KYSTVERKET

Rapport etter Jammetest Andøya

uke 38, 2023

Kunnskapsbygging GNSS interferens Kystverket

Sammendrag

Tittel:	Rapport etter Jammetest Andøya 2023	Title:	Report jamming trials Andøya 2023
Forfattere:	Steinar Nyhamn Alexander Sauter Geir Pettersen	Author(s):	Steinar Nyhamn Alexander Sauter Geir Pettersen
Dato:	13.03.24	Date:	13.03.24
Rapport Nr:	2	Report No:	2
Sider:	24	Pages:	24
Prosjekt:	GNSS interferens	Project:	GNSS interference
Prosjektleder:	Bjørnar Kleppe Odd Sveinung Hareide	Project manager:	Bjørnar Kleppe Odd Sveinung Hareide
Emneord:	GNSS, Jamming, sårbarhet, GNSS mottakere	Key words:	GNSS, Jamming, Vulnerability GNSS receivers

Sammendrag:

Hovedmålsettingen med testen var å måle hvor robust mottakerne var mot småjammere som kan befinne seg i nærheten av en maritim mottaker. Testene viser at disse jammerne kan påvirke en maritim mottaker, særlig hvis de kun har mulighet til GPS L1. Testen viste også at de såkalte sigarettenner jammerne ikke hadde noe særlig effekt på mottakerne, men med kun marginalt større effekt og hvis jammeren ikke er inne i en bil, er effekten vesentlig større.
CRPA antenne virket etter hensikten og avstanden mottakerne ble jammet ut på ble redusert.
Mottakerne blir mer robust ved å ha to eller flere bånd selv om de ligger ganske nært hverandre i frekvens. Mottakere som bruker hele båndet, er vesentlig mer robust og burde vært pålagt i en maritim mottaker.
Forskjellige fabrikanter SOLAS mottakere håndterer interferens forskjellig.
Alle mottakerne lot seg lure av spoofing i en eller flere scenarier.

Summary:

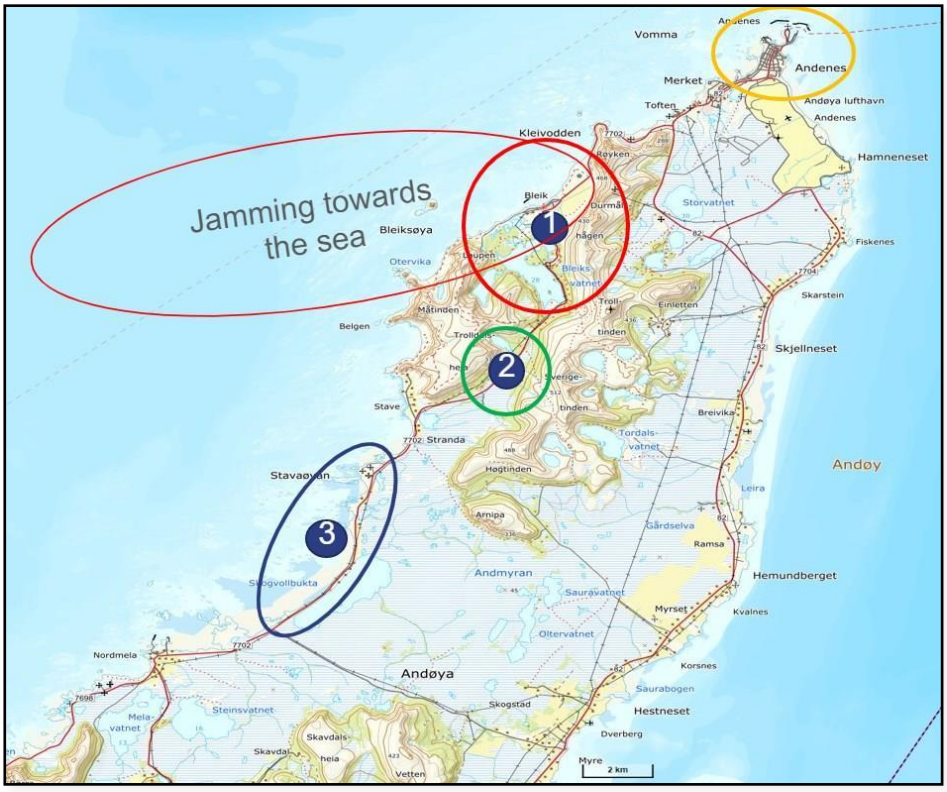
The main objective of the test was to measure how robust the receivers were against small jammers that may be in the vicinity of a maritime receiver. The tests show that these jammers can affect a maritime receiver, especially if they only have the option of GPS L1. The test also showed that the so-called cigarette lighter jammers had no particular effect on the receivers, but with only a marginally greater effect and if the jammer is not inside a car, the effect is significantly greater. The CRPA antenna worked as intended and the distance at which the receivers were jammed was reduced. The receivers become more robust by having two or more bands, even if they are quite close to each other in frequency. Receivers that use the entire band are significantly more robust and should have been required in a maritime receiver.
Different manufacturers' SOLAS receivers handle interference differently. All the recipients were fooled by spoofing in one or more scenarios.

Language of Report:	Norwegian

Innhold

1 Innledning

I uke 38, fra mandag til fredag, ble det Jammetest 2023 gjennomført. Stedet var i området Bleik på Andøy. Dette var tredje år på rad at det ble gjennomført en slik test som i 2021 var et initiativ fra Statens Vegvesen i samarbeid med NKOM og FFI. Som et resultat av voksende interesse var det denne gangen mer enn 200 deltakere, fra ca. 60 bedrifter, som kom fra mange forskjellige land, for eksempel Japan, Sverige og Finland.
Som en følge av mange deltakere ble det laget et relativt rigid program, men det var noe rom for fleksibilitet med hensyn til våre egne tester som for det meste foregikk i område 2. Ellers var det planlagt mest aktivitet i område 1.



Figur 1: oversikt over øvelsesområdet

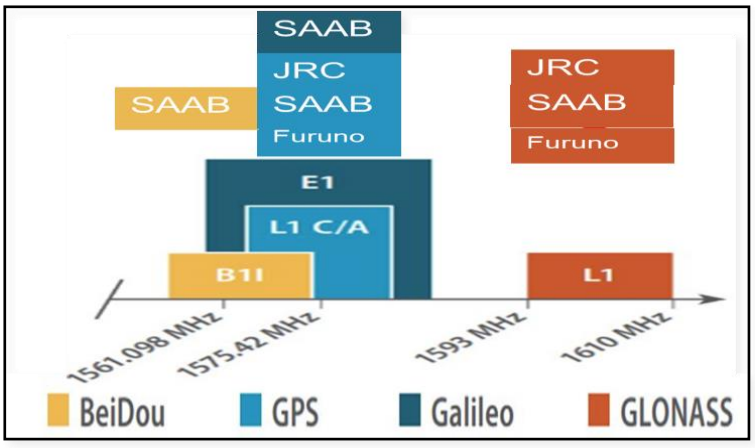
Denne rapporten beskriver erfaringer inkludert noen enkle analyse. Det er imidlertid lagret en betydelig mengde data som gjør det mulig å gjennomføres dypere analyser hvis ønskelig.

2 Målsetting

Målsettingen med deltakelsen i jamme-uken var å teste hvordan 3 SOLAS mottakere ble

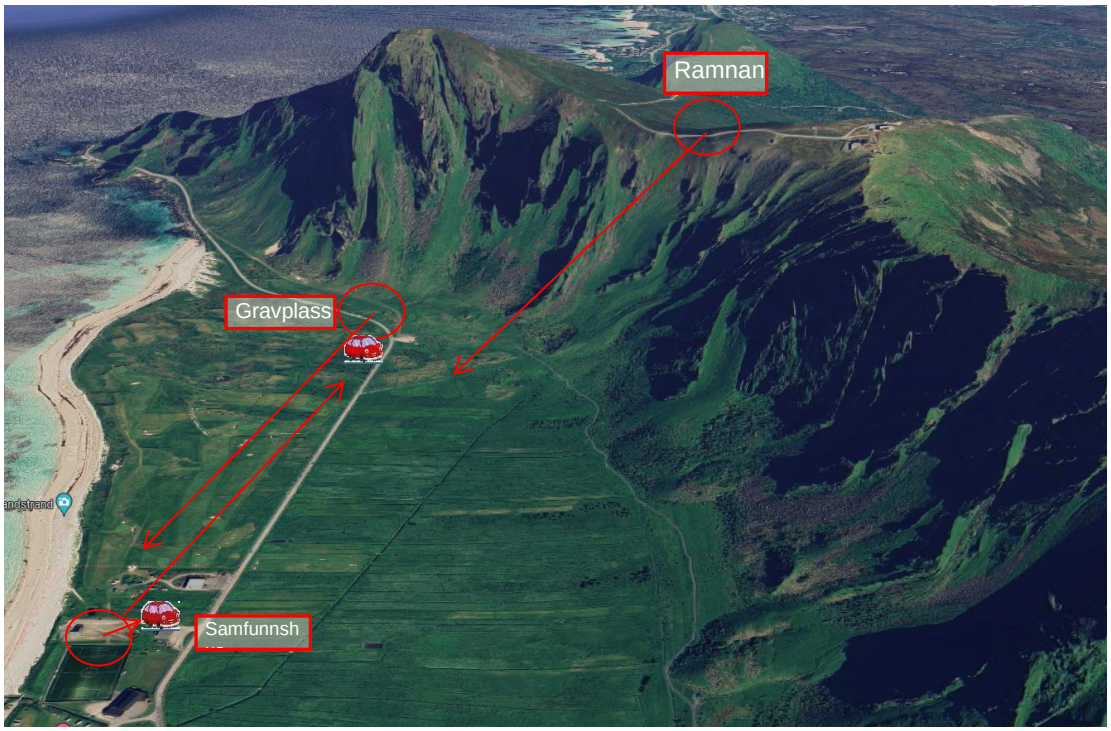
Figur 2: Antennene på taket

påvirket av interferens i form av jamming og spoofing.
Hovedvekt skulle legges på jamming og hvorledes småjammere (for eksempel jammere i biler) påvirket typiske moderne skipsmottakere.
Da det mest sannsynlig er mest vanlig at skip har kun GPS L1 eller kanskje GPS L1 og Glonass L1 var påvirkningen under bruk av disse to konstellasjonene hovedfokus. Oppsett
Alle mottakerne ble montert i en bil med antennene på taket (Figur 2). SOLAS mottakerne var Furuno - GP-170, SAAB -R5 SUPREME NAV MkII og JRC - JLR-8600. Furuno, SAAB og JRC har mulighet til GPS L1 (kort referert til som L1) og Glonass L1 (referert til som G1) mens SAAB har Galileo og Beidau i tillegg (ikke i fokus i denne rapporten). JRC kan ikke settes på Glonass alene, mens mottakerne ellers kan brukes i GP (GPS alene), GL (Glonass alene) eller GN (GPS og Glonass i multikonstellelasjon) modus. Alle regnes dermed som multikonstellasjon men alle holder seg innen L1 båndet (upper L-Band) som er frekvensbåndet fra 1559 MHz til 1610 MHz (se Figur 3).

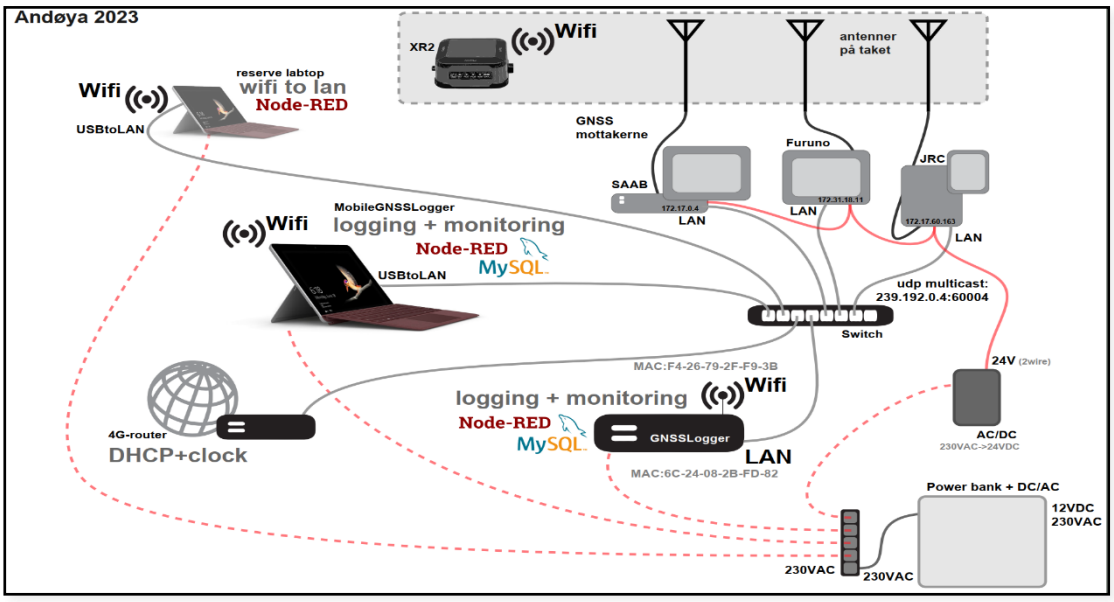


Figur 3: Alle mottakerne befinner seg i "Upper L-band")

XR2 (og ADQ2) ble med hensyn til denne rapporten bare brukt som en referanse. Det ble også anledning til å teste en CRPA (Controlled Reception Pattern Antenna) antenne av merke Tualcom i deler av testene for å undersøke i hvilken grad jamming eller spoofing kan unngås med en sånn «anti-jammeantenne».



Figur 3: Jammeposisjoner ringet inn med forskjellige jammeretninger



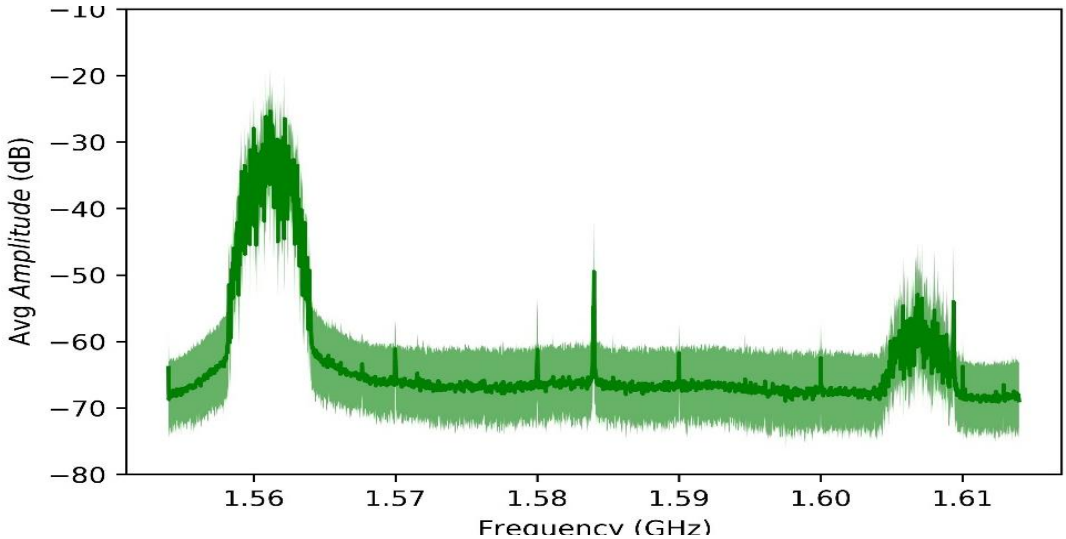
Figur 4: Oppsett for logging

Logging ble for det meste gjort elektronisk, både logging av NMEA data (i rå-format og tolket) og manuell notering i databasen, men også noe manuelt på papir (se Figur 4).

Det ble også til tider tatt film av mottakerne (se Figur 5). Alt loggeutstyr ble plassert inni eller på taket, på en leiebil, sånn at målinger kunne tas både mobilt under kjøring og statisk.

Figur 5: Utklipp fra film med lyd. Skjermene til de 3 mottakerne, tekstmeldinger som RDS via FM i bilen og Chat på telefon.

Mika Saajasto fra Finnish Geospatial Research Institute har delt data der spekteret under jamming kan observeres, for å kunne bekrefte frekvensen til jammeeffekten når virkning på mottakerne skal analyseres. Figur 6 viser et eksempel der det er interferens på G1 selv om det i dette tilfellet kun skulle bli jammet på B1I. Dette gjør det mulig å unngå feiltolkning av effektene til de forskjellige typer av jammingen.

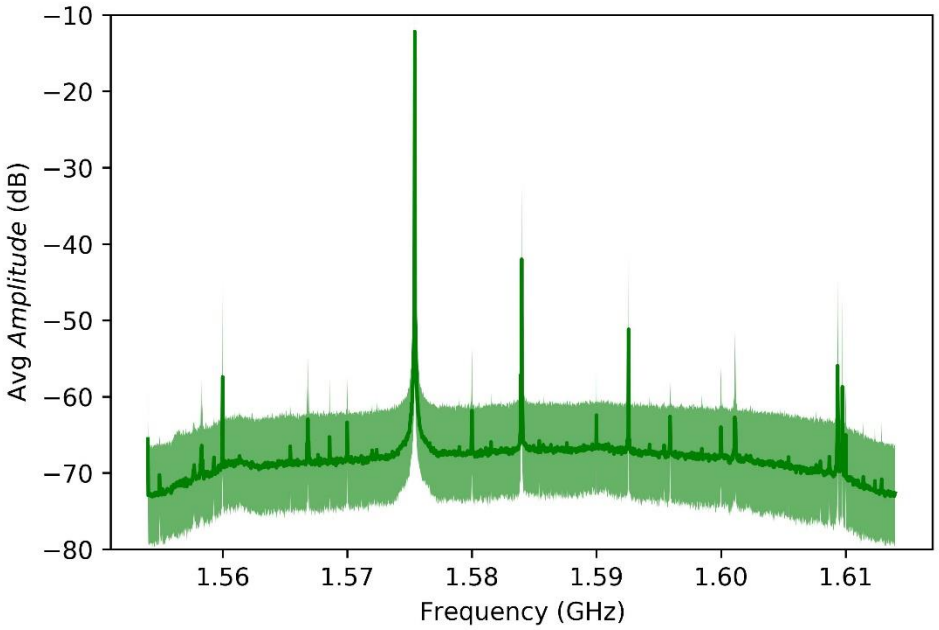


Figur 6: Eksempel på målt spektrum. Utslag nærmere 1.56 GHz ligger i B1I-området, mens mindre utslag nærmere 1.61 GHz er i G1-området (tiltenkt her).

3 Type jamming som ble benyttet

3.1.1 Continuous wave (CW)

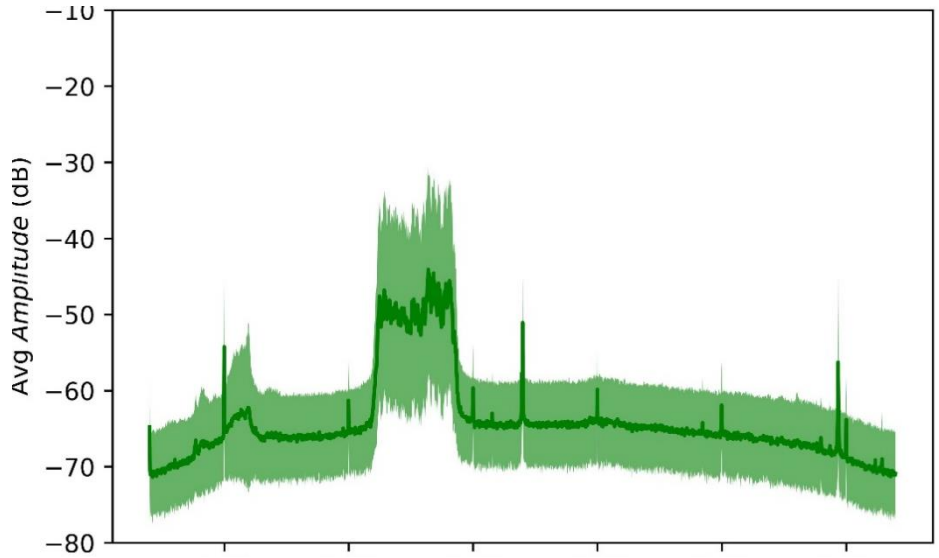
CW-jamming betegner sending av en kontinuerlig bølge (CW) modulasjon (enkeltfrekvenskomponent) ved hjelp av «Right Hand Circular Polarization» (RHCP) antenner. Figur 7 viser et typisk CW signal målt under jammetesten, her i midten av L1-båndet (GPS L1-jamming).



Figur 7: Spectrum av et CW-signal

3.1.2 Sweep/chirp

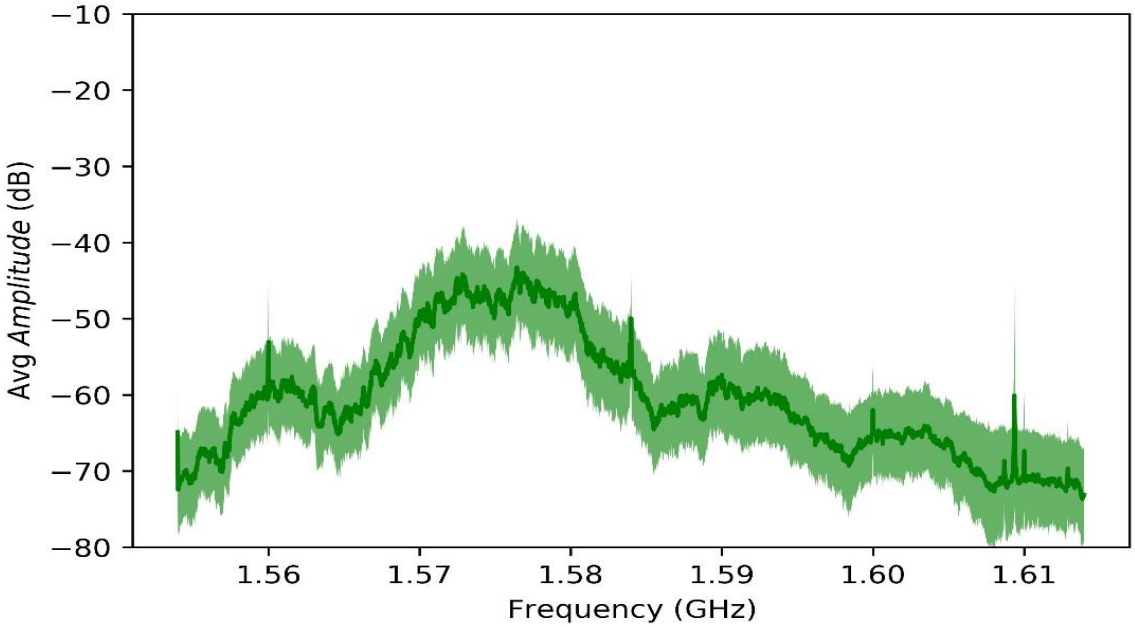
«Sweep/chirp» modulasjon betyr at frekvenskomponenten vil pendle frem og tilbake innenfor det spesifikke frekvensbåndet med en gitt svinge hastighet. Figur 8 viser et typisk eksempel på «Sweep/chirp» over en hel testperiode. Frekvensen varierer her innad L1-båndet.



Figur 8: Spectrum av sweep signal

3.1.3 Pseudo Random Noise (PRN)

Pseudo Random Noise (PRN) modulasjon brukte også RHCP antenner. PRN-signaler har samme spektrale form som de sanne signalene som sendes fra GNSS-satellittene, men med forskjellige spredningskoder. Spredningskodene er Binary Phase Shift Keying (BPSK) modulert på senterfrekvensen til det spesifikke GNSS-båndet. Figur 10 viser at PRN-jamming (her på L1) har en bredere frekvensfordeling, og kan påvirke nabofrekvenser.



Figur 9: PRN type spektrum (L1)

Opprinnelig plan var å ha en maksimal utgangseffekt på 200 Watt med i testene, men dette ble redusert til 20 watt pga. frykt for at utstyr kunne bli ødelagt.

4 Typer spoofing

4.1.1 Meaconing

Meaconing vil si GNSS-retransmisjon, der GNSS sendingene vil ha feil posisjon, men med ekte satellittdata som typisk blir videresendt med større effekt enn originalsignalet. Ved videresending vil den spoofede posisjonen tilsvare spooferens posisjon.

4.1.2 Incoherent spoofing

GNSS data fra spoofer som sender falske eller ekte efemerider. Simulerte signaler kan bruke en eller flere konstellasjoner og ett eller flere signalbånd. Falsk tid er vanlig virkemiddel i tillegg til posisjonsfeil.

4.1.3 Coherent spoofing

Simulerte spoofing-signaler blir produsert. De genererte spoofing-scenariene vil bruke ekte efemerider og være synkronisert med sann GPS-tid. Dette kan gjøres med en eller flere konstellasjoner og ett eller flere signalbånd. Utsendt signal kan modifiseres, som ved inkoherent spoofing, for å narre mottakeren til å være et annet sted enn den egentlig er.

5 Tester

Testene vi deltok på med erfaringene som ble gjort beskrives her dag for dag.
Benevningene er som følger:
L1, L2 og L5 står for GPS L1, L2 og L5. G1 og G2 står for GLONASS L1 og L2. E6 og E5b står for GALILEO E6 og E5b. B1I står for BEIDAU L1.

5.1 Mandag 18 september

Testplan med planlagte tider:
13:00-13:10 20 W CW: L1
13:20-13:30 20 W CW: L1, G1, L2, L5
13:40-13:50 20 W chirp: L1
14:00-14:10 20 W chirp: L1, G1, L2, L5
14:20-14:30 20 W PRN: L1
14:40-14:50 og 15:00-15:30 20 W PRN: L1, G1, L2, L5
15:40-15:50 20 W: L1
16:00-16:10 20 W: G1
Rampe-test med gradvis økende effekt til maks effekt og så gradvis synkende effekt igjen:
16:20-16:35 0.1 µW to 20 W, 2 dB increments PRN: L1
16:50-17:05 0.1 µW to 20 W, 2 dB increments PRN: L1, G1, L2, L5
Mottakerne (bilen) var her stasjonær med en avstand til jammer på 938 meter frem til 17:20. Fra 17:20-17:50 gjennomførte valgte vi et jammescenario etter vårt behov/forespørsel der vi fokuserte på å gjenta jamming av G1 og L1, da med forskjellige innstillinger på mottakerne. Hensikten ved testene denne dagen, og ved testene på slutten av dagen, var å undersøkelse om mottakerne, som kan velge mellom L1 og G1 kan klare seg med kun den ene, eller om mottakerne på noen måte er avhengig av f.eks. GPS L1. Dessuten kunne påvirkningen av de forskjellige jamme-typene undersøkes.

5.1.1 Erfaringer

Fra 13:00 og til 17:20 var mottakerne stilt på G1+L1.
Ved 20 watt CW jamming på alle 4 bånd mistet alle fix som også observert tidligere. XR2 holdt god fix. Ved 20 watt CHIRP jamming på L1, klarte alle seg, men ved jamming av alle 4 bånd falt de også ut ved CHIRP. Erfaringen var at PRN har størst jammeeffekt, deretter CHIRP og CW som har noe lavere virkningsgrad enn de to andre. Dette underbygges av tidligere observasjoner også, men da spektrene under jamming var kjent denne gangen, viser det seg at når FFI jammer med PRN er jammebåndet bredere enn når Justervesenet jammer med PRN. FFI sin PRN er derfor "sterkere". Samtidig er "real-world PRN" mer lokalt, men har veldig sterk effekt på våre mottakere.
Det er dermed en mulighet at våre erfaringer med at PRN er mest effektiv jammetype kan ha med at det ble jammet på et bredere bånd. Dette kan undersøkes nærmere ved neste anledning.
Fra 17:20 ble det innvilget jamming på G1 og L1. Først L1+G1, deretter bare L1 og til slutt bare G1. Jamming ble gjennomført fra Justervesenet fra ca. 30 meter, men med lavere effekt (ukjent effekt). Jammingen er her PRN, men mer avgrenset i spekteret, dermed en litt annen form for PRN.

Jammet bånd	Furuno	SAAB	JRC	Effekt	Merk
L1	Alle 3 til G1+L1			Fix på G1 GPS jammet ut eller veldig svake SNR.	Øker effekt 3 ganger. Jammestyrke ikke oppgitt.
G1	Alle 3 til G1+L1			Fix på L1 G1 falt ut umiddelbart	Reduserte jammeeffekt resulterte i noen G1 satellitter svakt inne.
G1	G1	G1	L1	Furuno og SAAB mistet fix på laveste effekt. JRC holder fix på L1	Selv ved økt effekt jamming på G1 holdt JRC fix.
L1	G1	G1	L1	Furuno og SAAB fikk raskt fix igjen, men JRC mistet fix.	Jamming ble skiftet fra G1 til L1 raskt uten endring på mottakerne. Furuno og SAAB klarte å holde fix selv med noe økning i effekt.
L1	L1	L1	L1	Alle jammet ut	Jammer bytter til G1
G1	L1	L1	L1	Mottakerne fikk fix igjen	G1 på lav effekt

Testen viste at mottakerne klarte seg med bare en av konstellasjonene. Det virket imidlertid som om mottakerne klarte seg bedre på L1 alene eller G1 alene (JRC kan ikke brukes på G1 alene). På bakgrunn av dette er det derfor ikke noe grunnlag for å påstå at mottakerne har en form for avhengighet av verken GPS eller Glonass. G1 har imidlertid litt færre satellitter og jevn over litt svakere SNR, som kan være en grunn til noe redusert robusthet på G1. Dog, ved sterk (økt) jamming, eller ved jamming på et bredere område (for eksempel PRN, FFI) jammes både L1 og G1 ut selv ved jamming forgår kun på en av dem.

5.2 Tirsdag 19 september

Jammeren var tirsdag plassert på en fjelltopp (Ramnan, Figur 3) ca. 1300 m avstand og i ca. 300m m høyde.
Gjentakelse av rampe-test med gradvis økende effekt til maks effekt og så gradvis synkende effekt igjen:
09:00-09:15 0.1 µW to 20 W, 2 dB increments PRN: L1
09:30-09:45 0.1 µW to 20 W, 2 dB increments PRN: L1, G1, L2, L5

Pyramidetest, først gradvis økende antall med jammede GNSS-bånd, og så gradvis færre påvirkede bånd igjen. I «inverse pyramide test» tilsvarende motsatt med flest påvirkede bånd i starten og i slutten og færre påvirkede bånd i midten.
10:30-11:15 Pyramidetest, 20 watt, PRN, 3 min jamming og 2 min pause.

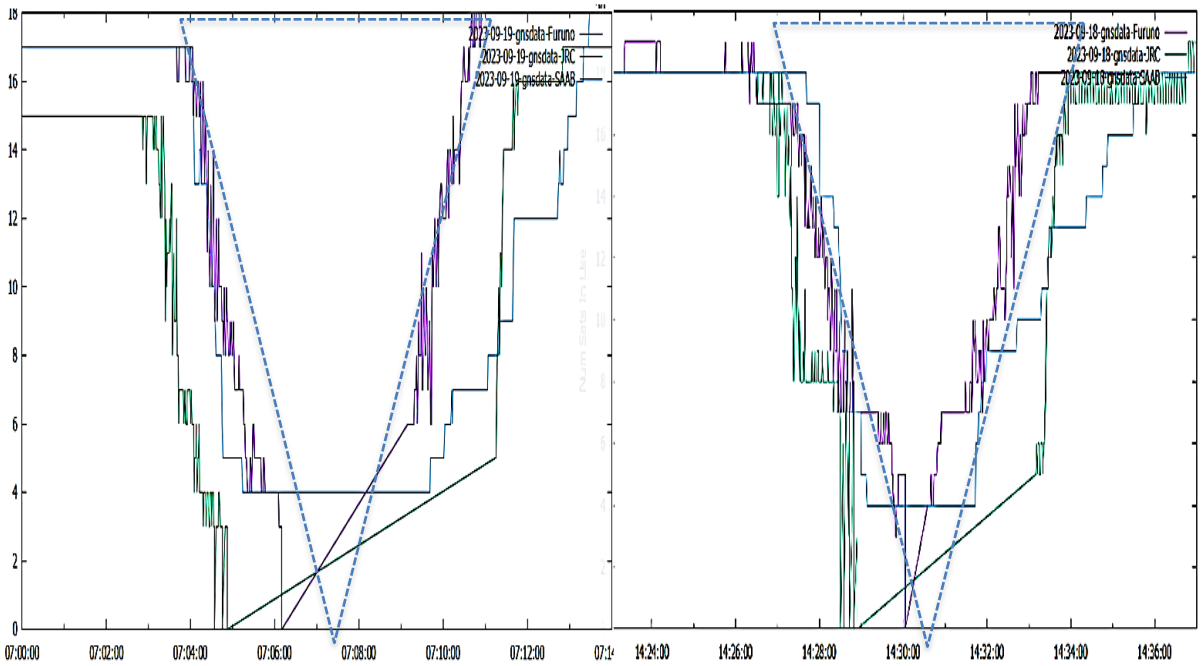
Start 10:30 (E6) og 11:30 (E5b)

E6	E5b, L5, E6, G2, L2, B1I, G1, L1
E6, E5b	E5b, L5, E6, G2, L2, B1I, G1
E6, E5b, L5	E5b, L5, E6, G2, L2, B1I
E6, E5b, L5, G2	E5b, L5, E6, G2, L2
E6, E5b, L5, G2, L2	E5b, L5, E6, G2
E6, E5b, L5, G2, L2, B1I	E5b, L5, E6
E6, E5b, L5, G2, L2, B1I, G1	E5b, L5
E6, E5b, L5, G2, L2, B1I, G1, L1	E5b
E6, E5b, L5, G2, L2, B1I, G1	E5b, L5
E6, E5b, L5, G2, L2, B1I	E5b, L5, E6
E6, E5b, L5, G2, L2	E5b, L5, E6, G2
E6, E5b, L5, G2	E5b, L5, E6, G2, L2
E6, E5b, L5	E5b, L5, E6, G2, L2, B1I
E6, E5b	E5b, L5, E6, G2, L2, B1I, G1
E6	E5b, L5, E6, G2, L2, B1I, G1, L1

Etter disse testene ble det gjennomført egen test med småjammere som blir beskrevet under avsnitt «Småjammere» for å undersøke hvordan realistiske småjammere kan påvirke SOLAS mottakere.
Deretter tilbake ved hovedlokasjonen. Fra 15:30 ble det gjennomført en meaconing test som følger:
0.1 W meaconing: 3 minutes
0.1 W meaconing: 3 minutes preceded by 5 min jamming (PRN GPS L1 + L2)
1 W meaconing: 30 seconds
1 W meaconing: 3 minutes
1 W meaconing: 3 minutes (repeat)
1 W meaconing: 3 minutes preceded by 5 min jamming (PRN GPS L1 + L2)
1 W meaconing: 15 minutes
1 W meaconing: 15 minutes (repeat)
1 W meaconing: 15 minutes preceded by 5 min jamming (PRN GPS L1 + L2)

5.2.1 Erfaringer

På første test ble det først jammet på L1 og så på både L1, G1, L2 og L5 med økende jammestyrke. Mottakerne som var innstilt på L1+G1 mistet fix før 20 watt var oppnådd. På første del holdt de noe lengre da det kun var jamming på L1. Furuno var den som holt posisjon lengst på L1-jamming. Alle hadde problemer med fix ved en jammeeffekt på ca. 1 watt. Ved jamming på 4 bånd begynner XR2 også å «flyte rundt» i posisjon og mistet posisjon på ca. 1,2 watt jammeeffekt ved jamming fra 1300 m.
Erfaringen fra pyramidetesten var at alle klarte seg bra når ikke L1 eller G1 var jammet samtidig. Dette er også naturlig da de var innstilt på G1-L1, men er viktig å få bekreftet. Dermed kan det saklig konkluderes med at det er lurt å ha en multikonstellasjonsmottaker når enkelte bånd kan være påvirket.
Det kan imidlertid se ut som om mottakerne kan slite med å holde fix på G1 når kun L1 er jammet, noe også andre tester viste. SAAB viste for eksempel 9 G1 satellitter, men hadde fortsatt ikke fix. Når man ser på PRN-spekteret FFI produserte, så ser man derimot at båndet er relativ bredt og kan «bløe» over til G1-båndet, som kan forklare dette. Der er allikevel interessant at SAAB ser satellittene, men klarer ikke å bruke disse.
Ved omvendt pyramidetest mister både JRC og SAAB fix når alle bånd utenom L1 ble jammet, altså inkludert B1I. Furuno klarte imidlertid å holde fix i samme periode. Som observert på testen på mandag har dette med at både L1 og G1 ligger nært og ved økning av jammeeffekt og båndbredde, vil alltid jamming på den ene også ta ut den andre.
Jamming fra Ramnan (altså jamming ovenfra) så ut til å være mer effektivt enn fra bakkenivå.



Figur 10: Venstre graf viser jamming fra Ramnan, høyre graf fra kirkegård. X-aksen=tid, Y-aksen=antall satellitter. Lilla(Furuno), blå (SAAB) og grønn (JRC). Blå prikket trekanter satt inn for å synliggjøre forskjell.

Figur 10 sammenligner reduksjon av satellitter ved jamming fra gravplassen som ligger i ca. samme høyde som mottakerne med jamming fra fjellet ca. 300 moh, (Line of sight ca 1300m). Her viser det at effektivt er større å bli jammet fra oven enn fra bakkenivå. På figuren til venstre som viser jamming fra Ramnan, forsvinner satellittene raskere, og kommer seinere tilbake enn på figuren til høyre.
Meaconing ble gjort med først kraftig (20 watt) jamming på L1 og L2 båndet etterfulgt av sending at ekte signaler som er sterkere enn originalsignalet. Signalene som ble videresendt

var også data fra hele L1 og hele L2 båndet.

Under meaconing testen ble mottakeren raskt lurt til å ta posisjonen til spooferen.
Å «ta over» mottakeren var definitivt lettere med jamming rett før spoofing, men SOLAS-mottakere lot seg også lure selv uten jamming først.
Under spoofing-testen analysert i avsnitt 5.4 hopper JRC rett til den spoofende posisjonen, men at de andre to ikke gjør det. Hvorfor dette skjer er vanskelig å si, men det er også observert tidligere at JRC har en tendens til å bli lurt tidligere enn de andre. Det har dog ikke vært mulig å finne noe fast mønster på dette sannsynligvis pga. kompleksiteten i scenariene, så denne observasjonen kan også være tilfeldig.

Det er interessant å nevne at en varierende spoofe-posisjon (tilsynelatende bevegelse av fartøyet) er mer overbevisende for mottakerne enn en statisk posisjon.
Denne type spoofing er det samme som fartøyer har sett i Svartehavet der posisjonen plutselig er inne på en russisk flyplass[1].

[1] https://nrkbeta.no/2017/09/16/over-20-skip-gps-hacket-i-svartehavet/

5.3 Småjammere

Selvvalgt test med småjammere ble gjennomført på tirsdag, onsdag og torsdag. Her ble det lagt opp til en test der det var mulig å måle nøyaktig hvorledes forskjellige småjammere påvirket mottakerne. Avstand ble målt med laser. Jammer startet på ca. 260 m og bevegde seg sakte mot mottakerne.

5.3.1 Småjammere brukt i vår (private) test

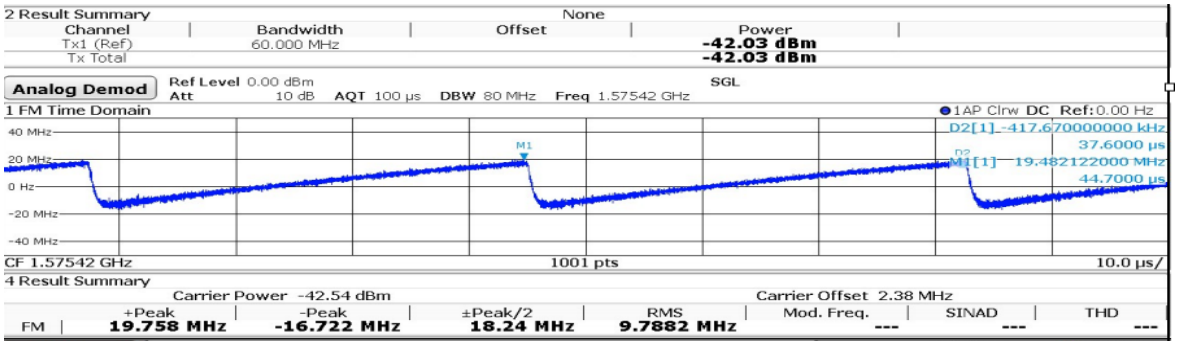
Merkingen av laveffekt småjammere ble gjort som følger:

1st Letter (Norwegian / English)	1st digit	2nd digit
S = Sigarett / Cigarette	**Number of antennas**	**# jammer within same category**
H = Håndholdt / Handheld		
U = USB / USB stick		
F = Fastmontert / Permanently installed (Fixed)		

5.3.1.1 S1.1, S1.2 og S1.3

Jammere merket S1.1 to S1.3 er en kategori jammere som ofte installeres i sigarettenneruttaket i biler.

Centre frequency (MHz)	Bandwidth (MHz)	Potentially afflicted GNSS bands
1575	30 - 40	L1, E1, B1I, B1C



Figur 11: Eksempel på målinger av S1, S2 og S3 jammere

Estimert utgangseffekt er 10 - 15 dBm (O,03-0,1 watt). Type modulasjon er sweep med sweep hastighet på 22 - 37 µs.
Disse er ment å dekke bilen, og en gitt radius rundt bilen.

5.3.1.2 S 2.2 og S 2.3

Centre frequency (MHz)	Bandwidth (MHz)	Potentially afflicted GNSS bands
1575	70 - 90	L1, E1, B1I, B1C, G1
1227	70 - 90	L5, E5a/b, B2a/b, G3

Estimert utgangseffekt på 15-20 dBm (O,03-0,1 watt), modulasjon er sweep med sweep-hastighet på 40 - 60 µs.

5.3.1.3 H 1.1

Novatels NEAT-jammer er en kommersiell multifrekvens-multimodulasjonstype jammer med lav effekt for GPS L1 og L2. Det kan velges mellom lav og høy utgangseffekt.
I vår test ble det valgt WB L1 – Bredbånd L1 BPSK-modulert med ca. 10 MHz PRN-kode og båndbredde, 20 MHz. Utgangseffekten i high power var 20 dBm (0,1 watt)

5.3.1.4 H 1.2

Centre frequency (MHz)	Bandwidth (MHz)	Potentially afflicted GNSS bands
1575	20	L1, E1, B1C

Utgangseffekt er estimert til 18 dBm (0.063 watt). Type modulasjon er sweep med sweep hastighet på 6 µs.

5.3.1.5 H 3.1 og H 3.2

Centre frequency (MHz)	Bandwidth (MHz)	Potentially afflicted GNSS bands	Relevant GNSS antenna #
1575	23-27	L1, E1, B1C, B1I	2

Disse er GPS L1 jammere som samtidig kan jamme mobile bånd som GSM og DCS. Utgangseffekt er estimert til 20 dBm (0.1 watt). Type modulasjon er sweep med sweep hastighet på 6 µs.

5.3.1.6 F 6.1

Centre frequency (MHz)	Bandwidth (MHz)	Potentially afflicted GNSS bands	Relevant GNSS antenna #
1591	68	L1, E1, B1C, B1I, G1	2
1589	72	L1, E1, B1C, B1I, G1	3
1242	80	L2, G2, B3I, B2b, E6	4
1176	17	L5, E5a, B2a	6

Dette er en jammer som bruker 220 volt så batteribank ble medbrakt, altså ikke en håndholdt jammer.
Estimert utgangseffekt er mellom 35 dBm (3,1 watt) og 27 dBm (0,5 watt) avhengig av antenne. Modulasjon er sweep med sweep-hastighet 5-7 µs.
FFI opplyser at de mest vanlige småjammere bruker nesten alle signaltypen chirp og sweep.

5.3.2 Gjennomføring av testene med småjammere

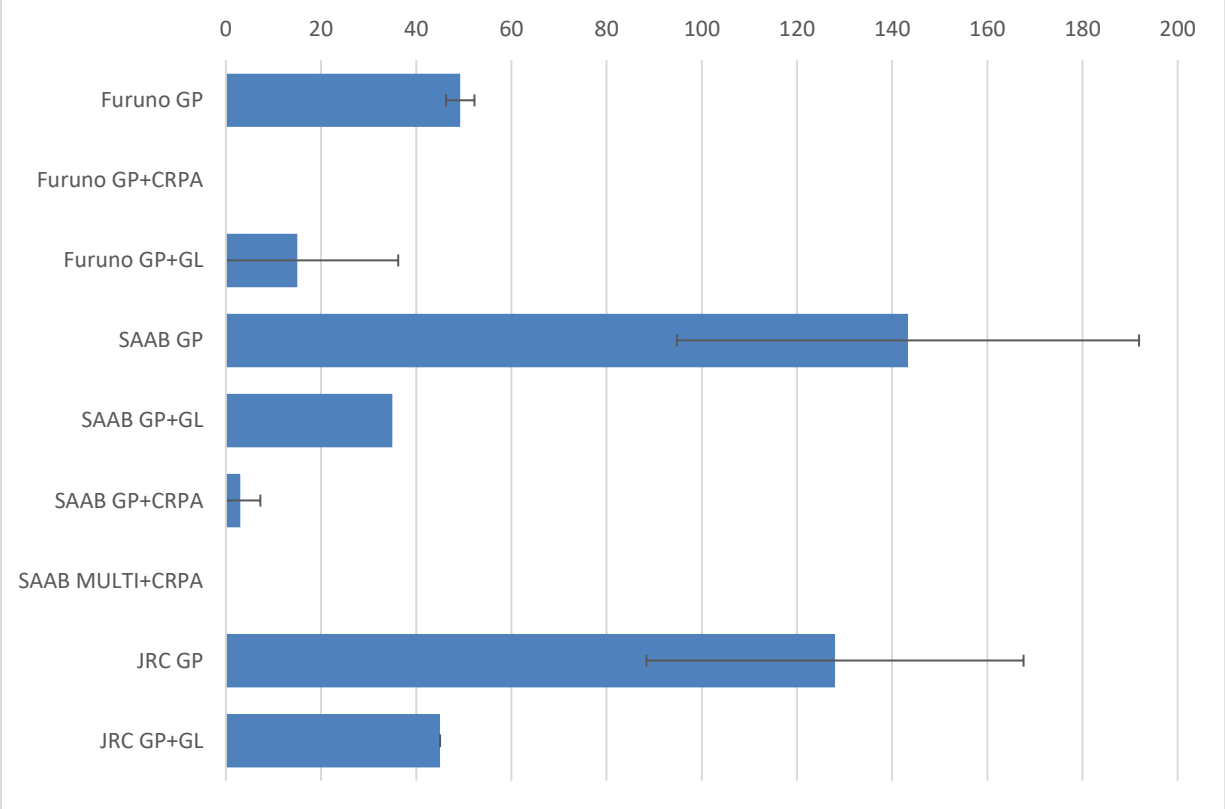
Testene ble gjennomført kun for oss der vi kunne bestemme jamme scenario og hvilke jammere som skulle brukes. De jammerne som ikke klarte å jamme ut noen mottakere før på under 3 meters avstand ble ikke gjentatt. Der jammerne ga effekt på flere meters avstand ble det gjort flere like tester for å øke kvaliteten på resultatene og eventuelt for å kunne beregne et standard avvik for avstandsavhengigheten.
Testene der mottakerne sto stille ble alle gjort på samme måte. Jammeren startet i en avstand på 265 meter og bevegde seg sakte mot mottakerne, enten ved at en person bar jammeren eller at den var inne i en bil.
Det ble kun gjennomført jamming på GPS L1, da det er mest vanlig ved småjammere.
Det ble også gjennomført tester ved at mottakerne beveget seg og jammerne sto stille. Disse dataene er ikke analysert i denne rapporten.

5.3.3 Erfaringer

5.3.3.1 Novatels NEAT-jammer, H1.1

Det ble testet med håndholdt jammer, H1.1, som ble satt til jamming på GPS, Bredbånd og high power (0,1 watt). Low power ble testet først, men hadde veldig lite effekt, så resten av testene forgikk i high power modus. Jammeren ble båret av en person som beveget seg mot mottakerne. Mottakerne var plassert som tidligere beskrevet.

Figur 12 viser resultatet med denne jammeren som var denne kraftigste bærbare jammeren i testen.
Når mottakerne var innstilt på GPS alene (GP) viser testen at Furuno var den som holdt lengst (50m) mens SAAB og JRC mistet fix på ca. 130-140 meter (med større standard avvik). Testen viste også klart at det hjelper å bruke GPS og Glonass, der jammeren måtte flyttes til mellom 15-45 meter for effektiv jamming, igjen med Furuno som mest robust mottakeren. Med CRPA antenne var det i praksis ikke mulig å bli jammet ut, allerede når bare GPS er i brukt som konstellasjon. Kombinasjon av GPS og GLONASS og CRPA-antenne er best, som er tydelig for SAAB-mottakeren. Ved Furuno-mottakeren var GP og CRPA-antenne nok for å unngå å bli jammet av denne jammeren. JRC har en annen antenne-kabel og kunne derfor ikke bli testet med CRPA-antennen.



Figur 12: Viser hvilken avstand i meter der mottakerne mistet fix samt standard avvik på bakgrunn av at noen målinger ble gjort flere ganger

5.3.3.2 Sigarettenner jammerne, S1.1, S1.2, S1.3, S2.2 og S2.3

Alle mottakerne var her satt til GPS alene og jammingen startet på 247 meter.
Figur 13 viser resultatet fra testen med jammere som var plassert i sigarettenneren i en bil som kom sakte imot mottakerne. Mottakerne var plassert som tidligere beskrevet. Det er kun SAAB som viser en reduksjon i antall satellitter og mister fix til slutt, dog veldig nært mottakeren. JRC viste også at det var interferens ved at HDOP alarm kom på ca. 140 meter, men holdt fix hele veien.

	S1.1	S1.2	S1.3	S2.2	S2.3
Furuno	0	0	0	0	0
SAAB	3	10	6	10	10
JRC	0	0	0	0	0
ADQ2	0	0	0	0	0
XR2	0	0	0	0	0

Figur 13: Oversikt over sigarettenner jammere. Tallene viser avstand i meter der mottakerne mistet fix. 0=aldri jammet ut.

5.3.3.3 H 3.1 og H 3.2, håndholdte jammere

Figur 14 viser resultatet av 2 like håndholdte jammere på 0,1 watt. Mottakerne var her stilt inn på GPS alene og avstanden til jammer startet på 265 meter fra mottakerne.

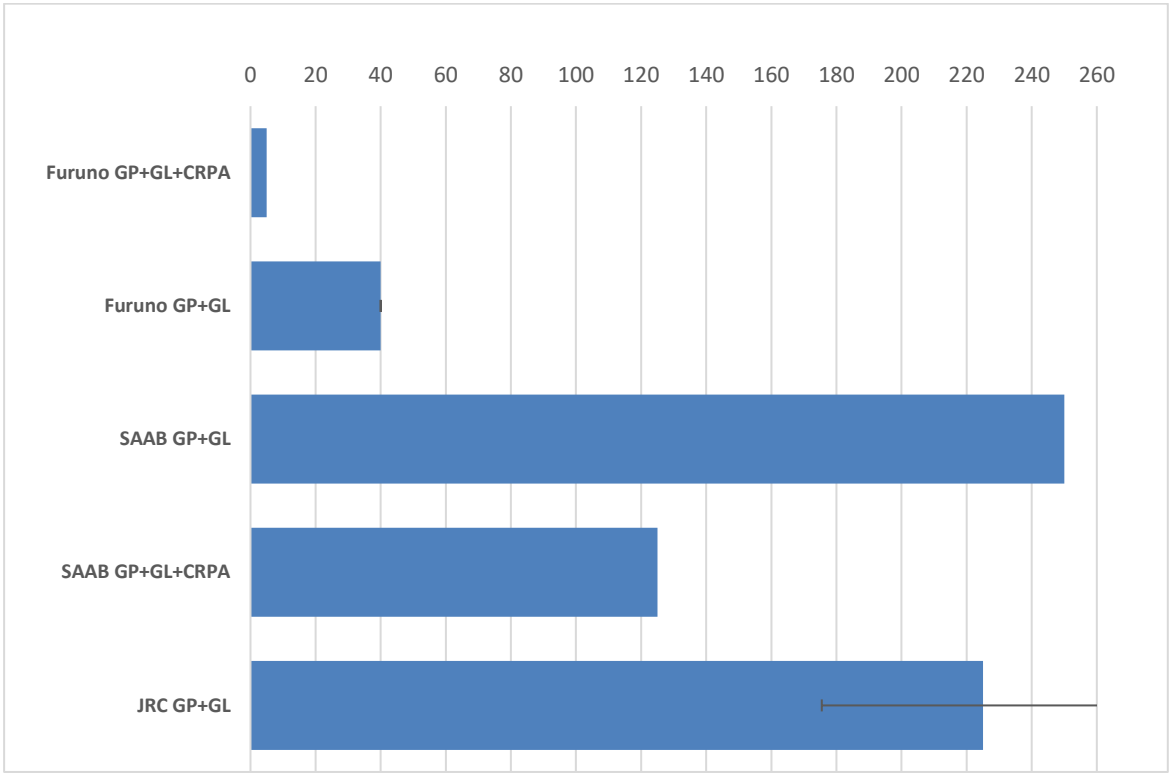
	H3.1	H3.2
Furuno	52	50
SAAB	52	122
JRC	27	50
ADQ2	0	0
XR2	0	0

Figur 14: Oversikt over håndholdte jammere H3.1 og 3.2. Tallene viser avstand i meter der mottakerne mistet fix. 0=aldri jammet ut.

Ingen av mottakerne hadde CRPA antenne. Mottakerne blir her jammet ut tidligere enn ved sigarettenner jammerne. Dette selv om utgangseffekten ikke er veldig stor, 15-20dBm på denne testen og 20 dBm på forrige.
Forskjellen er heller at disse jammerne var ut av bilen uhindret og dermed ble ikke signalet redusert av bilen.
JRC klarer seg noe bedre enn Furuno og SAAB sammenlignet med jamming fra NEAT jammeren. Hvorfor dette skjer er vanskelig å si, men den generelle erfaring er at JRC godtar dårligere kvalitet på signalet sammenlignet med SAAB som er mer kresen på kvaliteten på signalet og mister dermed fix tidligere.
Da det ikke er mulig å få tilgang til hvorledes de forskjellige mottakerne prosesserer, hvordan filtrene virker og hvordan de generelt er programmert er det vanskelig å analysere noe nærmere.
ADQ2 som har GPS og Glonass og XR2 som bruker alle 4 konstellasjoner klarer seg også her bra. Det viser også at det er en veldig liten og diffus grense for når jamming påvirker og når det ikke påvirker mottakerne.

5.3.3.4 F 6.1, Stasjonær jammer

F 6.1 er en jammer som går på 220volt så den er ikke like «bærbar». Den ble allikevel tatt med i testen da den hadde noe høyere utgangseffekt på ca. 3 watt, og fordi den jammer flere konstellasjoner samtidig. Scenariet var det samme ved at personene bar med seg en power-bank. Jammer ble her gjort på mange bånd og jammer startet på 260 meter.

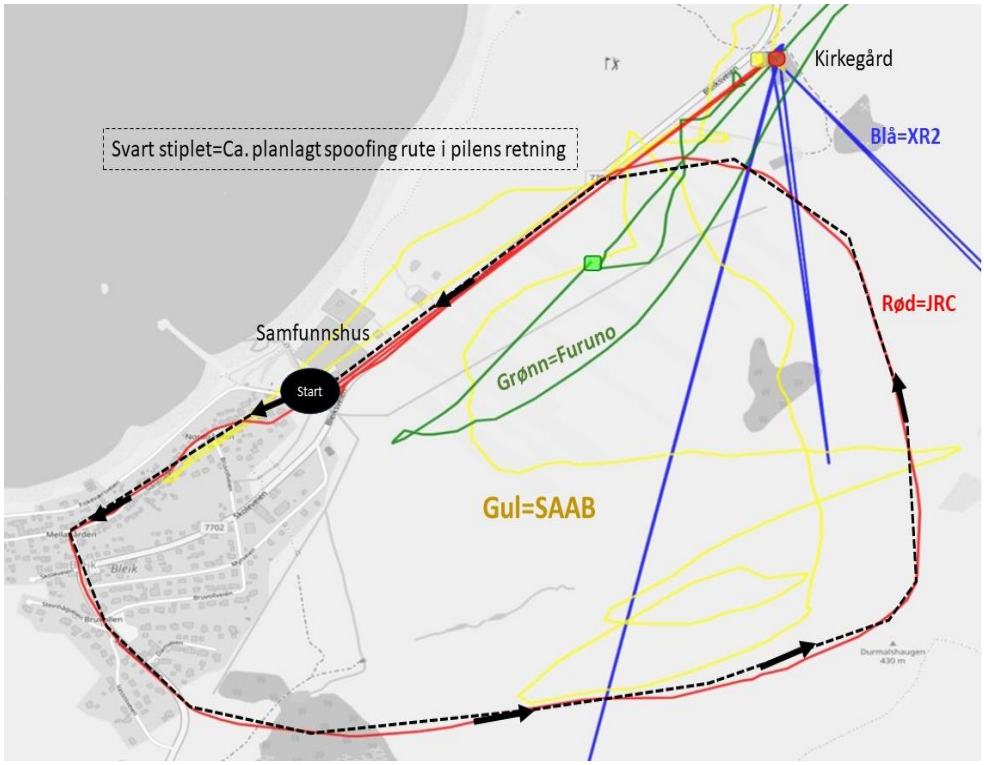


Figur 15: test med jammer F6.1. Ca 3 watt. Viser avstand i meter hvor mottakerne mistet fix. Svart strek er standard avvik.

Furuno og SAAB ble her prøvd med og uten CRPA antenne. Begge gangene holdt de fix lengre, men for Furuno sin del var forskjellen kun 35 meter. Selv om Furuno er rimelig robust fra før gir CRPA er ytterlige forbedring.
Testen viser også at ved denne styrke og bredde (bredere en bare L1) på jammingen blir både GPS L1 og Glonass L1 slått ut selv om jammingen forgår på GPS L1. SAAB viser seg igjen som den mest sensitive av de 3.

5.4 Spoofing

Det ble gjennomført forskjellige typer spoofing der erfaringen var at mottakerne som hovedregel ble lurt når det var jamming først. Her presenteres bare en av spoofing-testene, som eksempel. (bevegelsene finnes også som film)
I starten var mottakerne (bilen) plassert ved samfunnshuset hvor jammingen ble for sterk. Ny posisjon ble derfor til kirkegården ca. 800 meter unna jammeren som var ved samfunnshuset. Mottakerne/bilen var stasjonær.



Figur 16: Bevegelsesmønsteret på de forskjellige mottakerne ved spoofing. Bevegelsene finnes også som film. JRC følger hele den spoofede ruten (stiplet linje)

JRC og Furuno var satt til GPS og Glonass, SAAB i GPS alene med DGPS.
Scenariet var laget slik at det var først jamming etterfulgt av en fast posisjon markert med «Start» i figur 16. Deretter ble det sendt falske posisjoner som utgjorde en rute langs den prikkede linjen.
SAAB og JRC ble jammet ut umiddelbart. Furuno var koplet til CRPA og ble ikke jammet ut. Når spoofingen (falsk posisjon) startet flyttet JRC seg umiddelbart til spooferens startsted (samfunnshuset). SAAB flyttet seg også i nærheten av startsted, men hoppet litt rundt. Når posisjonen som utgjorde ruten ble sendt fulgte JRC spooferen nøyaktig. SAAB begynte også å bevege seg, men den tok muligens hensyn til både ekte og spoofede/falske satellitter som gjorde at den beveget seg, men fulgte aldri ruten nøyaktig, men etter hvert fulgte den rette bevegelser (kurs og fart) men ikke rette posisjoner.
Furuno hoppet til en ny posisjon når spooferen sendte start posisjon, og begynte så å hoppe rundt/sveve når spooferen kjørte sin planlagte rute. Da den ikke ble jammet ut før spoofing er det naturlig å tenke at den hadde noen ekte satellitter som ble med i kalkuleringen når den ble spoofet.
XR2 gjorde store hopp til ny posisjon langt borte for så å hoppe tilbake til rett posisjon. Dette skjedde flere ganger.
Mottakerne oppførte seg denne gangen svært forskjellige slik det kommer frem i Figur 16, så innstillinger og valg av mottaker har potensielt en del å si for hvordan spoofing påvirker posisjoneringen.

6 Konklusjon

Hovedmålsettingen med testen var å måle hvor robust mottakerne var mot småjammere som kan befinne seg i nærheten av en maritim mottaker. Eksempler på dette kan være i biler på fergen, broer, havneområder og fra land i trange sund. Testene viser at disse jammerne kan påvirke en maritim mottaker, særlig hvis de kun har mulighet til GPS L1, noe som antas at de fleste har.

Testen viste også at de såkalte sigarettenner jammerne ikke hadde noe særlig effekt på mottakerne, men med kun marginalt større effekt og hvis jammeren ikke er inne i en bil, er effekten vesentlig større. Dessuten ble det observert – ved rampe-testene – at jamming fra høyere elevasjon har større påvirkning, så jamming f.eks. fra en bro vil også ha større effekt enn fra bakkenivå.

CRPA virket etter hensikten og avstanden mottakerne ble jammet ut på ble redusert. Testene ila uken viste også at mottakerne blir mer robust ved å ha to eller flere bånd selv om de ligger ganske nært hverandre i frekvens slik solas-mottakerne gjør. XR2 som har 4 konstellasjoner og bruker frekvenser over hele båndet er mye mer robust enn Solas-mottakerne. ADQ2 som bruker GPS og Glonass har også vist seg å holde fix lengre enn de godkjente mottakerne.

En kombinasjon av flere konstellasjoner og CRPA-antenne er det mest robuste av de innstillingene som ble testet med hensyn til SOLAS-mottakerne.
Jammeøvelsen viste også at mottakerne, på tross av de er på samme nivå og sertifiserte mottakere, håndterer interferens svært forskjellige (Har antakeligvis svært forskjellige algoritmer, vekting av filtre og arkitektur). Dette har effekt på reaksjonene både ved jamming og spoofing. Eksempel på dette er at SAAB blir lettere slått ut av jamming, men gjør det omtrent like bra som Furuno ved spoofing. JRC blir lett overtalt av spoofing men holder et hakk bedre ved jamming.

Det så også ut som om jamming er mer effektiv når jammeren har større høyde over havet enn når jammer og mottaker er på samme nivå, selv ved lengre avstand. I begge tilfeller er det 'line of sight' mellom mottakere og jammer. Hvorfor dette skjer er ikke avklart, men det kan kanskje ha noe med antennediagrammet som er formet som en halvkule og er rettet mot himmelen. Det kan dermed være mer gain ved høyere, enn lavere elevasjon over horisonten. Om jammesignalet som går langs bakken på en måte blir redusert, reflekter el. vites ikke.

Alle mottakerne lot seg lure av spoofing som potensielt kan være en trussel for eksempel om bord på et passasjerskip. Spoofing med jamming i forhånd er det mest effektive, og det er vanskelig å se hvordan man skal kunne unngå å bli lurt da hvis spoofer er i nærheten av riktig posisjon. Men, samtidig kan det være lettere å oppdage spoofing, f.eks. ved at posisjonen plutselig gjør et hopp eller drifter kraftig.

Det ser ikke ut som om det er noe innebygget avhengighet av hverken GPS L1 eller GLO L1. Testene viste at mottakerne klarte å holde fix med både G1 alene og L1 alene. Det kan virke som om forstyrrelser i G1-båndet er mer skadelige enn i L1-båndet når mottakerne står til GPS+Glonass, men dette er ikke undersøkt godt nok ennå. På den annen side er ikke forstyrrelser i G1 båndet like forstyrrende når mottakerne er satt til GPS L1 alene.