Jammetest 2022

Rapport på jamming og spoofing av GNSS-utstyr og GNSS-baserte systemer på Andøya

Nkom, Statens vegvesen, FFI, Justervesenet

Mars 2023

Sammendrag

Jammetest 2022 ble gjennomført i uke 38 (19-23.09.22) på Andøya i Vesterålen. Hensikten var å kunne tilby et testopplegg til industri, akademia, forsvarsaktører og offentlig sektor, hvor deltagere kunne utsette systemene og rutinene sine for jamming og spoofing av GNSS under kontrollerte forhold.

Denne rapporten gjennomgår arrangementet; bakgrunn, hensikt og oppsummering av testaktivitetene, og går så gjennom noen av resultatene på et overordnet nivå. Den gjør deretter en kort evaluering og legger fram en anbefaling rundt et mulig lignende arrangement i framtiden ('*Jammetest 2023*').

Innholdsliste

1 Bakgrunn

Jammetest 2022 var et arrangement som samlet industri, akademia, forsvarsaktører og offentlig sektor for at deltagere kunne utsette systemene og rutinene sine for jamming og spoofing av GNSS under kontrollerte forhold. Dette skjedde i uke 38 på Andøya i Vesterålen.

Bakgrunnen for testene var arrangementet Testfest 2021, som var et Vegvesen-initiert opplegg med de samme hensiktene som årets Jammetest, men i mindre skala og gjort i Skibotndalen i Troms. Tankene bak Testfest og Jammetest 2022 oppstod etter diskusjoner gjort i Samordningsforum for GNSS.

Arrangørene av Jammetest 2022 var Statens vegvesen (SVV), Nasjonal kommunikasjonsmyndighet (Nkom) og Forsvarets forskningsinstitutt (FFI). Det ble leid inn støttefunksjoner for prosjektledelse, praktisk håndtering og kommunikasjonsarbeid gjennom tromsøfirmaet Testnor, og Justervesenet bisto arrangørene med teknisk gjennomføring av spoofingtester.

Definisjoner brukt i denne rapporten:

- GNSS – Global Navigation Satellite System, globalt satellittnavigasjonssystem. Fellesbetegnelse for satellittsystemer som tilbyr posisjonsbestemmelse, navigasjon og tidsbestemmelse (PNT). Eksempler er GPS (USA), Galileo (EU), Glonass (Russland) og Beidou (Kina).
- Jamming – elektromagnetisk støysending på en bestemt frekvens eller et bestemt frekvensområde («frekvensbånd») for å forstyrre for den legitime tjenesten som bruker disse frekvensene til (trådløs) kommunikasjon eller radionavigasjon.
- Spoofing – narring av en mottaker ved å sende signaler som simulerer den tjenesten man ønsker å narre, med det mål å kunne lure mottakeren til å prosessere disse falske signalene i stedet for de ekte (fra for eksempel satellittene).
- Høyeffektsjamming – Jammetransmisjoner fra en stasjonær signalgenerator med en fast direksjonell antenne, med en utgangseffekt på maksimum 20 W.
- Laveffektsjamming – Jammetransmisjoner fra håndholdt jammerutstyr (lik det som er tilgjengelig på Internett) med rundtstrålende antenner, med en utgangseffekt på maksimum 1 W.

2 Hensikt

Formålet med Jammetest 2022 var tredelt:

- Å kunne tilby testområder for storskala GNSS-jamming og -spoofing i felt, under kontrollerte forhold i den virkelige verden (med veier, terreng, bebyggelse, osv.). Deltagere kunne på det viset teste nøyaktighet, tilgjengelighet og robusthet til systemer/rutiner/nye teknologier, og testene skulle på det viset være med på å tilrettelegge for ny og mer robust teknologi.
- Å øke kunnskapen og forståelsen for de negative konsekvensene ved ulovlig GNSS-jamming og -spoofing hos privatpersoner, myndigheter og industri, samt demonstrere sårbarheter/robusthet gjennom å aktualisere/avkrefte teoretiske problemstillinger.
- Bidra til synliggjøring av proaktivt samarbeid på tvers i staten om et komplisert og sammensatt problem (GNSS-jamming og -spoofing), samt bidra til å anskueliggjøre Norge som et land som tar slike problemer på alvor, og hvor industri o.l. kan gjennomføre viktige tester de ikke får anledning til andre steder.

«*Jammetest er en arena for eksperimentering. Arenaen samler problemeiere og problemløsere og skal bidra til at industrien og andre utfordres til å løse relevante samfunnsutfordringer ved at løsninger utvikles i tett samarbeid med problemeier. Videre skal Jammetest bidra til samarbeid, tiltrekke relevante miljøer og bidra til økt kommersialisering av teknologi.*»

- Tomas Levin, sjefsingeniør i SVV

Gjennom å utforske for eksempel hvordan jamming i forskjellige sammensetninger (av utstrålt effekt, frekvensbånd og signalmodulasjoner) påvirker forskjellige teknologier, kan man utforske sammenhenger i de underliggende systemene og oppdage hvilke parameter som gir indikasjon på hvilke angrep.

Bakgrunnen med å legge testene til Andøya var fordi forholdene for å gjennomføre slike tester uten å forstyrre resten av samfunnet, er særlig gunstige her. Her er det høye fjell i riktig formasjon som minimerer signalutbredelsen, og lite flytrafikk og et lite sivilsamfunn som blir forstyrret av testene.

2.1 PNT-strategien (2018)

I regjeringens PNT-strategi av 2018 blir områder som «utnytte nye muligheter og ivareta norske interesser internasjonalt», «bidra til bevisstgjøring rundt avhengighet av PNT-tjenester», «bidra til å forebygge forstyrrelser og svikt i PNT-systemer» og «bidra til å sette samfunnet i stand til å takle svikt i PNT-tjenester» alle dratt tydelig frem som noe daværende regjering og departementsnivå ønsket at Norge skulle jobbe med. Disse formålene har blitt videreført inn i ny regjering og i 2022.

Jammetest 2022 bidrar til å oppnå disse formålene gjennom å skape internasjonalt samarbeid om testing av eksisterende og nye tekniske muligheter, skaper bevisstgjøring gjennom kommunikasjon om testenes hensikt og resultater, og hjelper til med å utvikle nye og/eller mer robuste PNT-/GNSS-løsninger slik at samfunnet er bedre i stand til å takle svikt i systemer som baserer seg på PNT/GNSS.

3 Oppsummering av testuka[1]

3.1 Oversikt over testområder

Figur 1: Kart som viser de hvor på Andøya testene foregikk.

Som vist i Figur 1 ble testene gjennomført i området rundt Bleik på Andøya (indikert med rødt). Innenfor dette området ble sendeutstyret i all hovedsak plassert ut på to områder:

- Hovedtestområdet (i grønt), rundt Bleik kirkegård og Bleik Samfunnshus
- Sekundært testområde ved Grunnvatn (i gult)

I tillegg til dette var bilkjøring tillatt i hele (det røde) område, mens flyving var begrenset til området rundt Bleik.

[1] For mer informasjon om angrepsmetodikker, se Tillegg 1.

3.2 Dagsprogram

Dag	Tema
Mandag	Del 1 (hovedtestområde): Referansetester av laveffektsjammere (medbrakt av Nkom og FFI); jammere 1 til og med 14 og høyeffektsjamme-signaltypene (generert av FFI); L1, G1, L2 og L5 i forskjellige kombinasjoner og med kombinasjoner av CW- og PRN-modulasjoner (eks: L1, G1 PRN). Del 2 (sekundært testområde): Langtidsjamming med laveffektsjammer.
Tirsdag	Del 3 (hovedtestområde): Rampetester/sensitivitetstester (med høyeffektsjamming i forskjellige kombinasjoner av frekvensbånd og modulasjoner), langstidsjamming med samme oppsett som mandagen, og «pyramidejamming» med høyeffektsjammeren. Del 4 (sekundært testområde): Jammere som ikke var i bruk ved hovedtestområde ble brukt «fritt», under styring av en representant for arrangørene.[2]
Onsdag	Del 5 (hovedtestområde): Aktiv bilkjøring, både fritt (under langtidsjamming) og organisert (jammere i bil og lignende scenarioer). Del 6 (sekundært testområde): Jammere som ikke var i bruk ved hovedtestområde ble brukt «fritt», under styring av en representant for arrangørene.
Torsdag	Del 7 (hovedtestområde): Spoofingtester, med spoofingangrep (både inkoherente og koherente angrep) i kombinasjon med innledende og underveis-kontinuerlig jamming fra laveffektsjammere på forskjellige frekvensbånd. Både posisjon og tid ble spoofet. Del 2 (sekundært testområde): Jammere som ikke var i bruk ved hovedtestområde ble brukt «fritt», under styring av en representant for arrangørene.
Fredag	Del 8 (hovedtestområde og sekundært testområde): Oppsummeringstester. Disse innebær for eksempel statiske tester med

[2] Det å sende på frekvensområder tildelt GNSS (satellite-to-earth-reception), eller å unødvendig forstyrre for frekvensbruk hvor GNSS deler frekvenser med andre tjenester, er ulovlig bortsett fra for Forsvaret eller Politiet, og da kun ved en godkjent frekvenssøknad av Nkom. Under Jammetest 2022 var det FFI som hadde juridisk lov til å bedrive støysendinger, ettersom det var FFI som var innehaver av frekvenstillatelsen fra Nkom. FFI delegerte så ansvar til andre arrangørrepresentanter under testene i de tilfellene en FFI-representant ikke kunne være til stedet.

	en eller flere laveffektsjammere, blant annet plassert ut i terrenget, bilkortesjetester med jammere i bil, gjentagelse av noen spoofingscenarioer og jamming mot satellitt for test av satellittkapabilitet til å oppdage interferens på bakken.

Tabell 1: Oppsummering av testaktivitetene som ble gjennomført under Jammetest 2022 på de forskjellige dagene.

4 Resultater

Dette kapittelet oppsummer noen overordnende observasjoner fra testene, samt noen tilbakemeldte resultater. Det gir ikke en total beskrivelse av resultatene fra alle testene til alle aktørene som deltok, men gir et inntrykk av hva slags resultater og erfaringer som aktørene fikk med seg. Det skal også gi andre noen idéer til hva de kan teste og/eller undersøke sine egne systemer med, for å se om de opplever de samme problemene. Første delkapittel, 4.1, gir et innblikk i de overordnede observasjoner. De to påfølgende delkapitlene, 4.2 og 4.3, gir et par anonymiserte, konkrete eksempler. Delkapittel 4.4 tar med andre ting som ikke passer inn i de foregående, og delkapittel 4.5 gir kontaktinfo for tilgang på måledatasett fra noen deltagere.

– *Både brukere og produsenter får testet ut sitt eget navigasjonsutstyr i et realistisk miljø hvor signalene fra GPS eller andre satellittnavigasjonssystemer er forstyrret, forfalsket eller rett og slett utilgjengelige*, oppsummerte Anders Rødningsby i Forsvarets forskningsinstitutt til Inside Telecom. [3]

4.1 Overordnede observasjoner

På et overfladisk nivå kan man si at det er veldig tydelig at noen systemer står bedre imot jamming- og spoofing-angrepene enn andre, og deltagerne fikk noen indikasjoner om hva som gjør noen systemer robuste, og hva de systemene som enklere har latt seg ta over, mangler for å stå imot spesielt spoofing. For eksempel så ved å forfalske – eller spoofe – GNSS-signalene, klarte man blant annet å få biler som stod helt i ro på flatlandet ved Bleik til å tro at de var ute og kjørte på fjellet. Når bilene så begynte å kjøre, kunne man se at en del av systemene i bilene raskt merket at noe var galt, og prøvde å korrigere, slik at kartvisningen i bilene lugget. Men til slutt lot noen av systemene seg lure av de falske signalene, og fortsatte visningen av den falske, spoofede ruta.

En av de nevnte indikasjonene er at noen navigasjonssystemer blir ekstra sårbare fordi de lener seg tyngre på GPS enn andre GNSS-systemer. Navigasjonssystemer som også skal kunne hente inn informasjon fra andre satellittsystemer, og på andre frekvensbånd enn de man prøvde å spoofe, vektla ofte GPS-signalene så mye at de lot seg lure av spoofede GPS-signaler i stedet for å bruke andre data til å korrigere feilen. Ofte kunne de til og med basere seg på at de måtte ha fix på i hvert fall én GPS-satellitt før mottakeren ville bruke de resterende (ujammede ikke-GPS-signalene). Derimot så kom det også fram at forskjellige innstillinger (enn default) i utstyret vil påvirke dette. Som en deltager sa: «If multi-constellation receivers are designed to be “reliant on” GPS L1, this is a serious matter that might reduce the resilience, making the use of multi-constellation receivers [somewhat] pointless [in a security perspective] ». Derimot så ble det bekreftet på andre multibåndsmottakere at disse falt tilbake på andre frekvensbånd når for eksempel GPS L1 ble jammet ut, så dette er utstyrs- og systemavhengig.

En annen interessant observasjon var at noen mottakere prøvde desperate å holde på GNSS-fix i jamming-RF-miljøer. Dette gjorde at de opplevde små til enorme unøyaktigheter (heller enn å beslutte å ikke bruke satellittsignalet lengre), av og til opp til flere titalls kilometer. Slike feil kan også oppleves som spoofing, selv om de skyldes signaljamming. Det var også veldig forskjell i hvor lang tid mottakere

[3] https://www.insidetelecom.no/artikler/omfattende-jammetester-pa-andoya/522377

(og systemene de var implementert i) trengte på å komme seg igjen (få ny GNSS-fix) etter jamming- og spoofing-angrep, alt fra nesten med en gang, forbi noen få minutter og til aldri (måtte en restart til).

For spoofingens del var det veldig tydelig at ved inkoherent spoofing klarte mange mottakere å beholde GNSS-fix, men ved koherent spoofing ble de aller fleste mottakere lurt (om de ikke hadde spesielle ekstrating, som implementerte andre sensorer eller spesialdesignede «brannmurer»). Det var også variasjoner i hvor fort de ble spoofet (og om de ble det overhode) ut ifra om de hadde god GNSS-fix før spoofingen startet. Et eksempel på forskjellen mellom inkoherent og koherent spoofing var at mobiltelefoner som i utgangspunktet skulle bruke alle GNSS, ble ikke spoofet av inkoherente angrep før man skrudde av A-GPS (støttefunksjon for å bruke nærmeste mobilbasestasjon til å gi riktig posisjon/raskere TTFF), men da ble den og spoofet av reine GPS L1-only og Galileo E1-only spoofingsignaler. Ved koherente angrep ble mobilene lurt med en gang, selv med A-GPS skrudd på.

På tidssiden ble det observert at enkle GNSS-tidstjenere vil akseptere ethvert spoofet GNSS-signal. Noen ganger tar det litt tid før de locker på det spoofede signalet, men etter hvert skjer det. Mer sofistikert utstyr, med innebygde kontrollalgoritmer og/eller sammenligninger med andre kilder vil detektere at noe er galt og dermed gå i holdover, hvor de bruker interne oscillatorer. Her var det også forskjell fra type til type, og noen angrep påvirket de forskjellige tidstjenerne ganske forskjellig.

En annen interessant observasjon er at høypresisjonsutstyr, som svært følsomt geodetisk landmåleutstyr, kan være mye mer påvirkelig enn billigere mottakere, eller spesielle mottakere installert i større system (som biler). Dette skyldes enten sensorfusjon i større systemer, eller at billigere mottakere ofte kan ha et kompromiss med nøyaktigheten i forhold til tilgjengeligheten, mens høypresisjonsutstyr har det heller motsatt. Slike kompromisser gjelder for eksempel i mobiltelefoner, men de som testet på mobiltelefoner fikk som overordnet erfaring at selv små laveffekts-jammere kan være overraskende effektive. Den samme trenden ser man i forhold til mottakeres evne til å komme seg igjen etter spoofingangrep. Noen mottakere ble dyttet over i uopprettelige tilstander av spoofingen. For eksempel begynte en mottaker å rolig drifte oppover etter spoofing, og fikk aldri mer satellittkontakt enn fem Glonass-satellitter, selv timer etter at det var slutt på spoofing og jamming. Dette antyder at noen mottakere, som kan ha en 'sanity check', ikke har konseptuell forståelse for en 'insanity check'. Altså så kan selve spoofingangrepet vare i noen få minutter, men innvirkningen fra angrepet kan vare i timer(?), dager(?) eller til når systemet blir startet på nytt(?).

Resultatene fra Jammetesten ble også brukt inn i en konseptvalgsutredning om vegprising. Her ble det blant annet nevnt at[4]

- En jammer inne i et kjøretøy vil hindre GNSS-signaler for de om bord-løsninger vurdert, og tilleggsmuligheter for posisjonsbestemmelse er derfor nødvendig.
- En jammer i et kjøretøy før eller etter aktuelt kjøretøy blokkerer ikke i særlig grad for GNSS-signaler brukt i de vurderte om bord-løsninger.
- En jammer i et kjøretøy som passerer i motsatt retning forstyrrer kun i en kort periode, avhengig av fart, men vanligvis kun i noen sekunder.

[4] https://www.skatteetaten.no/contentassets/343a9f921ade437c81482661e96320de/2022-11-5-3-vurdering-av-tekniske-losninger.pdf

- Påvirkning fra spoofing på de vurderte om bord-løsninger er så teknisk krevende at det ikke er en aktuell problemstilling i et vesentlig omfang per i dag.

Som nevnt, så kan jamming i seg selv føre til ganske store posisjon- og tidsunøyaktigheter, siden signalmottak- og prosesseringen blir påvirket. Den samme observasjonen ble gjort i oppstarten og avslutningen av spoofing. Når dette ble undersøkt litt nærmere, ble det klart at RFI-faseovergangene kunne skape uventede resultater. Forskjellige faser i angrepene kan produsere forskjellige resultater, og resultatene kan forbi lenge etter at RF-miljøet er tilbake til normalen (og noen ganger forble de helt til restart eller fabrikkreset). Disse faseovergangene kan derfor være farlige for GNSS-mottakere, selv om de har gode beskyttelsesmekanismer. Overgangene det er snakk om er mellom fasene 'ingen RFI' og 'RFI', altså

- Overgangen fra ingen RFI til RFI → Initierer RFI
- Overgangen fra RFI til ingen RFI → Avslutter RFI

Det virker som at problemet er at mange av de implementerte beskyttelsesmekanismene er designet for binærforholdet ingen RFI vs RFI, og de fungerte ikke tilstrekkelig i overgangen mellom disse. Det er derfor ikke gitt at for eksempel GNSS-styrte oscillatorer vil kontrollert gå inn i holdover når de oppdager RFI, det kan oppstå ustabiliteter i overgangen til holdover før beskyttelsesmekanismene håndterer RFIen. Det vil si at om kortvarige ustabiliteter eller avvik er uakseptable, så kan dette skape farlige situasjoner. Interessant nok, så betyr denne observasjonen at svakere jammesignaler kan være vel så farlige, om ikke farligere, enn veldig sterke jammesingaler, siden de forlenger denne overgangsperioden hvor holdover-tilstanden ikke er skikkelig initiert.

Derimot så var en relativt gjennomgående observasjon at mye av utstyret som var utstyrt med jamming- og spoofing-beskyttelsesprogramvare, kunne motstå mange av laveffektsjammerne, men høyeffektsjammeren ga veldig varierende resultater, og for tidstjenere var posisjonsspoofing relativt uproblematisk, men tidsspoofing, og spesielt skuddsekund-tilførsel, kunne påvirke i stor grad. Det ble også observert at noen beskyttelsesmekanismer kunne bli påvirket av jamming eller spoofing om dette pågikk over lang nok tid. En mulig forklaring på dette er at algoritmene etter hvert begynte å oppfatte det forstyrrede RF-miljøet som normalen (siden det hadde pågått så lenge), og dermed kunne spoofingen til slutt bli effektiv, selv om den ble oppdaget helt i starten. Tankevekkende, så måtte noen systemer bli restartet etter at dette skjedde med dem, siden de aldri startet å bruke de ekte satellittsignalene igjen.

For multikonstellasjonsmottakere kan man oppsummere ved å si at det gir økt robusthet, men siden det er implementert på forskjellige vis, så er det ikke den automatiske beskyttelsen man kanskje skulle tro det var, selv mot enkel GPS L1-jamming og -spoofing.

4.2 Konkret eksempel på observasjoner

Det som følger er diverse erfaringene fra en av deltagerne, som kjørte i bil med enheter med GNSS-moduler og MEMS-sensorer. Enhetene var fra samme leverandør, men den ene var fra den nyeste generasjonen mens den andre var fra generasjonen tidligere:

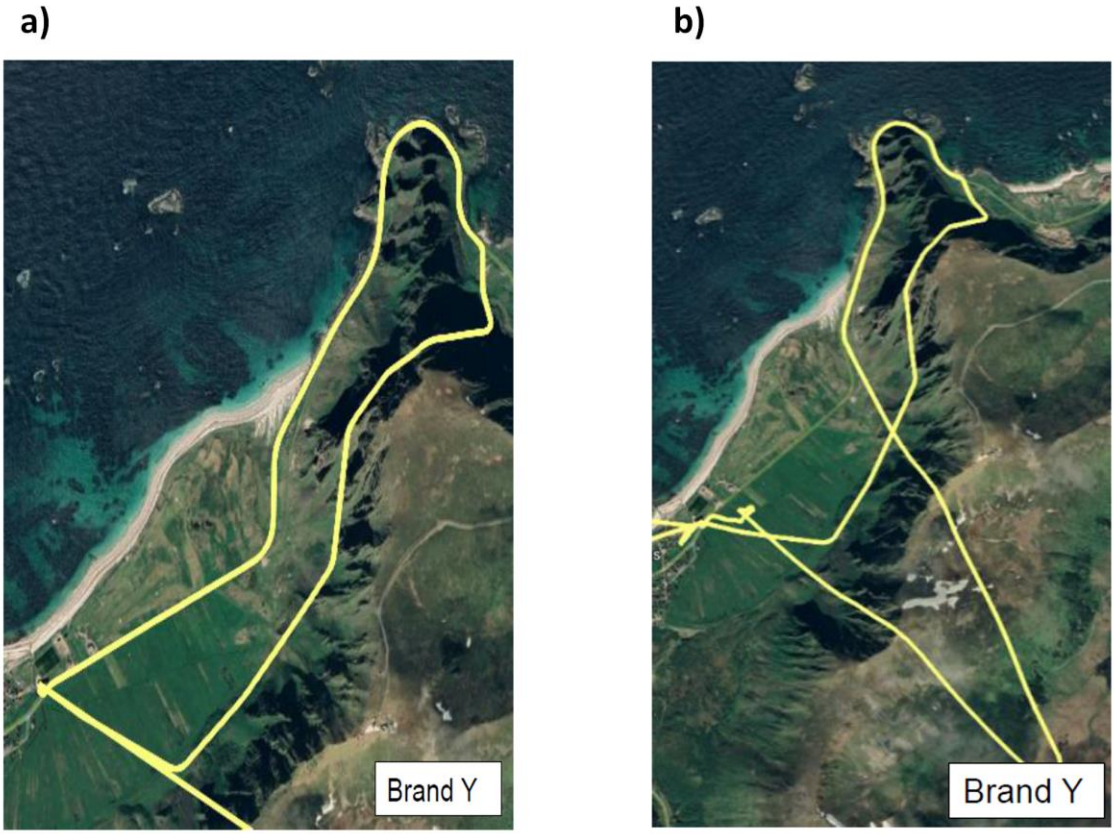
Ved kjøring i kolonne med jammer (L1 only) i en annen bil og test av nyeste enhet, så ble det opplevd degradert ytelse, men ikke noen større problemer (det var et lite drift i bevegelsessporet idet jammeren startet opp, men bevegelsen oppførte seg så rett, bare forskjøvet fra ekte posisjon).

Ved møte med jammer (L1 only) i truck og test av nyeste enhet, så forsvant GNSS-dekning i noen få sekunder, men det ble ikke opplevd noe større PVT-nøyaktighetstap.

Ved kjøring med jammer (L1 only) i egen bil og test av nyeste enhet, forsvant alle GNSS-satellitter, og etter rundt seks minutter var unøyaktigheten på 150-200 m. Ved videre testing med flere jammere i egen bil ble det observert forskjeller på resultatene avhengig av oppstartskriterier, spesielt om de andre sensorene var initialisert eller ei (jammer slo ut mottaker med fix i bil med en gang). I et tilfelle klarte mottakeren å beholde GNSS-fix og PVT, men med degradert signal, og i et annet hvor det ble brukt en annen jammer, så mistet mottakeren GNSS-fix, men beholdt PVT fra andre sensorer. Dvs. at forskjellige jammertyper vil resultere i forskjellig resultat (for eksempel GNSS-fix eller ikke).

Det ble også testet hvordan enhetene reagerte på spoofing. Bilen var da parkert i nærheten av spooferantenne og «målantenne». Når de forskjellige enhetene med GNSS-fix og initialiserte sensorer ble utsatt for inkoherente posisjonsspoofing så forble den nyeste generasjonen upåvirket, mens den eldre generasjonen ble spoofet (interessant nok ble unøyaktigheten i overtakelsesperioden svært stor, før spoofet posisjon ble godtatt (se Figur 2 a))). Hvis bilen kjørte, så fikk den nyeste enheten trygg posisjon, mens den eldre opplevde usikkerhet i starten, som ble veldig stor før posisjonen til slutt begynte å følge spoofet signal (se Figur 2 b)). Usikkerheten i starten kan skyldes at det ble gjort innledende jamming. Ved koherente spoofingangrep og stillestående bil, så opplevde begge enhetene unøyaktighet først og så spoofet posisjon etter hvert, men ved bevegelse opplevde den nyeste enheten lite påvirkning, mens den eldre opplevde forskjellige respons avhengig av om det ble gjort innledende jamming eller ei: ved innledende jamming hektet den seg på spoofet signal, mens ved

ingen innledende jamming ble posisjonsporet en blanding av ekte bevegelse og spor av falskt signal og ekte bevegelse, men ikke på riktige lokasjoner ut ifra hverken spoofet signal eller ekte bevegelse.



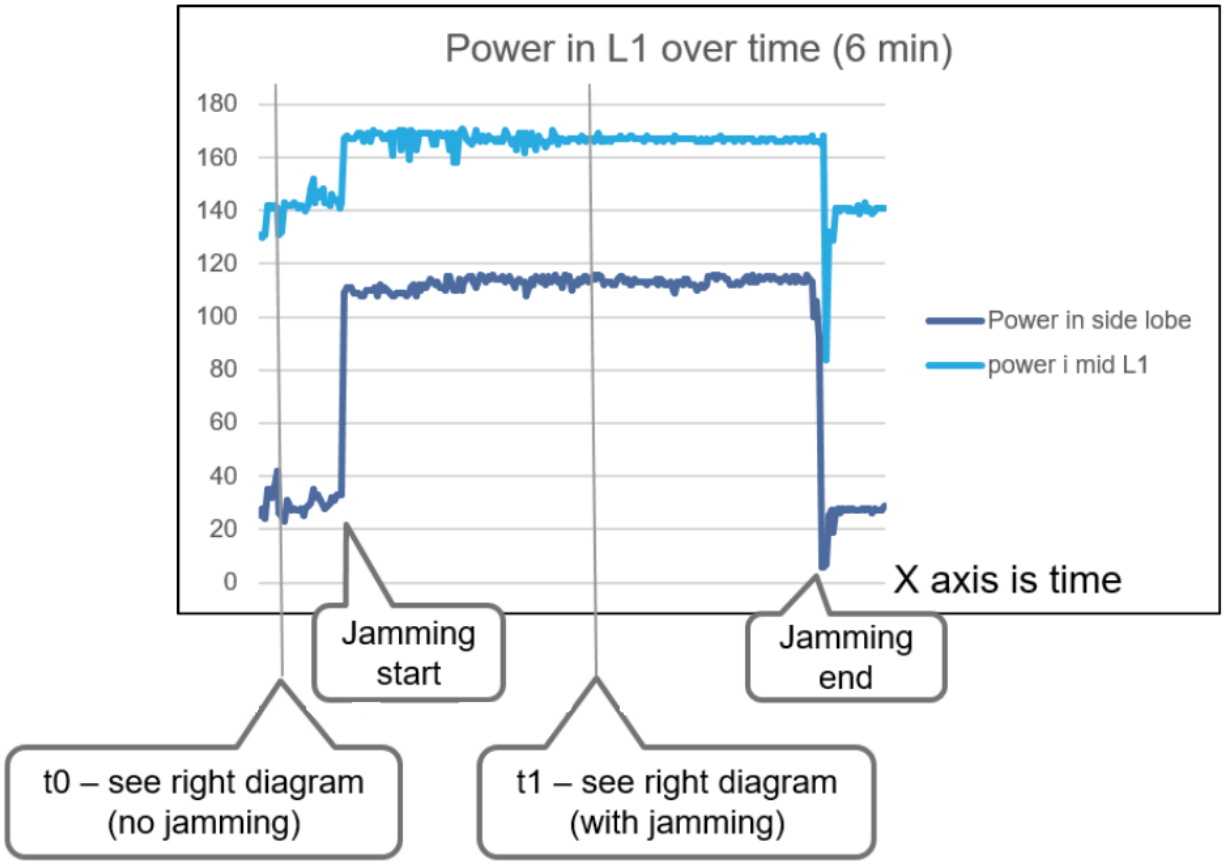
Figur 2: Eldre enhet under spoofingangrep, med alle sensorser initialisert. a) er når bilen er parkert, b) er mens bilen er i bevegelse.

Denne deltageren gjorde også noen vurderinger rundt deteksjon:

Jamming kan ofte enkelt ses i spektrumet, som i Figur 3. Spoofing er vanskeligere, og her er det mye variasjon ut ifra hvilke parametere som tas i bruk i deteksjonsalgoritmen (egne «spoofing detector-parametre» fra chipprodusentene blir ofte utløst i det spoofingen starta, men så skrur de seg av igjen lenge før spoofinga er over), hvor lenge spoofingen holder på (til slutt «lures» også deteksjonsmekanismer til å tro at det spoofa miljøet er det nye normalmiljøet). To mottakere koblet sammen med en fast avstand er også en effektiv måte å oppdage spoofing på.

Andre tanker rundt dette ble fint oppsummert av Harald Hauglin i Justervesenet: «*Basic spoofing signals used satellite data very different from those transmitted by the actual satellites and ought to be flagged as fake by sufficiently alert receivers. Advanced spoofing signals used data/ephemerides identical to those transmitted by the actual satellites and for some synchronized scenarios gave insignificant changes in position and timing at the target location. Even these more advanced spoofing signals may be detectable by fairly basic consistency checks (e.g. two antennas with a known*

displacement should not report the same position), robust multisensor fusion, RF spectrum analysis or by new authentication mechanisms such as Galileo OSNMA»[5].



Figur 3: Spektrumsmåling fra innebygd spektrumsanalysator i nyeste enhet.

En annen observasjon er at AGC kan være en nyttig parameter for å oppdage spoofing, selv om den ikke alltid er like nyttig for å oppdage jamming.

[5] https://www.linkedin.com/posts/harald-hauglin-3140a610_jammertest2022-galileo-osnma-activity-6979791066744934400-kAs0/?originalSubdomain=no

4.3 Konkret eksempel på deteksjonsutstyr

En deltager testet kommersielt tilgjengelige GPS-interferens-deteksjonsutstyr fra Chronos; CTL3510 og CTL3520. Det som følger er en oppsummering av deltageres erfaringer med dette utstyret under testuka.

Enhetene er designet for å oppdage interferens i et 20 MHz frekvensområde, sentrert på 1575 MHz. Begge enhetene reagerte godt på å oppdage både jamming- og spoofing-signalene, og alle de forskjellige modulasjonene (som chirp, CW, PRN).

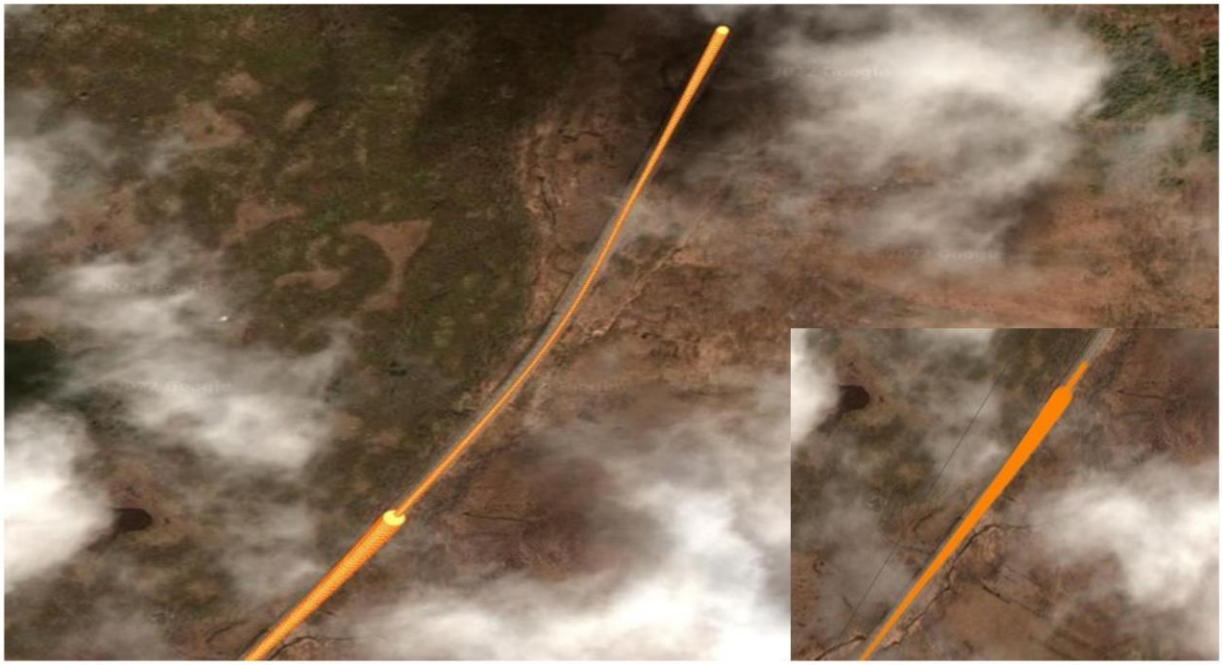
«CTL3510 is a user-friendly handheld, yet compact and versatile detector. Tests shows a practical range of appr. 50 meters if a 10-mW low-cost "eBay jammer" is used inside a car. It will record and time stamp the measured levels to an internal file which can be downloaded through USB. The graph can be used later to document if jamming or spoofing signals were present at a certain time. A LED bar graph for relative signal strength indication is provided, as well as a switchable vibrate/alert function. Use cases may be covert operations and intelligence, or if carried by a public servant on everyday basis. CTL3510 has limited range but the value to the user is instant response if being near to a source.

During the high-power sessions, the CTL3510 triggered and showed approximately a half-scale level reading at the community house, 1100 meters away from the jamming transmitter site.»

«The CTL3520 was valuable to locate and eliminate any jammer, spoofing or noise signal on GNSS frequencies. With or without experience in radio direction finding, the product is quite intuitive in operation.
The received relative signal strength will be indicated through a LED bar graph. When approaching successively to the signal source, the built-in attenuator must be increased on the go to facilitate a max/min reading to properly determine the direction. The current attenuator setting is always visible. By rotating and holding the locator vertically, it is possible to find the elevation in a higher structure or building. In one actual case, we found that the jammer was located inside a truck cabin, elevated only 2m meters above ground level. Knowing the elevation will reduce the time used when locating a source.
Several 'hide-and-seek' of hidden jammer scenarios were carried out, and we were able to locate the hidden jammer in each case. The smaller CTL3510 was engaged in some of the tests, giving the user extra confidence in the locating process. Even during the high-power jamming sessions, we could apply the attenuation needed to determine the direction.
Tests show that the CTL3520 has a quite sensitive receiver. At maximum sensitivity, it is possible to determine the direction and of an incoming signal from a 10 mW "eBay-jammer" at about 1 km. If the source is airborne, significantly larger range apply.»

4.4 Annet

Noen forsvarsindustriaktører kunne ikke dele informasjon om resultatene og erfaringene deres, men som et eksempel på at også disse fikk nyttig informasjon ut av testene så oppgav Teledyn Flir at «The tests we were able to conduct at Andøya directly contributed to a new software that improved GPS denied and spoofing performance for the Black Hornet 3. The Black Hornet 3 with that software is being actively used in Ukraine.»



Figur 4: Eksempel på hvordan feil fra andre sensorer i en mobil plattform bygger seg opp over tid når GNSS-tilgangen faller bort.

Ellers så er datafangsten som ble gjort av flere deltagere svært nyttig for videreutvikling av for eksempel forbedret sensitivitet mot ikke-koeherente spoofingangrep, forbedret falske-positive spoofing-deteksjoner (altså jammesignaler som oppfattes som spoofing), data på ekte jammere og mange forskjellige typer jammesignal, erfaringer med verdien av fallback-løsninger om GNSS faller ut (og hvordan disse hang sammen i forskjellige faser av jamming og spoofing), forskjeller i hvordan sensitive systemer håndterer militære jammesignaler og sivile signaler og bekreftelser på om og at mostandstiltak mot jamming fungerte.

Se ellers resultater i følgende artikler og innlegg i Tabell 2:

Sak	Sted	Dato	Lenke
Interessante resultater: Nkom håper jammetesten på Andøya kan bli årlig	InsideTelecom	26.9.2022	Interessante resultater: Nkom håper jammetesten på Andøya kan bli årlig - Inside Telecom
Nyttige resultater etter jammetest	Nkom	28.9.2022	Nyttige resultater etter jammetest
Alle fikk problemer, så de var veldig fornøyde	vegvesen.no	28.09.2022	Alle fikk problemer, så de var veldig fornøyde

Nyttige resultater etter jammetesten	Security worldmarket	29.9.2022	Nyttige resultater etter jammetesten
World's Largest Jammer Test Held in Norway: Awaiting results	Resilient Navigation and Timing Foundation	28.9.2022	World's Largest Jammer Test Held in Norway: Awaiting results
First Results – World's Largest Jammer (& Spoofing) Test	Resilient Navigation and Timing Foundation	29.9.2022	First Results – World's Largest Jammer (& Spoofing) Test
JammerTest 2022: Unauthorized Jamming, Accidental Spoofing – GPS Patron discusses the event & results	Resilient Navigation and Timing Foundation	11.10.2022	JammerTest 2022: Unauthorized Jamming, Accidental Spoofing – GPS Patron discusses the event & results
JammerTest2022 Norway	GPSPatron	10.10.2022	JammerTest2022 Norway
Testet jamming og spoofing av navigasjonssignaler	Norsk Romsenter	21.10.2022	Testet jamming og spoofing av navigasjonssignaler
GNSS/GPS jamming and spoofing tests under actual conditions	Ublox	08.03.2023	GNSS/GPS jamming and spoofing tests under actual conditions
Norsk øvelse afslører at simpel GPS-jamming slår helikoptere og skibe ud af kurs	Ingeniøren	03.02.2023	Norsk øvelse afslører at simpel GPS-jamming slår helikoptere og skibe ud af kurs
Impact analysis of spoofing on different-grade GNSS receivers	IEEE	08.06.2023	Impact analysis of spoofing on different-grade GNSS receivers
Mitigating Jamming and Spoofing with Grit	Hexagon	2023	Mitigating Jamming and Spoofing with Grit (page 50 and onwards)

Tabell 2: Nyhetssaker med lenker som sier noe om resultatene fra Jammetest 2022.

4.5 Tilgang på måledatasett

4.5.1 Nkom

Nasjonal kommunikasjonsmyndighet (Nkom) har spektrumsålinger (effekt mot tid) av de fleste høyeffektsjammesignalene, en del av laveffektssignalene og noe av spoofingsignalene. For tilgang til disse målefilene, ta kontakt med Nicolai Gerrard i Nkom, nge@nkom.no.

4.5.2 Sintef

Sintef monitorerte og tok opptak av de aller fleste signalene som ble sendt rundt Samfunnshuset. For å få tilgang til datasettet deres, ta kontakt med Senior Research Scientist Aiden Morrison, aiden.morrison@sintef.no.

4.5.3 GPSPatron

GPSPatron monitorerte spektrumet fra flere forskjellige prober, hvor alle måledataene er samlet i skya. Datasettet er tilgjengelig for alle, https://jammertest2022.gp-cloud.io/, og man ber om tilgang gjennom denne linken: https://forms.gle/Wgjdu7WE4kASLamJ6.

5 Konklusjon

Testene tilbydde en (sivil, ubegrenset og åpen) arena for større felttester med GNSS-jamming og -spoofing, som man finner få andre steder i verden (og da alltid i militær regi). Undersøkelsene og arrangementet tilbydde muligheten til å øke kunnskapene om GNSS-interferenspåvirkninger på systemer og teknologistacker, å oppdage nye utfordringer som ikke tidligere var påtenkt eller analysert, og å kunne gjøre unike målinger og datafangst på GNSS-jamming og -spoofing, alt i ekte omgivelser i den virkelige verden.

Basert på tilbakemeldingene fra deltagerne i løpet av testuka, så ble alle disse mulighetene oppfylt, og det var et sterkt ønske hos så å si alle som deltok om å kunne gjennomføre slike tester på nytt, for eksempel med det formål å teste de tiltak som i mellomtiden var blitt implementert på bakgrunn av erfaringene de gjorde seg denne uka.

Slike tester er også med på å la offentlige myndigheter ta mer aktive grep mot samfunnsfarene fra GNSS-jamming og -spoofing enn bare monitorering og varsling om hendelser; det bidrar til å utvikle løsninger som kan tåle å bli utsatt for slike ondsinnede angrep, og dermed er det med på å sette industri og bransje i stand til å håndtere og løse flere saker/hendelser uten at de trenger bistand fra offentlige myndigheter som Nkom.

I tillegg til egennytten som arrangørene selv fikk ut av testene, så var dette arrangementet en unik læringsmulighet for deltagerne, som fikk innsikt og innføring i mange forskjellige systemer (med den fellesnevneren at de bruker GNSS til et eller annet i systemet), og det viste seg å bli en god networking-arena for ingeniører og deltagende fagpersoner med felles interesser og felles systemutfordringer/-risikoer.

Arrangørene er av den oppfatning av at kostnaden som arrangementet hadde er rettferdiggjort i forhold til den nytten det vil få for både deres egne organisasjoner, Norge som land og for framtidig utstyr og systemer basert på GNSS.

På to tidspunkt ble det gjennomført en liten undersøkelse om deltagerne ville ønske å delta på Jammetest 2023. Ved det ene tilfelle, torsdagens oppsummering, var det samstemt bifall til dette, og ved det andre tilfellet, evalueringsskjemaet, svarte alle unntatt en (som svarte kanskje), ja på spørsmålet om de ønsket å delta på en potensiell Jammertest 2023.

Det er derfor arrangørenes anbefaling at dette arrangementet gjentas til neste år, og at det bør gjøres til en jevnlig hendelse, ettersom det ganske åpenbart fyller en mangel som industri, akademia, myndigheter og andre viktige GNSS-brukere har.

5.1 Oppsummering av observasjoner

Satellittnavigasjonssystemene om bord i et fartøy oppfører seg veldig forskjellig fra for eksempel høypresisjonsutstyr eller svært nøyaktige tidstjenere. Siden både feilmarginen og konsekvensene er forskjellige for forskjellige systemer, alle med forskjellig implementasjon av GNSS i teknologistacken sin, er det vanskelig å si noe generelt om systemrespons. Men, på et overfladisk nivå kan man si noen observasjoner bør merkes:

- Multi-GNSS-systemer kan være avhengig av en referansekonstellasjon, sånn at angrep mot denne konstellasjonen alene kan forringe, og i noen tilfeller forhindre, PVT-løsninga, selv om andre, upåvirkede konstellasjoner er tilgjengelige.
- Jamming kan skape spoofing-aktige symptomer, noe som illustrerer noen mottakeres høye feiltoleranse (dette er altså et problem som skyldes avhendingen mellom feiltoleranse og satellittfix).
- Forskjellige faser i angrepene kan skape forskjellige resultater, og disse resultatene kan forbli lenge etter at RF-miljøet har returnert til normalen (og i noen tilfeller, forbli helt til systemet ble restartet). Disse faseovergangene kan være farlige for GNSS-mottakere, selv med beskyttelsesmekanismer (som ofte er laget for jamming/ingen jamming-tilfeller). Overgangene det er snakk om er:
    - Overgangen fra ingen RFI til RFI → Initierer RFI
    - Overgangen fra RFI til ingen RFI → Avslutter RFI
- Inkoherent spoofing kan fungere når offersystemene ikke har noen, eller har dårlige, sikkerhetsbarrierer, men krever ofte en angrepskombinasjon med jamming.
- Koherent spoofing fungerer veldig ofte veldig godt, og trengte mange ganger ikke jamming for å være suksessfull. Noen multi-GNSS-systemer ble helt spoofet selv med spoofing av bare en konstellasjon, kanskje fordi dette var deres referansekonstellasjon, selv om andre GNSS og frekvenser var tilgjengelige.
- Selv det som først så ut som vellykkede beskyttelsesmekanismer kunne bli spoofet om spooferen var aktivert lenge nok, hvorpå det spoofede RF-miljøet ble oppfattet som det nye «ekte» miljøet, og når det faktiske ekte RF-miljøet gjenoppstod, ble dette muligens tolket som et nytt angrep).

Tillegg 1 – Angrepsmetodikker

Jamming ble foretatt med et assortiment av laveffektsjammere, samt en høyeffektsjammer. Laveffektsjammerne dekket i hovedsak GPS L1, GPS L1+L2, GPS L1+L2+L5+E6, alt med rundtstrålende antenner og varierende utgangseffekt. Høyeffektsjammeren var en signalgenerator som kunne brukes til å jamme på alle GNSS-bånd, med en direksjonell antenne (høyrehåndssirkulærtpolarisert) og maks utgangseffekt på 20 W. Denne jammerer brukte CW-modulasjon og PRN-modulasjon (P-kode, BPSK-modulert med udefinert satellittnummer), hvor frekvensdetaljene er å finne i Tabell A1. Alle disse jammesignalmulighetene ble så brukt i de kombinasjoner som er beskrevet i kapittel 3.

Jammesignal	Senterfrekvens (MHz)	BPSK-modulasjons-rate (MHz)
L1	1575,42	10,23
L2	1227,6	10,23
L5	1176,45	10,23
G1	1602	5,11
G2	1246	5,11
E5b	1207,14	10,23
B1I	1561,1	2

Tabell A1: Frekvensdetaljer for PRN-BPSK-modulerte jammesignaler.

Forklaring til spoofingen (fra Harald Hauglin, Justervesenet):
«Hovedforskjellen på formiddag ('basic spoofing') og ettermiddag ('advanced spoofing') er satellittdata som ble brukt.

Basic spoofing [inkoherent] brukte andre satellittdata (dvs. informasjon om hvor satellittene er og hva klokken i satellittene er) enn det man mottok fra de faktiske satellittene. Dvs. at de simulerte satellittene sendte ut andre data om seg selv enn de faktiske satellittene på det tidspunktet vi gjennomførte spoofingen. Dette vil da innføre et «hopp» i mottakerens PVT-løsning når den begynner å locke på spoofing-signalene i stedet for de ekte satellittsignalene.

Avansert spoofing [koherent] simulerte satellitter som sendte de samme data om seg selv som de faktiske satellittene. For en del av scenariene var i tillegg tidspunkt for utsendelse synkronisert med GPS systemtid og forsinkelser i vår simuleringskjede korrigert ned til noen titalls nanosekunder. For mottakere med antenne nær vår 'offerantenne' ville det simulerte signalet og det sanne signalet inneholde identisk informasjon og bli mottatt samtidig innenfor titalls nanosekunder. Det vil si at «hoppet» beskrevet tidligere vil være så å si borte, og eventuelle spoofing-oppdagelsesalgortimer innebygd i mottakerne vil ha mye større vansker med å stanse et slikt angrep.

Vi simulerte bare GPS L1 C/A og Galileo E1.»