_{fel,0},$$

där b är

$$b = \frac{p_{fel,N} - p_{fel,0}}{(t_N - t_0)^a}.$$

Alltså blir $\hat{p}_{fel,i}$ förenklat

$$\hat{p}_{fel,i}(a) = \frac{(p_{fel,N} - p_{fel,0}) \cdot (t_i - t_0)^a}{(t_N - t_0)^a} + p_{fel,0},$$

där t_0 är tiden då vilseledning detekteras och t_N är tiden då GNSS åter används. I Tabell 6 visas feltillväxten och den modellerade feltillväxten för fyra scenarion och en detektorinställning.

Tabell 6: Feltillväxt utan GNSS vid vilseledning med detektor med en fönsterlängd på 20 sampel och som räknar om sitt tillstånd från 20 sampel bakåt i tiden med död räkning vid detektion.

Start [s]	Slut [s]	Tillväxtperiod [s]	Azimutfel [°]	Tid utan GNSS [s]	Feltillväxt [m]	a	Feltillväxt/s ^a
95	190	10	5	108	10.43	1.2	0.03916
95	190	80	5	93	4.29	1.3	0.01218
95	190	10	30	111	12.10	1.2	0.04343
95	190	80	30	106	9.40	1.1	0.05680

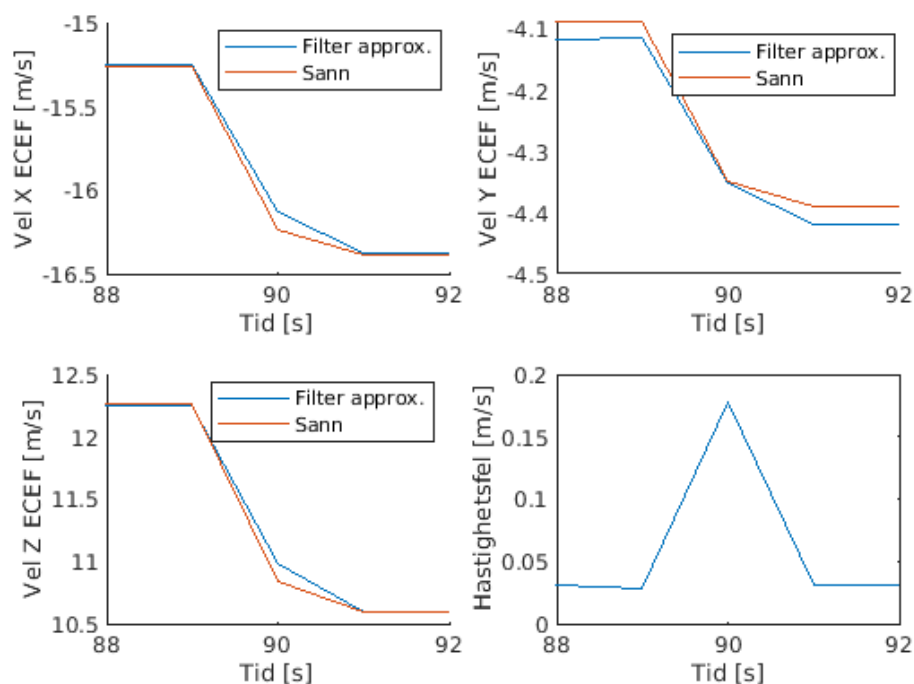
Resultaten blev bättre för den innovationsbaserade detektorn än för detektorn baserad på relativa positioner. Därför testades den innovationsbaserade detektorn i ytterligare fyra scenarier där azimutfelet växer till 1 grad, enligt Tabell 7. I dessa scenarier läggs vilseledningen på under två olika tidsperioder för att testa detektorn under olika skeenden i trajektorian. Första tidsperioden av vilseledning börjar innan en kurva. Den andra tidsperioden börjar ett par sekunder efter första kurvan och slutar ett par sekunder innan andra kurvan.

Det sker endast en attack per scenario och alltså inte flera efter varandra. Om flera attacker sker efter varandra spelar fönsterlängden på detektorn större roll. Fönsterlängden påverkar möjligheten att hinna detektera frånvaro av vilseledning och få in sanna GNSS-signaler mellan attackerna. Mottagarens beteende och benägenhet att skifta mellan att använda sanna och vilseledda GNSS-signaler kan också påverka resultaten i hög grad. Detta har dock inte utvärderats i denna studie.

Tabell 7: 4 ytterligare scenarion att pröva test (3) mot.

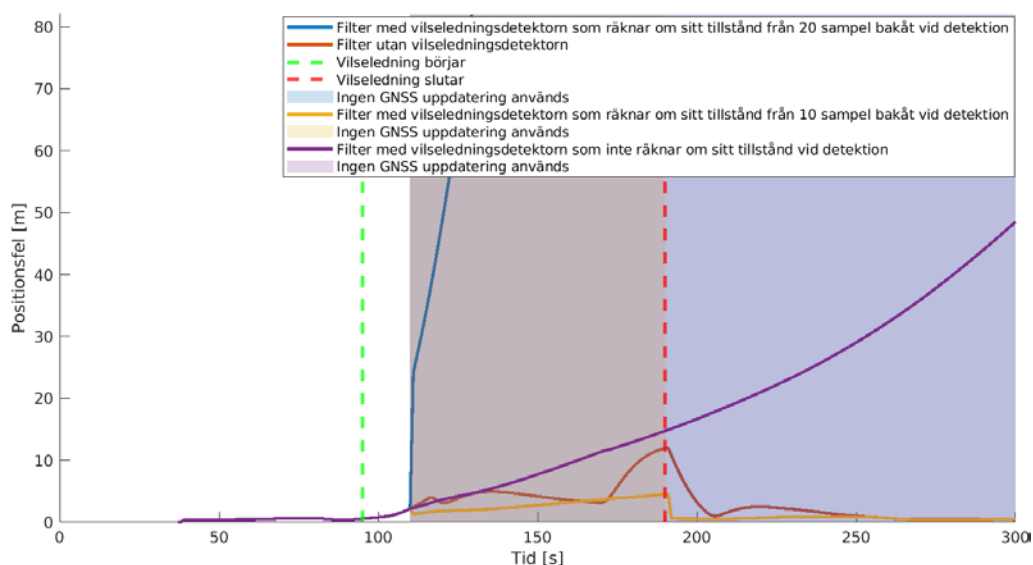
Scenario	Start [s]	Slut [s]	Tillväxtperiod [s]	Azimutfel [°]
5	95	190	10	1
6	95	190	80	1
7	125	160	10	1
8	125	160	20	1

För scenario 5 uppkommer ett intressant resultat som inte har observerats i tidigare scenarier. Där blir lösningen mycket sämre när filtrets tillstånd räknas om med död räkning från 20 sampel bakåt vid detektion. I Figur 16 visas positionsfelet för detta scenario och det är tydligt att ett större fel fås när filtrets tillstånd räknas om från 20 sampel bakåt. Detta beror troligen på att det sker en hastighetsförändring vid den tidpunkten (Figur 15).



Figur 15: Filtrets hastighets skattning nära tidpunkten 90 s för scenario 5 och inställning 6.

Initialiseringsfelets påverkan förväntas bli större då död räkning sker vid tidpunkter då hastigheten inte är konstant och speciellt när den inte är noll. För att undvika detta problem bör ett test införas för att hitta en lämplig tidpunkt, med pålitliga GNSS- och IMU-data, att börja död räkning från. Det kan göras exempelvis genom att hitta flera sampel efter varandra med konstant hastighet och börja död räkning därifrån. Detta har inte studerats vidare i denna rapport.



Figur 16: Positionsfel för scenario 5 med test (3) med fönsterlängd på fem sampel.

I Tabell 8 presenteras ytterligare en detektorinställning och Tabell 9 visar resultaten för de nya scenarierna i Tabell 7. Vilseledning detekteras även för dessa scenarier med undantag för fallet ovan beskrivet på förekommen anledning.

Tabell 8: Detektorinställningar för utvärdering av test (3) för scenario 5-8 i Tabell 7.

Detektor-inställning	Metod	Fönsterlängd	Antal sampel bakåt död räkning börjar vid detektion	Tröskel
9	(3)	5	10	1

Tabell 9: Resultat med vilseledningsdetektion enligt test (3).

Scenario se Tabell 7	Detektor-inställning se Tabell 4 och Tabell 8	Första larm [s]	Mottagarfel vid larm [m]	RMSE [m]	Tid från attack är slut tills GNSS används oavbrutet [s]	Största positions-fel [m]
5	-	-	-	4	-	12
6	-	-	-	4	-	8
7	-	-	-	1	-	5
8	-	-	-	1	-	6
5	6	110	3	931	Aldrig	2319
5	9	110	3	2	0	5
5	5	113	4	2	5	6
6	5	117	4	2	20	6
7	5	131	1	1	20	3
8	5	132	1	1	20	3
5	8	110	3	20	Aldrig	49
5	7	113	4	28	Aldrig	66
6	7	117	4	9	Aldrig	22
7	7	131	1	10	Aldrig	24
8	7	132	1	9	Aldrig	24

6 Diskussion

För att realisera modulära och robusta PNT-system krävs möjlighet att övervaka osäkerheter och integritet för varje modul (sensor eller delsystem) i systemet. I detta avsnitt diskuteras flera aspekter av prestanda och framtida utveckling av de detektorer som har utvärderats för undertryckning av GNSS-vilseledning med stöd av INS.

6.1 Test baserat på relativ rörelse

Vi har visat att vilseledning kan upptäckas med de använda detektorinställningar för test (1), vilket är baserat på jämförelse av rörelse mellan GNSS och INS, i de utvärderade scenarierna. Dock har sådana test svagheten att de bara jämför rörelser inom ett observationsfönster och inte med information innan detta tidsintervall. Därmed kommer information om den sanna positionen vid vilseledningsdetektion inte att utnyttjas vid attacker som är längre än observationsfönstret, eftersom tidpunkten för denna position ligger utanför fönstret. Om den vilseledda mottagaren rör sig likt den sanna trajektorian ökar risken för att inkludera falska positioner i navigeringsfiltret, vilket har observerats i denna studie. Risken för falsklarm är också förhöjd då vilseledningen stängs av, eftersom en snabb förflyttning sker i mottagaren till de sanna GNSS-signalerna. Detta gör att en normal rörelse bedöms som vilseledning när mottagaren återfår de sanna GNSS-signalerna.

En potentiell vidareutveckling av testet (1), för att förbättra prestanda vid återtagande av de sanna GNSS-signalerna, är att använda variabel fönsterlängd. Detta kan exempelvis göras genom att låta fönsterlängden växa efter vilseledningsdetektion för att jämföra med positionen vid detektionen under hela tidsperioden som GNSS exkluderas. För detta behövs vidare studier av hur teststatistiken (1) varierar beroende på fönsterlängd.

I denna utvärdering har INS-lösningen initialiserats från stillastående, utan uppdatering därefter. Alternativa sätt är exempelvis att initialisera från ett tidigare tillstånd i filtret eller från flera efterföljande mottagarmätningar genom att skatta orientering och hastighet från dem.

Vid långsammare feltillväxt bör också bias skattas. Detta bör göras under ett pålitligt tidsintervall när mottagaren inte är påverkad av vilseledning. Om bias skattas medan mottagaren är utsatt för vilseledning kan bias-skattningen göra mer skada än nytta, eftersom fel introduceras i filtret. Dessa åtgärder kan motverka den feltillväxt som har observerats i test (1) till följd av IMU-fel.

6.2 Innovationsbaserat test

Innovationsbaserat test av typen (3) har visat bra resultat i de utvärderade scenarierna. En viktig åtgärd har visats vara att räkna om filtrets tillstånd med död räkning från en tidpunkt innan detektion av vilseledning. Utan denna åtgärd detekteras inte när vilseledning upphör, så att mottagarpositionen kan nyttjas återigen. Detta beror på att teststatistikens värde inte minskar tillräckligt för att vara under beslutströskeln efter att attacken har upphört. Några anledningar till detta är sämre skattning av position samt en för liten skattad osäkerhet till följd av att filtret har uppdaterats med flera mottagarpositioner under påverkan av vilseledning. Utvärderingen har också visat att filterlösningen kan få ett stort och snabbt växande fel om filtret börjar dödräkna från en tidpunkt som råkar ha stor osäkerhet i hastighet och orientering, exempelvis när hastigheten ändras kraftigt. För att minska risken för initialiseringsfel när GNSS exkluderas och endast INS används bör tidpunkten då död räkning påbörjas väljas med varsamhet. Detta kan göras exempelvis genom att identifiera tidigare tidsintervall då hastigheten är konstant, så att initialvärdena vid starten av död räkning har låg osäkerhet.

Vidare bör kovariansen för mottagarmätningarna undersökas och skattas bättre. I denna utvärdering används den precision som U-blox-mottagaren anger, vilket är kring 3 m för varje axel i ECEF-koordinatsystemet, men 2-3 m större än positionsfelet. Med en bättre skattning, i detta fall lägre, kovarians blir teststatistiken (3) mer överensstämmande med empiriska mätdata (och eventuellt mer lik den teoretiska approximationen).

Fönsterlängden är en kompromiss på så sätt att ett långt fönster övervakar ett längre tidsintervall och därmed inte inkluderar falska positioner om deras rörelse korsar filtrets lösning över få sampel. Samtidigt ger stor fönsterlängd en fördröjning tills mottagarpositionen återigen används efter att vilseledningen har stängts av.

6.3 Framtida arbete

Mottagarpositionerna för vilseledning har skapats syntetiskt i denna studie, och därför inte inkluderat alla egenskaper hos en riktig GNSS-mottagare. Exempelvis har positioner generats i varje tidssteg oavsett vilseledning eller inte, och övergångarna från vilseledning tillbaka till de sanna GNSS-signalerna har skett genom en momentan förflyttning. En riktig mottagare beter sig ofta inte så, utan konvergerar under en tidsperiod mot de sanna GNSS-positionerna. Innan mottagaren konvergerar mot en ny positionslösning kan den följa både sanna och falska satellitsignaler, och ofta inte beräkna någon position alls under en period. Likaså kan en mottagare vara utan GNSS under perioder med varierande kvalitet på mätningar, exempelvis i tät stadsmiljö med höga byggnader, inomhus eller om den blir utsatt för störning. Därför bör en detektor enligt test (3) eller en vidareutveckling av test (1) ha en dynamisk fönsterlängd beroende på hur ofta mottagarmätningar beräknas eller när GNSS är tillgängligt under dessa perioder. Realistiska beteenden hos mottagare bör beaktas i framtida studier, exempelvis genom hårdvarusimuleringar med GNSS-simulator eller med data från verkligheten i störda miljöer och miljöer med varierande kvalitet på signalerna.

Vidare bör detektorerna undersökas med olika tröghetssensorer som har större och mindre sensorfel, samt hur detta påverkar teststatistiken. Bland annat bör studeras, med olika tröghetssensorer, hur positionsfelet växer utan GNSS och om innovationen och dess osäkerhet växer korrelerat för det innovationsbaserade testet (3).

Hur osäkerheten hos filtret och innovationen påverkar prestanda väcker ytterligare intressanta frågor som bör studeras. Exempelvis:

- När är osäkerheten så stor att sannolikheten för att inkludera de sanna GNSS-signalerna är lika stor som att ta in en vilseledd position?
- Hur relaterar osäkerheten hos IMU:n till hur små avvikelser hos vilseledningen som kan upptäckas för att exkludera eller återta de sanna GNSS-signalerna?

En lösning som kan förbättra prestanda är att nyttja hastighetsskattningar från andra sensorer, till exempel odometrisensorer eller Doppler-hastighet, för att korrigera hastigheten i filtret och få en långsammare feltillväxt under perioder utan GNSS. Sådana uppdateringar kan också ge mindre och långsammare växande osäkerhet kring filtrets tillstånd.

7 Slutsatser

För att möjliggöra modulära och robusta PNT-system är det nödvändigt att inkludera integritetsövervakning av varje modul (sensor eller delsystem) i systemet. Denna rapport visar att vilseledning av GNSS-mottagare kan upptäckas med de utvärderade detektionsalgoritmerna, med stöd av INS. Att upptäcka starten på vilseledning fungerar bra med alla utvärderade detektionsmetoder. Att upptäcka när vilseledningen slutar, så att korrekt mottagarposition återigen kan användas, är mer utmanande speciellt för de utvärderade detektorerna baserat på jämförelse av relativ rörelse mellan mottagar- och INS-positioner. Innovationsbaserad detektion fungerar ofta bättre i de utvärderade scenarierna än metoden som baseras på relativ rörelse. Den innovationsbaserade detektorn tar inte in vilseledning efter detektion men har en viss fördröjning, på grund av observationsfönstret längd, innan GNSS tas in igen efter attackernas slut.

Osofistikerade fall av vilseledning, då positionen avviker kraftigt under kort tid från den sanna positionen, är relativt lätta att upptäcka och därmed att exkludera ur filterlösningen. Mer sofistikerade attacker, då vilseledningspositionen avviker gradvis under längre tid är svårare att hantera. Ofta upptäcks sådana attacker först en tid efter att de påbörjas. Därför bör mottagarpositionen exkluderas ur filterlösningen redan innan attacken upptäcks. Hur långt tillbaka filtret bör räknas om beror på flera faktorer, bl.a. längden på observationsfönstret, vilseledningens karaktär och kvalitet på tröghetssensorer. Detta har till viss del utvärderats i denna rapport, men bör studeras vidare.

Utvärderingen har också visat att filterlösningen kan få ett stort och snabbt växande fel om filtret börjar dödräkna från en tidpunkt som råkar ha stor osäkerhet i hastighet och orientering, exempelvis när hastigheten ändras kraftigt. För att minska risken för initialiseringsfel när GNSS exkluderas och endast INS används bör tidpunkten då död räkning påbörjas väljas med varsamhet. Detta kan göras exempelvis genom att identifiera tidigare tidsintervall då hastigheten är konstant, så att initialvärdena vid starten av död räkning har låg osäkerhet.

I detta arbete har vi uteslutit metoder för att, oberoende av INS, upptäcka vilseledning eller förbättra skattningen av precision i GNSS-mottagare. Att nyttja fler typer av data från mottagaren, liksom att nyttja ytterligare sensorer för t.ex. odometri, i kombination med INS bör studeras ytterligare.

8 Referenser

- [1] C. Tanil, "Detecting GNSS spoofing attacks using INS coupling," Illinois Institute of Technology, Chicago, USA, 2016.
- [2] j. D. Quartararo och S. E. Langel, "Detecting Slowly Accumulating Faults Using a Bank of Cumulative Innovations Monitors in Kalman Filters," *NAVIGATION: Journal of the Institute of Navigation*, vol. 69, nr 1, 2022.
- [3] B. Kujur, S. Khanafseh och B. Pervan, "Optimal INS Monitor for GNSS Spoofer Tracking," *NAVIGATION: Journal of the Institute of Navigation*, vol. 71, nr 1, 2024.
- [4] B. Sun, Z. Zhang, D. Qiao, X. Mu och X. Hu, "An Improved Innovation Adaptive Kalman Filter for Integrated INS/GPS Navigation," *Sustainability*, vol. 14, p. 11230, 2022.
- [5] B. Gao, G. Hu, Y. Zhong och X. Zhu, "Cubature Kalman Filter With Both Adaptability and Robustness for Tightly-Coupled GNSS/INS Integration," *IEEE Sensors Journal*, vol. 21, nr 13, pp. 14997-15011, 2021.
- [6] D. Sabzevari och A. Chatraei, "INS/GPS Sensor Fusion based on Adaptive Fuzzy EKF with Sensitivity to Disturbances," *IET radar, sonar & navigation*, pp. 1535-1549, 11 2021.
- [7] R. Sun, J. Wang, Q. Cheng, Y. Mao och W. Y. Ochieng, "A new IMU-aided multiple GNSS fault detection and exclusion algorithm for integrated navigation in urban environments," *GPS Solutions*, vol. 25, nr 4, p. 147, 2021.
- [8] C. Tanil, S. Khanafseh, M. Joerger och B. Pervan, "An INS Monitor to Detect GNSS Spoofers Capable of Tracking Vehicle Position," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 54, nr 1, pp. 131-143, 2018.
- [9] C. Tanil, S. Khanafseh, M. Joerger och B. Pervan, "Kalman filter-based INS monitor to detect GNSS spoofers capable of tracking aircraft position," i *IEEE/ION Position, Location and Navigation Symposium (PLANS)*, Savannah, GA, USA, 2016.
- [10] Z. Clements, J. E. Yoder och T. E. Humphreys, "Carrier-phase and IMU based GNSS Spoofing Detection," i *The International Technical Meeting of the The Institute of Navigation*, Long Beach, California, 2022.
- [11] J.-H. Lee, K.-C. Kwon, D.-S. An och D.-S. Shim, "GPS spoofing detection using accelerometers and performance analysis with probability of detection," *Int. J. Control Autom. Syst.*, vol. 13, nr 4, pp. 951-959, 2015.
- [12] S. Lo, Y. H. Chen, T. Reid, A. Perkins, T. Walter och P. Enge, "The Benefit of Low Cost Accelerometers for GNSS Anti-Spoofing," i *ION Pacific PNT Meeting*, Honolulu, Hawaii, 2017.
- [13] J. T. Curran och A. Broumendan, On the use of Low-Cost IMUs for GNSS Spoofing Detection in Vehicular Applications, 2017.
- [14] Z. Feng, N. Guan, M. Lv, W. Liu, Q. Deng, X. Liu och W. Yi, "Efficient drone hijacking detection using onboard motion sensors," i *Design, Automation & Test in Europe Conference & Exhibition (DATE)*, Lausanne, Schweiz, 2017.

- [15] P. F. Swaszek, S. A. Pratz, B. N. Arocho, K. C. Seals och R. J. Hartnett, "GNSS Spoof Detection Using Shipboard IMU Measurements," i *ION GNSS+*, Tampa, Florida, 2014.
- [16] A. Broumandan och G. Lachapelle, "Spoofing Detection Using GNSS/INS/Odometer Coupling for Vehicular Navigation," *Sensors*, vol. 18, nr 5, 2018.
- [17] M. Ceccato, F. Formaggio, N. Laurenti och S. Tomasin, "Generalized Likelihood Ratio Test for GNSS Spoofing Detection in Devices With IMU," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 3496-3509, 2021.

