Hvor robust er losenes navigasjonsutstyr?

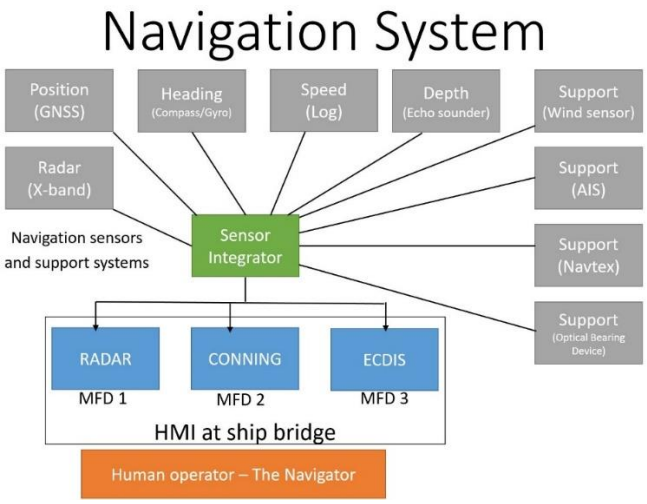
S. Nyhamn, G. Pettersen[1] and O.S. Hareide[1,2]
[1]Kystverket lostjenesten
[2]Institutt for havromsoperasjoner og byggteknikk, NTNU

Abstrakt – I det maritime domenet, og på skipsbroen, er det en økende avhengighet av elektronisk navigasjon, spesielt automatisk posisjonering fra GNSS. Kystverket lostjenesten skal besørge sikker seilas for lospliktige fartøy i norske farvann, og den losfaglige kompetansen beror både på tradisjonelle og elektroniske hjelpemidler. Økt bruk av elektroniske hjelpemidler for posisjonering introduserer også en potensiell økt sårbarhet. Artikkelen analyserer resultatene av test av sårbarhet på losenes utstyr. Grunnlaget for analysen var en test initiert av Statens vegvesen der Forsvarets Forskningsinstitutt (FFI) gjennomførte jamming og spoofing av sensorene som losene bærer med seg om bord. Dette er utstyr som kommer i tillegg til skipets utstyr. Kystverket lostjenesten benytter seg av personlig standardutstyr (ADQ2+) og høyytelsessensorer (XR2) levert av AD Navigation. Utstyret ble utsatt for jamming og narring og det ble oppdaget at sensorer som kun inneholder GPS L1 er mye mer sårbart enn enheten som inneholder flere GNSS bånd (XR2). XR2 opererer på et bredere frekvensspektrum og har dermed mer motstandskraft og holder lengre i et miljø med interferens.
Det ble belyst at nøyaktig posisjonsbestemmelse ved RTK og prosessering av retning (heading) er mer sårbart enn å prosessere en pseudo-range posisjonsløsning. Det er også forskjell på hvorledes de forskjellige kartsystemene viser verdier og alarmer som er forårsaket av interferens. Ingen alarmer gir et varsel om mulig interferens.
Testen ga et godt grunnlag for innovasjonsprosjektet som skal utvikle et mer robust system for Kystverkets loser.

Søkeord
GNSS sårbarhet, Jamming, Spoofing, Narring, Los, Navigasjonssensorer, Kystverket, Innovasjon, Navigasjonsteknologi.

Bakgrunn

Maritim navigasjon har gjennomgått et paradigmeskifte de siste tiårene med innføring av elektronisk navigasjon (Norris, 2010). Elektronisk navigasjon er alle hjelpemidler knyttet til navigasjon som går på strøm, og det mest kjente er av mange elektroniske kartsystem. Electronic Chart Display and Information System (ECDIS) har blitt godkjent av IMO for papirløs navigasjon. På moderne skip er det i dag avanserte integrerte navigasjonssystemer (Figur 1) som kobler sammen flere sensorer som til slutt presenteres på et display, gjerne kjent som Multi Function Display (MFD). Innføringen av papirløs navigasjon har utvilsomt bidratt til økt sjøsikkerhet (Weintrit, 2009), samtidig som det har ført til en ny type ulykker. Maritime Investigation Accident Board (MAIB) omtaler dette som ECDIS-assisterte ulykker (MAIB, 2014), og er i stor grad relatert til manglende systemforståelse og høy tillit til posisjonen som er presentert av det valgte elektroniske posisjoneringssystemet. I det maritime er det hovedsakelig posisjon levert av NAVSTAR GPS (IMO, 2007), men det er også mottagere som benytter multikonstellasjons Global Navigation Satellite Systems (GNSS) sammen med støtte fra differensiell satellittnavigasjon som; Differential GPS (DGPS), Satellite-based Augmentation Systems (SBAS) og Ground Based Augmentation System (GBAS) (Hofmann-Wellenhof, 2008).

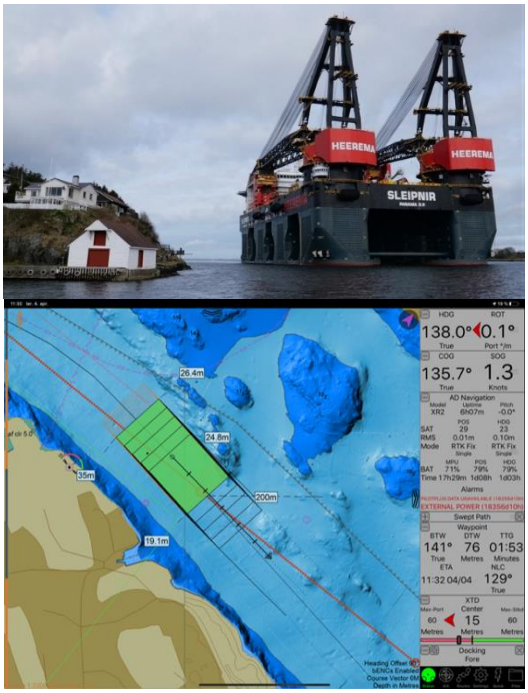


Figur 1: Prinsippskisse integrert navigasjonssystem

Sårbarheten knyttet til GNSS ble først anerkjent i Volpe-rapporten fra 2001 (Volpe, 2001), som konkluderer med at samfunnet er generelt sett avhengig av globale navigasjonssatellittsystem (GNSS). Det er i ettertid kommet en rekke rapporter som påpeker de samme utfordringene, blant annet fra The Royal Academy of Engineering (RaENG,

2011) og Norsk Romsenter (NRS, 2013). I det maritime domenet er det de siste årene blitt et økt fokus på sårbarheten til posisjonsbestemmelse fra GNSS, blant annet gjennom rapporter om både narring og jamming av posisjon til skip fra Svartehavet, Middelhavet, Østersjøen og andre plasser. Et forskningsprosjekt utført av Texas University viste at de endret kurs til et cruiseskip i Middelhavet (Psiaki & Humphreys, 2016).

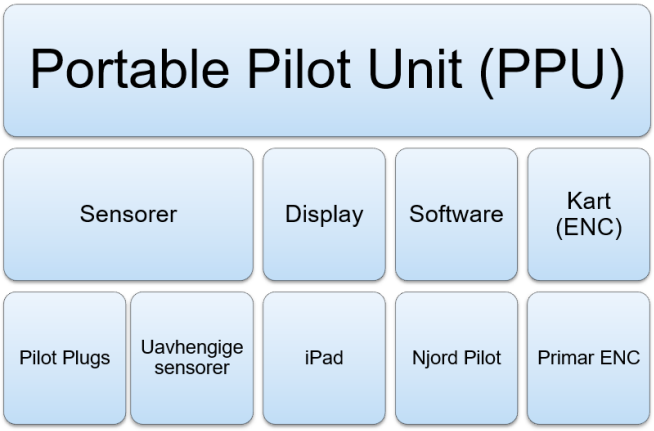
Kystverket lostjenesten bidrar til å trygge ferdselen på sjøen og verne om miljøet ved å tilføre fartøyets mannskap nødvendig farvannskunnskap. Losen er kapteinens nautiske veileder i navigering og manøvrering. Selv om losen i dag har tilgang til stadig mer avanserte digitale verktøy, er det fremdeles kompetanse rundt farled og kyst, værforhold og seilingsrutiner som er hovedproduktet som tilbys fra losen og Kystverket. Lostjenesten utfører omlag 40 000 oppdrag per år (Kystdatahuset.no), og har 7 losoldermannskap og 25 losstasjoner i Norge, fra Halden til Kirkenes. Oppdragene varierer i kompleksitet, fra korte losinger til havn og til mer komplekse operasjoner med små marginer (uvanlige losoppdrag).



Bilde 1: Eksempel på spesialoppdrag er kranfartøyet Sleipnir sitt anløp i Haugesund

På normale eller rutineoppdrag, er losen tjent med nøyaktigheten en PPU gir. Noen ganger er marginene små og losen må dimensjonere utstyret deretter. Dette kalles uvanlige losoppdrag eller spesialoppdrag (Bilde 1). Disse jobbene krever planlegging og koordinering i form av møtevirksomhet i forkant. Dette for å fastsette maksimum grense for vær, vind og sikt, eller minimum klarering til bunn eller land.

Samtidig ser Kystverket lostjenesten en økende etterspørsel etter at losene bidrar med veiledning og støtte også innenfor elektronisk navigasjon. Dette har ført til at losen har med seg Portable Pilot Unit (PPU) på losoppdrag (Figur 2). Portable Pilot Unit er et samlebegrep for utstyret som losen har med seg ombord, og består av tre hovedkomponenter; Sensor, display og programvare. Denne artikkelen vil også sette søkelys på PPU Sensorer for å se om det kan være nyttig i forbindelse med utvikling av neste generasjons høyytelse PPU sensor for Kystverket lostjenesten.



Figur 2:Oppbygning av losens støttesystem, Portable Pilot Unit (PPU)

Innledning

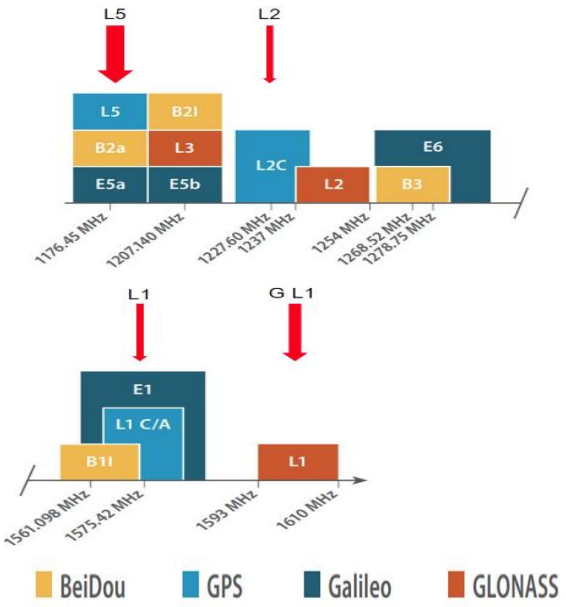
Lostjenesten skal gjennom et innovasjonspartnerskap utvikle fremtidens støtteverktøy for lostjenesten (IA, 2020) i perioden 2020-2023, og deltok i september 2021 på en jammetest der dagens utstyr ble utsatt for signalinterferens.

Målet med testen var å utforske hvor sårbart eksisterende navigasjonssensorer (PPU sensor) er, samt identifisere hvordan dette påvirker navigasjonssystem (PPU software - Njord Pilot og SeaIQ) som er mest brukt av losene.

I tillegg var målsetningen å undersøke om noe av denne lærdommen kunne brukes som innspill til innovasjonspartnerskapet, der neste generasjon støttesystem for lostjenesten skal utvikles.

Gjennomføring

Testene var ledet av Statens Vegvesen der hovedfokus var sensorer i biler. Sensorene som losene bruker, ble derfor satt på en bil (se bilde 2) for å simulere hvordan de monteres om bord på et lospliktig fartøy.



Figur 3: GNSS frekvenser og bånd. Rød pil er bånd som kunne jammes. (Kilde FFI)

Bilde 2: Losens sensorer plassert på bil

FFI var ansvarlig for sender utstyr og hadde mulighet å jamme på frekvensene beskrevet i Figur 3. Tabell 1 viser at XR 2 bruker flere bånd enn de som var mulig å jamme på. Det er verdt å merke seg at noen av frekvensene i de bånd som ikke ble jammet på er lik, eller ligger nær de bånd som det ble jammet på, for eksempel GLO L2 som er nær GPS L2 og GPS L2C som er samme området som GPS L2. Båndene kan imidlertid ha forskjellig struktur som gjør at de kan påvirkes forskjellig.

Frekvens bånd	Senterfrekvens MHz	PRN rate MHz	ADQ2+ 1561-1610	CatRot 1561-1610	XR2 1207-1256 1561-1610	Garmin 1561-1610
Mulige Jamme freq						
GPS L1	1575.42	1	X	X	X	X
GLO L1	1601.72	5			X	
GPS L2	1227.6	1			X	
GPS L5	1176.45	10			X	
Ikke jammet bånd som XR 2 bruker						
GLO L2	1598-1609				X	
GPS L2C	1227.6	Samme freq som GPS L2			X	
Galileo E1	1575.42	Samme freq som GPS L1			X	
Galileo E5b	1207.14				X	
Beidou B1I	1561.098	Nært GPS Ll			X	
Beidou B2I	1207.14	Nært GPS L5			X	

Tabell 1: Frekvenser det var mulig å jamme på sammen med oversikt over hvilke bånd sensorene bruker (GLO=Glonass)

I de fleste moderne jammere er det mulig å generere forskjellige jamme signaler og bølgeformer. Forskjellen mellom jammersignal og jammerbølgeform er at bølgeform består av flere jammersignaler som representerer en sekvens av jamme signal på ønsket frekvens.

Jammetyper som ble brukt var Continous Wave (CW) og Pseudorandom Noise (PRN). CW betyr at jammesignalet svinger med en fast frekvens, mens PRN er jamming med et signal som har omtrent

samme form (i frekvensspekteret) som de ekte signalene fra satellittene. PRN kalles også bredbåndsjamming.

Alle sensorer (Bilde 3), 5 i alt (1 håndholdt Garmin, bilens system og 3 iPader med tilkoblede PPU sensorer) var satt opp på alle testene. Garmin mottaker ble brukt da den har et bilde med skyplott (bilde over satellitter på himmelen) og signal støyforhold som er nyttig. Bilens mottaker ble også brukt som referanse da den hadde visning av antall satellitter.

Bilde 3: 3x iPad med kartsystem, Garmin og bilens kartsystem

Det ble lagt opp til flere forsøk med forskjellige parameter som ga et godt grunnlag for en bred test av losens sensorer.

Losens sensorer og kartprogram

Til vanlige losoppdrag benytter losene ADQ-2+ PPU (Portable Pilot Unit Sensor - PPU Sensor), levert av AD Navigation. Denne kobles til skipets AIS med en pilotplug (ledning). ADQ2+ videresender skipets posisjon (fra skipets GPS), antenne offset, fysiske dimensjoner og AIS mål, via Wifi. I tillegg har ADQ2+ en innebygget GPS og en ROT (Rate of turn) sensor. I praksis benyttes kun ROT fra ADQ2+ og resten er fra skipets AIS via pilotplug.

Bilde 5: ADQ2+ og de tre enhetene i XR2

Til uvanlige losoppdrag (spesialoppdrag) hvor det er større krav til nøyaktighet i posisjon, benyttes XR2. Denne er også levert av AD Navigation og består av tre PPU sensorenheter.

XR2 systemet er et uavhengig og vesentlig mer nøyaktig enn ADQ2+. Til posisjon benyttes en multifrekvens mottaker med alle konstellasjoner (GPS/Glonass/BeiDou/Galileo). De tre boksene kommuniserer seg imellom via UHF. Master Processing Unit (MPU) (Bilde 4) boksen prosesserer all data og videresender denne via Wifi.

XR2 bruker to av enhetene til å frembringe heading og har RTK kapasitet for bedre nøyaktighet (se kapittel; Multikonstellasjon og multifrekvensmottaker XR2).

Bilde 4: Kartprogram Njord Pilot

Kartprogrammet som losene benytter er Njord Pilot (Bilde 4) levert av SevenCs.
Dette programmet kjøres på iPad (iOS), som er losenes arbeidsverktøy. Under testene ble også programmet SeaIQ benyttet, da det er utbredt internasjonalt samt har mer informasjon og verdier som er nyttig under jamming og spoofing. For eksempel var funksjonen; *Sammenligne Ext NMEA med innebygget GPS* nyttig under spoofing angrep, for å enkelt kunne sammenstille visuelt posisjonene gitt av to ulike posisjonskilder.

Funn

Innledning

Alle testene ble styrt av FFI som genererte jamming eller spoofing enten på alle frekvensene samtidig eller en frekvens etter den andre. Testen ble enten gjort med maksimal utgangseffekt eller stegvis opp eller ned. Jammer var alltid stasjonær. Ved kun en av testene var sensorene i bevegelse, ellers stasjonære. Logging ble gjort ved å notere fortløpende. Elektronisk logging ble gjort med screen grabber og logging av NMEA data på PC via loggeprogrammet Tera Term. Det var direkte samband med FFI som opplyste tid og hva som ble initiert. Observasjon av sensorene ble gjort av to personer.

Test 1; CW jamming, økende frekvensbånd

I test 1 ble det jammet på CW i sekvens GPS L1 - GLO L1 - GPS L2 - GPS L5, deretter motsatt rekkefølge. Avstanden til jammer var 17 meter og utsendt effekt var 0,1 watt som var maksimum jammeeffekt. Sensorer og jammer var stasjonær.

Allerede ved jamming av GPS L1 var alle sensorene som kun baserer seg på GPS L1 slått ut. XR 2 som har flere bånd og frekvenser opprettholdt posisjonsbestemmelse (Tabell 2).

	GPS L1	GLO L1	GPS L2	GPS L5	Garmin	Catrot	XR2	ADQ2+
09:53	X				Ikke fix	Ikke fix	fix	Ikke fix
09:57	X	X			Ikke fix	Ikke fix	fix	Ikke fix
10:00	X	X	X		Ikke fix	Ikke fix	fix	Ikke fix
10:02	X	X	X	X	Ikke fix	Ikke fix	fix	Ikke fix

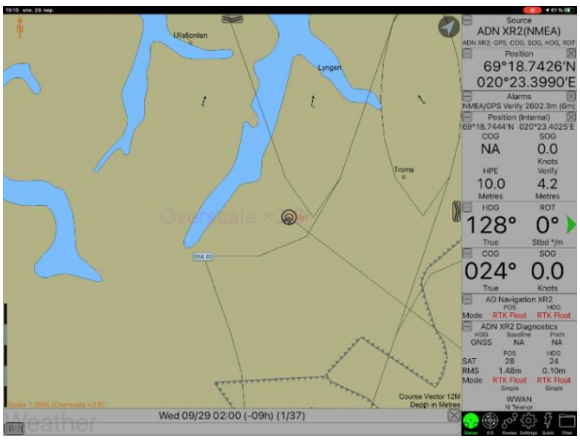
Tabell 2:Resultat jamming ved å legge til nye bånd, men start på GPS L1(X betyr at bånd blir jammet)

Noen indikasjoner på problemer også på XR 2 kom også når alle 4 bånd var jammet, men den holdt posisjonsbestemmelse.

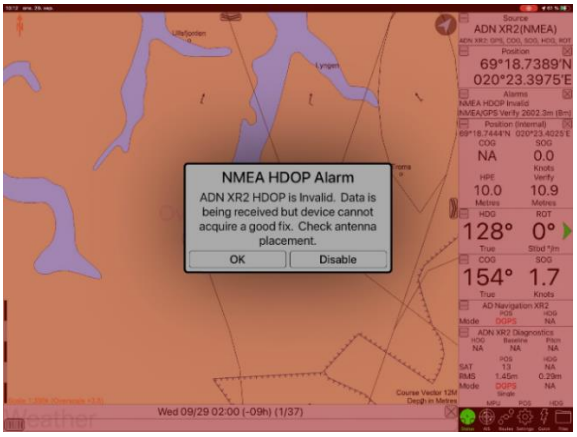
Når alle bånd var jammet begynte del to av testen der båndene ble jammet i motsatt rekkefølge (start med GPS L5). Resultatet ble da litt annerledes da XR2 fikk problemer med RTK allerede ved jamming av GPS L2 og RTK fikk problemer ved jamming av GLO L1 (Tabell 3).

	GPS L1	GLO L1	GPS L2	GPS L5	Garmin	Catrot	XR2	ADQ2+
10:07				X	fix	fix	fix	fix
10:09			X	X	fix	fix	fix	fix
10:10		X	X	X	fix	fix	fix RTK probl	fix
10:12	X	X	X	X	Ikke fix	Ikke fix	fix, RTK probl, få sat, alarmer	Ikke fix

Tabell 3:Resultat jamming ved å legge til nye bånd, start på GPS L5



Bilde 6: Skjemdump SeaIQ. Tid 10:10 Ustabil og i mode RTK Float



Bilde 7: Skjermdump SeaIQ. Tid 1012, viser RTK float, ikke Fix, Heading Ok på grunn av backup

Dette kan indikere at XR2 bruker GPS L2 eller GLO L1 for å få RTK løsning. Da GPS L1 også forvant mistet alle de andre fix (posisjon) men XR2 slet betydelig mer enn ved forrige test, noe den alarmerte om.

Etter dette ble samme test gjennomført, men jammesignalet var PNR, bredbånd (se kapittel; Gjennomføring på side 3). Den samme utviklingen skjedde her, men XR2 mistet helt posisjon ved jamming av det tredje og fjerde båndet uansett hva som startet først.

Testen viste dermed at PNR jamming gikk hardere utover multikonstellasjons- og multifrekvens-mottaker XR 2 enn CW jamming.

Test 2; PNR Jamming, Gradvis økning av effekt

Test 2 startet med lav effekt; 85dB demping med 5 dB steg. Signalet var PRN og det var jamming på alle 4 bånd. Denne testen ville gi indikasjoner på hvordan systemene påvirkes av svak jamming og hvilke indikasjoner som kommer først.

Oppsettet på sensorer og kartprogram var som tidligere. Sensorer og jammer var stasjonære.

Dempning	Tid	GPS L1	GLO L1	GPS L2	GPS L5	Garmin	Catrot	XR2	ADQ2+
85 db demp	11:13:07	X	X	X	X	fix	fix	fix	fix
80 db demp	11:14:35	X	X	X	X	fix	fix	fix	fix
75 db demp	11:17:29	X	X	X	X	fix	fix	fix	fix
70 db demp	11:17:29	X	X	X	X	fix	fix	fix	fix
65 db demp	11:21:11	X	X	X	X	fix	fix, HDOP 1,5	fix	fix
60 db demp	11:24:41	X	X	X	X	fix	fix, HDOP 1,5	fix HDOP 0,6	fix
55 db demp	11:25:06	X	X	X	X	fix	fix, HDOP 1,6	fix HDOP 0,6	fix
50 db demp	11:26:22	X	X	X	X	fix	fix, HDOP 1,1	fix HDOP 0,6	fix
45 db demp	11:25:56	X	X	X	X	fix	fix, HDOP 1,2	dårlig fix RTK probl	fix
40 db demp	11:32:02	X	X	X	X	svak fix	fix drop i SNR	fix	fix
35 db demp	11:33:38	X	X	X	X	svak fix	fix drop i SNR	fix	fix
30 db demp	11:27:11	X	X	X	X	Ikke fix	fix drop i SNR HDOP 1,6	fix HDOP 0,6	fix
20 db demp	11:41:00	X	X	X	X	Ikke fix	Ikke fix	fix HDOP 0,7	fix, svak
10 db demp	11:46:00	X	X	X	X	Ikke fix	Ikke fix	fix HDOP 2,1	Ikke fix
5 db demp	11:49:00	X	X	X	X	Ikke fix	Ikke fix	pos, Heading er borte,Hopper i pos	Ikke fix
0 db demp	11:57:00	X	X	X	X	Ikke fix	Ikke fix	Ikke fix	Ikke fix

Tabell 4:Resultat PNR Jamming med gradvis reduksjon i dempning

Tabell 4 viser at det allerede ved 65dB dempning kom indikasjoner på en høyere HDOP verdi på Catrot. XR2 som har mange flere satellitter å velge mellom har derimot ikke noe problem med HDOP. Garmin og ADQ2+ hadde muligens høyere HDOP verdi, men dette vises ikke på kartprogrammet. Ved 45 dB demping ble det noe problem med RTK og noe dårligere fix. Dette kom seg imidlertid etter noen sekunder. Ved 40dB demping som tilsvarer 10 mikrowatt utsendt effekt viste også Catrot og Garmin en nedgang i signal-støyforhold fra ca 40dB til ca 25dB som er på grensen til å klare å frembringe posisjon. Ved dempning 30 til 10dB (10 db demping =10 milliwatt effekt) mistet som forventet GPS L1 mottakerne fix. Etter det forsvant heading fra XR2, posisjonen ble ustabil og til slutt var den også helt jammet ut tilsvarende de andre testene.

Også her håndterte XR2 interferens best. Den får først problemer med RTK så litt høyere HDOP, mister heading og posisjon til slutt.

Test 3; Spoofing (narring)

Test 3 gikk ut på å narre tid og posisjon på GPS L1. Det var først 5 min jamming etterfulgt av Spoofing angrep på GPS L1. Både tiden på posisjon ble forfalsket og sendt til mottakerne. Plassering var det samme som i forrige test.

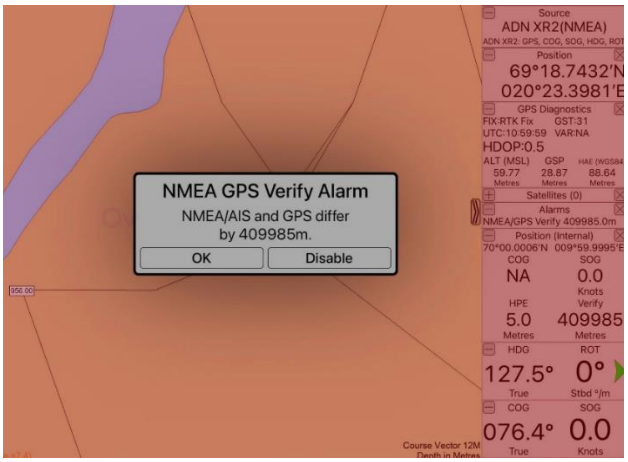
Etter 5 min jamming var posisjon borte fra alle enheter deretter ble spoofing satt i gang på GPS L1

Type PPU	CatRot	ADQ2+	XR2
Spoofet	Ja	Ja	Nei
iPad med SIM kort	Ja	Ja	Nei
Intern iPad GPS spoofet	Nei	Nei	Ja

Tabell 5; Viser om enhetene ble spoofet eller ikke

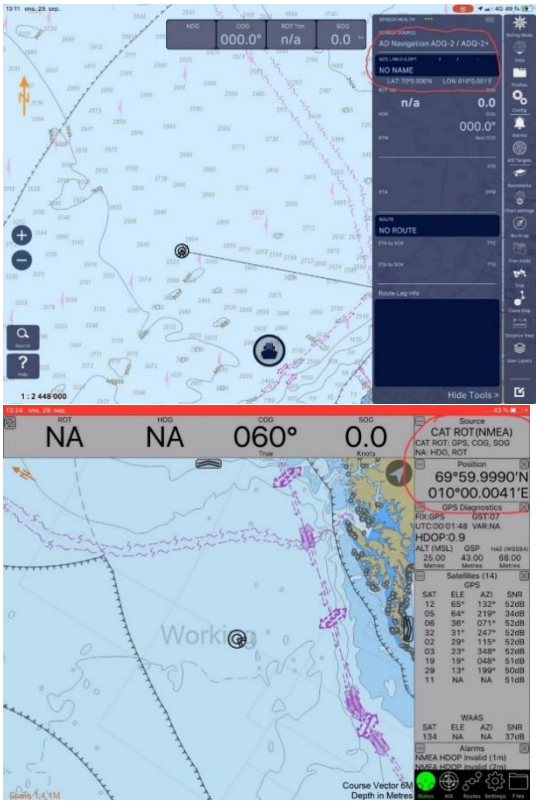
I stort ble alle som er avhengig av GPS L1 spoofet (Tabell 5). XR2 ble ikke spoofet men viste alarm om at den interne GPSen i iPaden var vesentlig forskjellig fra XR2 sensorene (Bilde 6).

Det visste seg svært nyttig å få en alarm som visste avvik mellom intern (innebygget GPS iPad) og ekstern PPU (Bilde 6).



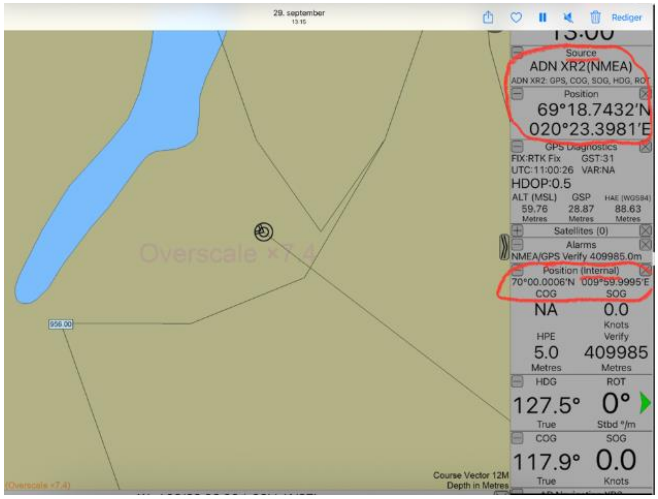
Bilde 6: Skjermdump SeaIQ. Alarm om forskjell på intern GPS og XR2 sensorer

Alarmen var nyttig, men det burde også være en alarm om at pos på GPS L1 ikke stemte.
ADQ2+ og CatRot var tilkoblet iPad med SIM kort installert. Her ble begge PPU'ene spoofet, mens den innebygde iPad GNSS sensoren beholdt riktig posisjon (Bilde 7).



Bilde 9. Skjermdump Njord Pilot og SeaIQ. ADQ2+og Catrot spoofet ut i havet (40mil unna)

XR2 er en multimottaker og var tilkoblet en iPad uten SIM kort installert. Her ble den innebygde iPad GPS spoofet, mens XR2 beholdt riktig posisjon (Bilde 7).



Bilde 7: Skjermdump SeaIQ. XR2 beholdt riktig posisjon under spoofing test, mens den interne GPS ble spoofet

Test 4, Jamming, test av skjerming med metallring (kakeboks)

Effektrampetest - starte med lav effekt og øke stegvis oppover til alt er slått ut

Testen ble utført på alle bånd. Oppsett som tidligere, men det ble kjøpt inn en Kakeform (26cm i diameter) som skulle brukes som en skjerm mot jammeren (Bilde 8).

Bilde 8:Skjerming av sensor

Selve testen ble utført med to ADQ-2+ PPU (hvor den ene ble forsøkt skjermet, Bilde 8) samt en XR2. Under testen ble kartprogrammet SEAiq og Njord Pilot benyttet. Antennene (PPU) ble plassert på biltak, ca 7m fra jamming antenne. Ved å sammenligne de to identiske ADQ2+ ville det bli mulig å se om det ble en forbedring på den som var skjermet.

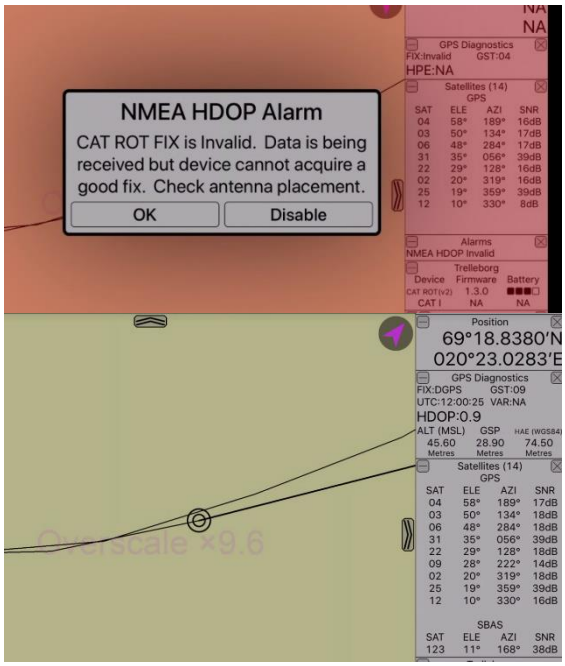
Fra starten, uten jamming tok den skjermede inn 1-2 færre satellitter, noe som skyldes selve kakeboksens høyde (skjermingseffekt). Ved 40dB dempning fikk begge problemer med HDOP men verdiene var like. Til sammenligning hadde XR2 nå 24 satellitter tilgjengelig, en nedgang fra 32 i starten. Ved 28dB demping ble det forskjell på de to. Den skjermede mistet fix mens den uten skjerming klarte seg akkurat. Ved 22dB demping mister XR 2 heading og RTK samt at viser at den har ca 16 tilgjengelige satellitter.
Testen viste at den skjermede sensoren ga dårlige geometri og mistet signalet før den som ikke var skjermet.

Test 5, Jammer med PRN (alle bånd) signal stasjonær, bil passerer.

I denne øvelsen kjørte bilen forbi en jammer i henholdsvis 90 og 50 km/t. Jamming på alle bånd og 0,1 watt effekt. PPU ADQ2+, CatRot og XR2 ble benyttet og festet med magnet til bilens tak.

Jammer var plassert nær veien slik at den ville ha effekt i hele veibanen et stykke før passering og etter passering. PPU ADQ2+, CatRot og XR2 ble benyttet og festet med magnet til bilens tak. Ved passering av jammer falt både ADQ2+ og CatRot ut. XR2 beholdt posisjon, men gjorde et utfall mot jammer.

Det ble kjørt begge veier (på retur var farten redusert til 50 km/t) og observerte det samme.



Bilde 10:Skjermdump SeaIQ. Passerer jammer i fart, få sekunder seinere alarm.

Analyse

Innledning

Analysen baserer seg på observerte data sammenstilt med de elektronisk loggede data samt en detaljert oversikt over utført jamming og spoofing gitt av FFI.

Analysen fokuserer på målene som var å finne sårbarheten hos losenes navigasjonssystem og på de erfaringer som vil gi viktige innspill i innovasjonsprosjektet.

Sensorer med GPS L1 alene

PPU ADQ2+, CatRot og Garmin har kun mulighet til å motta signaler fra GPS L1. GPS L1 er det åpne og mest brukte signalet til GPS. International Committee on Global Navigation Satellite Systems (ICG) er kommet til enighet i å ha en felles frekvens som var kompatibel med alle GNSS systemer. En av begrunnelse beskrives de slik i ICG vision statement (ICG, 2021).

> *«The International Committee on Global Navigation Satellite Systems (ICG) strives to encourage and facilitate compatibility, interoperability and transparency between all the satellite navigation systems, to promote and protect the use of their open service applications and thereby benefit the global community.»*

Alle 4 systemene har derfor en kompatibel frekvens nær eller lik GPS L1 som har sine fordeler, men på den annen side også gjør de mer sårbare.

Nettopp denne sårbarheten ble synlig på testene som ble avholdt. Så snart GPS L1 ble jammet var ADQ2+, CatRot og Garmin ikke i stand til å gi posisjon. Om de hadde vært multibånd mottakere hadde det sannsynligvis ikke hjulpet stort, men dette ble ikke avdekket under disse testene.

Testene viser at når Signal-Støyforholdet (SNR) kommer under ca 20dB vil mottakene slite med å levere posisjon. Det viste seg at både økt HDOP verdi og lav SNR kommer omtrent samtidig. Dette viser at alarmer som enten viser høy HDOP verdi eller reduksjon i SNR begge kan være indikasjoner på interferens. Forutsetning er imidlertid at høy HDOP verdi ikke skyldes fysisk skjerming av satellitter. På en multiband mottaker på L1 båndet vil det være flere satellitter synlig de aller fleste plasser. En høy HDOP verdi på en slik mottaker vil dermed være en enda sterkere indikasjon på interferens.

En fellesnevner for alle testene var at disse mottakerne klarte seg når andre bånd ble jammet, men ble raskt slått ut når GPS L1 ble jammet.

HDOP (horizontal dilution of precision)

HDOP Verdi er en funksjon som viser om nøyaktigheten blir redusert av ikke-optimal geometri på det mottatte satellittene. Ved flere enn 4 satellitter tilgjengelig kan mottakeren velge de som gir best geometri og dermed redusere unøyaktigheten som følge av dårlig geometri. Lav HDOP er bedre og HDOP=1 er ideelt (Kjerstad, 1997; Kystverket, 2021)

DOP Value	Rating	Description
1	Ideal	Highest possible confidence level to be used for applications demanding the highest possible precision at all times.
1-2	Excellent	At this confidence level, positional measurements are considered accurate enough to meet all but the most sensitive applications.

Bilde 11: beskrivelse av HDOP verdi (Kilde: marxact.com/article/111)

Mottakerne brukt under testene har alle mange kanaler og kan velge de beste satellittene, noen av mottakerne flere enn andre. På mottakerne med kun GPS L1 er det færre muligheter enn ved XR 2, men en felles erfaring var at redusert HDOP verdi er en av de første indikasjonene på at det er interferens til stede. XR2 var som forventet mindre påvirket enn for eksempel ADQ2+. I test 2 viste det seg at ved 20dB demping hadde XR2 en HDOP på 0,6 og Catrot 1,6. Når Catrot og ADQ2+ hadde mistet fix hadde XR2 fortsatt kun en redusert nøyaktighet på grunn av geometri med HDOP på 2,1. Dette viste at det var viktig med en god presentasjon av HDOP til brukerne av kartsystemer.

Multikonstellasjon og multifrekvensmottaker XR2

XR2 mottar både på flere bånd og flere frekvenser. Dette er gjort nettopp for å gjøre mottakeren mer robust. I tillegg består XR2 av 3 poder som dermed gir mulighet til å kalkulere en nøyaktigere posisjon ved å utnytte fasemåling (RTK) (Kjerstad, 1997; Kystverket, 2021). Heading poden blir da Rover og posisjons poden Base. Kalkulering av posisjon ved fasemåling er mye mer krevende og sårbart særlig når referanse korreksjonen også er påvirket av interferens. Det er dermed forventet at RTK skal falle ut tidligere enn posisjonsbestemmelse ved vanlig Pseudo Range målinger. Heading beregning er også avhengig av fasemåling og vil også være mer sårbart og er også forventet å falle ut tidligere. Andre fordeler som for eksempel «fast aqusition» blir ikke analysert her (Nesreen, 2015).

I alle testene var det tydelig at XR2 innfridde forventningene og den var klart den mest robuste sensoren. XR2 viste at den hadde ca 32 satellitter tilgjengelig i løpet av testene. Da den mistet posisjon viste den imidlertid ca 12-13 satellitter tilgjengelig noe som burde indikere at dette skulle være godt nok. Analysen har ikke klart å finne ut hva dette skyldes, men en mulig løsning er at visningen av antall satellitter «henger etter» og ikke viser korrekt antall eller at visningen er for «snill». Det vil si at ikke alle satellitter som er synlige kan brukes i posisjonsløsningen. Videre analyser og tester må imidlertid til for å avdekke dette. Analysen av test 1 viser også at XR2 klarte seg bedre når GPS L1 ble jammet til slutt. Den hadde fix selv etter at GPS L1 ble jammet ut til slutt, noe som ikke var tilfelle da GPS L1 ble jammet ut først.

I et jammetilfelle var det forventet at relativ RTK (også benevnt som moving base RTK) først vil bli rammet, og analysen bekrefter dette. Det viste seg også at RTK falt ut når Glonass L2 ble jammet. RTK skal ikke være avhengig av noen spesielle bånd, men i praksis viser det seg at den blir påvirket hvis noen av båndene den bruker er jammet ut. I denne sammenhengen er det interessant å merke seg at den har flere bånd, noen som har samme frekvens som de som ble jammet, noen nært og noen litt lengre unna senterfrekvensen som ble jammet. Testen viste at selv om XR2 har flere bånd og frekvenser, og dermed en bedre mulighet til å opprettholde funksjonen til basen og roveren i interferens på noen av frekvensene, var dette ikke tilfelle og XR2 fikk problemer selv om den hadde flere muligheter. I denne analysen har det ikke vært mulig å få nok innsikt i programarkitekturen eller detaljerte nok tester til å kunne konkludere hvorfor RTK ble degradert når 3 av 10 bånd ble jammet. Det er sannsynlig at det har med kompleksiteten og sårbarheten i beregningen av hvilken bølge mottakerne befinner seg i, kjent som “ambiguity resolution” (Teunissen, Joosten, & Odijk, 1999). En annen faktor kan være at ved reduksjon av antall satellitter, kan base og rover mottakerne få problemer med å se samme satellitt som er en forutsetning for riktig bølgeberegning. Dette er imidlertid ikke mulig å analysere utfra data tilgjengelig fra testen.

Det ble også gjennomført en test som var lik test 1, men jammetypen ble skiftet fra CW til PNR (se avsnitt Gjennomføring). Resultatene var i grovt like, men det var helt tydelig at PNR jamming påvirket

mottakerne mer med samme effekt. XR2 mistet fix mens den hadde dårlig fix på CW jamming.

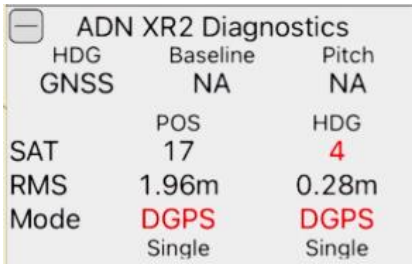
XR2 beregner heading basert på relativ RTK (også kjent som "GPS kompass"), der den 3 dimensjonale vektoren mellom Position pod og Heading pod danner grunnlaget. Heading er mer sårbar fordi både moving base (Position pod) og rover (Heading pod) er eksponert samtidig. Dermed vil GNSS heading antakeligvis falle bort først, og i tillegg gir XR2 heading-backup basert på RoT i 5 minutter. Dette skjer ved at akkumulert RoT legges til siste kjente GNSS heading inntil neste validerte GNSS heading er tilgjengelig. RTK posisjon (referert til Position pod) kan også bli degradert under eksponering. Den er da mindre sårbar så lenge korreksjonene ikke stammer fra en referanse som også er eksponert. Under eksponering er det dog forventet at høyeste nøyaktighet ikke er oppnåelig, og at mottaker rapporterer en RTK float[1], DGPS eller ukorrigert posisjonsløsning. Det kan være mer krevende å slå fast kvaliteten på posisjonen under eksponering.

På samme måte som med RTK, viste det seg at heading kalkulering var mer sårbar enn å oppnå pseudo-range posisjon. Grunnen til dette er tilsvarende til at RTK begrenses, samt at heading også er avhengig av fasene i bærebølgene fra to satellitter. Begrunnelsen er dermed mye den samme som for RTK.
Alarmer om mistet heading vil dermed også være en mulig indikasjon på interferens, selv om det også kan være andre årsaker som for eksempel blokkering av satellitter under broer ol. Det er imidlertid viktig å merke seg at heading backup kan gi en forsinkelse i tap av heading på 5 min, men på test 1 og 2 så det ikke ut som om det gikk 5 min til alarmen kom da trinnene i økning av jamming foregikk hvert minutt. For å endelig fastsette årsaken til dette må det utføres flere tester. Ideelt sett bør det komme varsel ved bortfall av GNSS-kompasset selv om backup holder i 5 min.

Kartprograms evne til å opplyse brukeren om interferens

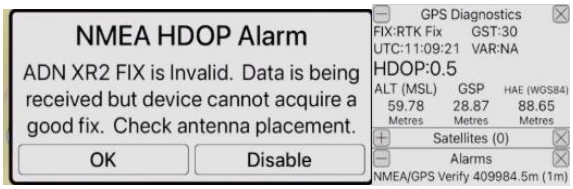
For en operatør av et kartprogram er det viktig å bli varslet hvis noe er galt, særlig hvis feilen potensielt kan påvirke sikkerheten for seilasen. Det ble derfor loggført hvordan programmene varslet om interferens og hvilke nyttige funksjoner som lå i programmene som kan overvåke kvalitet på signalet.

SEAiq og Njord Pilot kom begge opp med alarm når de mister posisjon, heading og RTK. SEAiq er imidlertid vesentlig bedre. Den har et bilde med «Diagnostics» (Bilde 12) som er nyttig.



Bilde 12: Skjermdump SeaIQ.
Diagnostic vindu til SEAiq

Ingen av alarmsystem er imidlertid programmert for å varsle om interferens, men for eksempel antenne problemer, som i de fleste tilfeller vil være misvisende (Bilde 13).



Bilde 13: Skjermdump SeaIQ.
Nyttige alarmer og info på SEAiq

Under testen så det ut som om sensorene som var tilknyttet Njord Pilot ble mindre påvirket enn de som var tilkoplet SeaIQ. Dette var ikke tilfelle og viser at brukeren trenger god informasjon i de tilfellene sensorene blir påvirket og her har SeaIQ et bedre utgangspunkt enn Njord Pilot.

4G SIM kortets betydning

Spoofing testen viste at den interne GNSS mottakeren i iPaden som hadde SIM kort installert ikke lot seg lure (spoofe) av at feil tid og posisjon ble sendt til iPad. Årsakene til dette er ikke videre analysert i denne artikkelen men det er kjent at iPad fra andre generasjon med simkort benytter «Assisted GNSS» (A-GNSS) (Zandbergen & Barbeau, 2011) og har integrert GNSS modul, som gjør at iPad utnytter navigasjonsdata fra mobildata og ikke fra satellittene (Merry & Bettinger, 2019). Spoofingen innebar en 40 000km og 1 uke offset. Det så ut som om Ipaden mottok tidsinformasjon via A-GNSS som gjorde at den ikke ble lurt på tiden, noe som kan være årsaken til at iPad med sim-kort ikke lot seg spoofe.

[1] I en Float-løsning er algoritmen ikke løst (ennå) og kan ikke produsere en akseptabel FIX-løsning (ennå) Kilde: https://support.marxact.com/article/85-what-is-the-difference-between-rtk-fix-and-rtk-float.

Det som imidlertid virker klart, er at det kan være nyttig å ha tilgang på 4G (eller tilvarende) som en kilde for verifisering av GNSS data.

Effekt ved bevegelse

Under scenariet der sensorene var i fart og passerte en kilde for interferensen viste det seg enda viktigere at programmene gir en rask og tydelig indikasjon på det sensoren blir utsatt for.
Like før passering av jammer (20-30 sekunder) var det en tydelig reduksjon i signal-støy forhold (SNR) uten at det ble varslet ved alarm. Ved passering var det et tydelig hopp bort fra veien, men på grunn av for lang avstand mellom hvert lagringspunkt fremkommer ikke dette «hoppet» på slepestreken (past track). Hvis ikke operatøren hadde fulgt godt med, ville denne interferensen ikke blitt oppdaget, noe som kan være med på å gi et uriktig situasjonsbilde.
En markert nedgang i signal-støy forhold burde logges og ligge som informasjon til brukeren.

Skjerming av antenne

En måte å hindre multipath (refleksjoner) fra bakken er skjerming. Høy kvalitets antenner bruker høy som for eksempel brukes til landmåling, bruker skjerming som er ringer som sørger for at uønskede signaler ikke når mottakeren. I testene sto jammeantennen i ca. samme høyde som mottakerne på taket og det ble derfor kjøpt inn en skjerm (kakeform) der mottakeren er inne i formen. Resultatet av denne testen var det motsatte av hva som var forventet, den skjermede mottakeren mistet fix før den tilsvarende mottakeren uten skjerming. Analysen her viser at det er vanskelig å konkludere, men det var allerede i starten indikasjoner at den skjermede sensoren hadde 1-2 færre satellitter. Det så med andre ord ut som om skjermen hindret at sensoren kunne ta inn satellitter som hadde lav elevasjon. Skjermen hindre ikke at sensoren ble jammet, noe som også var forventet, men det var marginal forskjell på de to sensorene. Det at den skjermede mistet fix først skyldes sannsynligvis at den hadde 1-2 færre satellitter å spille på.

Konklusjon

Hensikten med testene var å vurdere losenes navigasjonssystem med hensyn på interferens og dens evne å alarmere om interferens. Det var også viktig å få innspill til innovasjonsprosjektet som skal utvikle neste generasjons støttesystem for lostjenesten.

Felles for alle sensorer som kun hadde GPS L1 var at det var svært sårbare for interferensen og mistet fix ved jamming av dette båndet med en effekt på 0,1 watt. Avstand ca 17m.

XR2 som er en multifrekvens og multikonstellasjonsmottaker (mange bånd, GPS, GLONASS, BeiDou med flere) klarte seg som forventet da den hadde alternativer til de jammede bånd. Det viste seg at selv om den hadde bånd som ikke ble jammet mistet den fix likevel da 4 bånd ble jammet. Noe av grunnen til dette er at alle båndene ligge relativt tett, og har sidebånd som går over i hverandre. Kalkulering av RTK og heading bruker fasemåling og er derfor mer sårbar for jamming enn normal posisjonsberegning.

Ved spoofing av tid (1 uke) og posisjon (40 000m) ble alle systemer til slutt lurt, men det er klart mer krevende enn jamming.
Det viste seg også at CW jamming er mindre effektiv enn PRN jamming. Det var indikasjoner på at iPad med SIM kort (A-GNSS) ikke lot seg lure på samme måte som de uten. Dette kan skyldes at den mottar rett tid og «vet» at den er i en basestasjons nedslagsfelt.

Testing av skjerming ga motsatt effekt da satellitter ble skjermet istedenfor jammeren.

De to kartprogrammene, SeaIQ og Njord Pilot hadde forskjellig måte å vise mulig interferens. SeaIQ hadde flere viktige parameter som var lett å hente opp, mens Njord Pilot hadde mindre og «skjulte» dermed viktig informasjon for brukeren. Generelt var alarmer for få og til tider misvisende.

Testene ga den ønskede effekt og målene ble oppnådd både innen måling av robusthet og innspill til innovasjonsprosjektet.

Viktige funn listet opp:

- XR 2 var mest motstandsdyktig på grunn av at den er multikonstellasjonsmottaker og har et bredt frekvensspekter.
- RTK var sårbart når 3 av 10 bånd var jammet og når 4 bånd ble jammet forsvant RTK.
- Heading i XR2 var sårbart da fasemålinger brukes og er lettere å påvirke på grunn av konvergens problematikk.
- XR2 klarte seg også best i narring, men det gjorde også iPad som hadde SIM kort 4G dekning på grunn A-GNSS.
- Det visste seg svært nyttig å få en alarm som visste avvik mellom intern (innebygget GNSS iPad) og ekstern PPU (SeaIQ).
- Skjerming mot jamming hadde med dette oppsettet (kakeboks) motsatt effekt, og førte til færre mottatte signaler eller multipath (flerveis interferens) som forringet sensoren istedenfor å skjerme for jamming.
- Ved svake jammesignaler er HDOP verdien og synkende signal-støyforhold det første som gir indikasjon på interferens.
- PRN jamming er mer effektiv enn CW jamming.
- Alarmer er ikke tilpasser interferens.

Fremtidig forskning:

- Teste RTK mottaker og hva som gjør at den går i float (jobber med å få fix) når den fortsatt har bånd tilgjengelig.
- Hvordan effektivt presentere alarmer ved interferens for å øke operatørens situasjonsbevissthet.
- Teste XR2 mottaker med tanke på hvorfor den ikke klarer å beregne fix med mange satellitter tilgjengelig.
- iPad med A-GNSS virkemåte og påvirkning ved signalinterferens og spoofing.

Referanser

Hofmann-Wellenhof, B. (2008). *GNSS--global navigation satellite systems : GPS, GLONASS, Galileo, and more*. Wien: Springer.

IA, I. a. (2020). Støtteverktøy for Lostjenesten. Retrieved from https://innovativeanskaffelser.no/stotteverktoy-for-lostjenesten/ Access date: 21.08.2021

ICG, I. C. o. G. N. S. S. (2021). International Committee on Global Navigation Satellite Systems (ICG). Retrieved from https://www.unoosa.org/oosa/en/ourwork/icg/icg.html Access date: 15.10.2021

IMO. (2007). *Resolution MSC.252(83). Adoption of the revised performance standards for Integrated Navigation Systems (INS)*. London

Kjerstad, N. (1997). *Elektroniske navigasjonssystemer for maritime studier*: Høgskolen i Ålesund.

Kystverket. (2021). *Navigasjon for lostjenesten* (Vol. 1). Ålesund: Hatlehols Grafiske AS.

MAIB, M. A. I. B. (2014). *Report on the investigation of the grounding of Ovit in the Dover Strait*. Retrieved from Southampton:

Merry, K., & Bettinger, P. (2019). Smartphone GPS accuracy study in an urban environment. *PloS one, 14*(7), e0219890.

Nesreen, I. Z. (2015). *Multi-Constellation Fast Acquisition Through Utilization of Orbit Predictions and Positioning Data.* Paper presented at the Proceedings of the 28th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2015).

Norris, A. (2010). *Integrated Bridge Systems vol 2 ECDIS and Positioning* (Vol. Volume 2 og Integrated Bridge Systems). London: Nautical Institute.

NRS, N. R. (2013). *Vurdering av sårbarhet ved bruk av globale satellittnavigasjonssystemer i kritisk infrastruktur*. Retrieved from https://www.romsenter.no/Aktuelt/Publikasjoner/Rapport-om-saarbarhet-ved-bruk-av-satellittnavigasjon Access date: 02.10.2021

Psiaki, M. L., & Humphreys, T. E. (2016). GNSS spoofing and detection. *Proceedings of the IEEE, 104*(6), 1258-1270.

RaENG, T. R. A. o. E. (2011). *Global Navigation Space Systems: reliance and vulnerabilities*. Retrieved from London: https://www.raeng.org.uk/publications/reports/global-navigation-space-systems Access date: 03.04.2021

Teunissen, P. J., Joosten, P., & Odijk, D. (1999). The reliability of GPS ambiguity resolution. *GPS Solutions, 2*(3), 63-69.

Volpe, J. A. (2001). *Vulnerability assessment of the tranportation infrastructure relying on the Global Positioning System*. Retrieved from https://www.navcen.uscg.gov/pdf/vulnerability_assess_2001.pdf Access date: 02.06.2021

Weintrit, A. (2009). *The Electronic Chart Display and Information System (ECDIS), An Operational Handbook*: A Balkema Book, CRC Press, Taylor & Francis Group.

Zandbergen, P. A., & Barbeau, S. J. (2011). Positional accuracy of assisted GPS data from high-sensitivity GPS-enabled mobile phones. *The Journal of Navigation, 64*(3), 381-399.