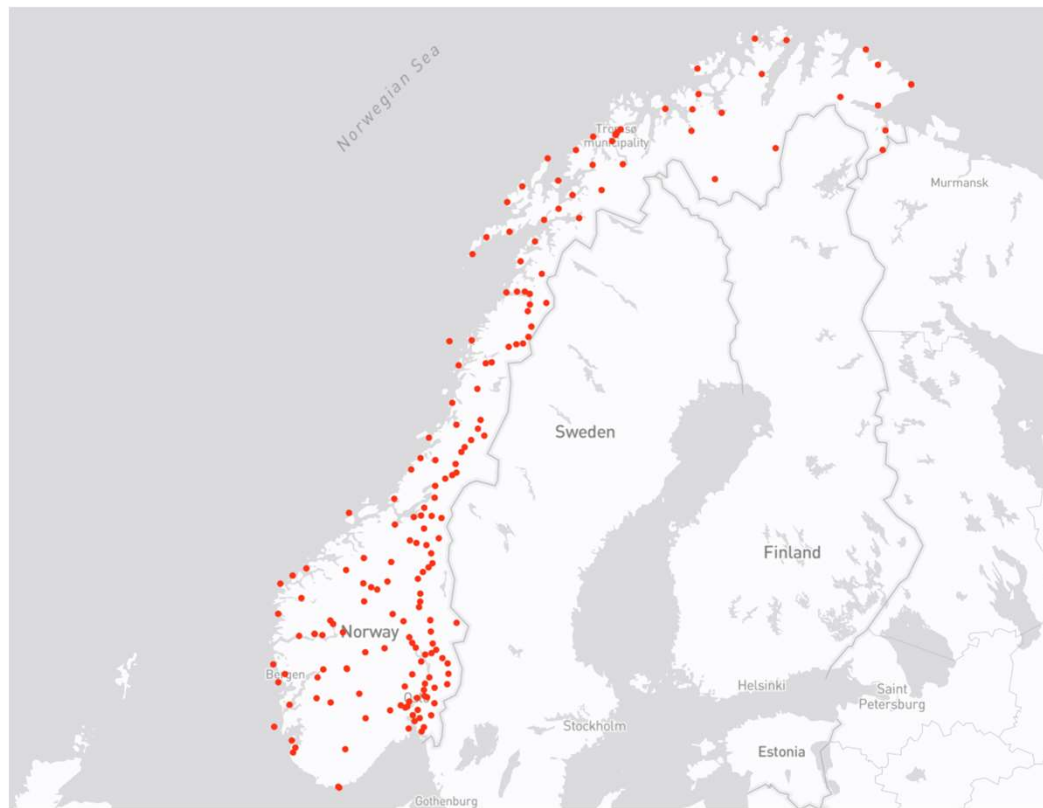


Jammertest 2024

Testing av Leica GR50 mottaker





Motivasjoner

- Hvor robust er GR50 mot ulike angrep?
- Hvordan er påvirkningen fra småjammere og utilsiktet radiostøy?
-
-
- Hvor godt fungerer interferens-loggingen?
- Fungerer mottiltakene - altså filtrene man kan definere på mottakeren?
- Datagrunnlag for å bedre kunne analysere interferenshendelser i nettverket.
- Erfaringer med tanke på bruk av CNR som en interferens-indikator



Resultater

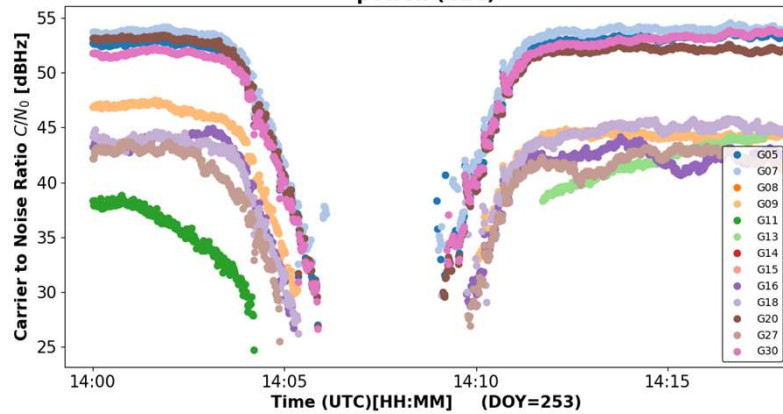
- Datarapport
- Visualisere observasjonsdata
- Begrenset til GPS
 - L1 C/A kode (C1C)
 - L2C(M) kode (C2S)
- Carrier-to-noise (CNR)
- Code pseudorange
- Mulig å logge posisjon, men observasjonsdata viktigere for nettverk-RTK løsning

9 Unintentional RFI	8
9.1 Test 1.18.4 - Continuous wave jamming, 1545-1620 MHz, 1 minute sweep	8
9.2 Test 1.18.5 - Continuous wave jamming, 1545-1620 MHz, 15 minute sweep	10
9.3 Test 1.18.7 - Continuous wave jamming, 1620-1545 MHz, 15 minute sweep	13
9.4 Test 1.18.8 - Continuous wave jamming, higher bandwidth, 1545-1620 MHz, 1 minute sweep	15
9.5 Test 1.18.13 - Continuous wave jamming, 1150-1300 MHz, 15 minute sweep	17
9.6 Test 1.18.15 - Continuous wave jamming, 1300-1150 MHz, 15 minute sweep	19
9.7 Test 1.18.16 - Continuous wave jamming, higher bandwidth, 1150-1300 MHz, 1 minute sweep	21
10 Realistic jamming	23
10.1 Test 1.1.1 - Cigarette jammer S1.1 (L1)	23
10.2 Test 1.1.2 - Cigarette jammer S1.2 (L1)	26
10.3 Test 1.1.4 - Cigarette jammer S2.1 (L1,L2)	28
10.4 Test 1.1.5 - Cigarette jammer S2.2 (L1,L2)	31
10.5 Test 1.1.8 - USB jammer U1.1 (L1)	34
10.6 Test 1.19.1 - Cigarette jammers S1.x (L1) (3 jammers 50m from center)	36
10.7 Test 1.19.2 - Cigarette jammers S1.x (L1) (3 jammers 100m from center)	37
10.8 Test 1.19.3 - Cigarette jammers S1.x (L1) (3 jammers 150m from center)	39
10.9 Test 1.19.4 - Cigarette jammers S2.x (L1,L2) (3 jammers 50m from center)	41
10.10 Test 1.19.5 - Cigarette jammers S2.x (L1,L2) (3 jammers 100m from center)	44
10.11 Test 1.19.6 - Cigarette jammers S2.x (L1,L2) (3 jammers 150m from center)	46
10.12 Test 1.19.7 - USB jammers U1.x (L1) (3 jammers 50m from center)	49
10.13 Test 1.19.8 - USB jammers U1.x (L1) (3 jammers 100m from center)	50
10.14 Test 1.19.9 - USB jammers U1.x (L1) (3 jammers 150m from center)	52
10.15 Test 1.19.10 - Handheld jammers H6.4 (L1,L2,L5) (3 jammers 50m from center)	53
10.16 Test 1.19.11 - Handheld jammers H6.4 (L1,L2,L5) (3 jammers 100m from center)	55
10.17 Test 1.19.12 - Handheld jammers H6.4 (L1,L2,L5) (3 jammers 150m from center)	55
10.18 Test 1.19.13 - Handheld jammer H1.1, low power (L1,L2) (3 jammers 50m from center)	57
10.19 Test 1.20.10 - Handheld jammers H1.1, high power (L1,L2) (3 jammers 50m from center)	59
10.20 Test 1.20.11 - Handheld jammers H1.1, high power (L1,L2) (3 jammers 100m from center)	61
10.21 Test 1.20.12 - Handheld jammers H1.1, high power (L1,L2) (3 jammers 150m from center)	63
11 Jamming	65
11.1 Jamming: Summary	65
11.2 Test 1.2.1 - Continuous wave jamming on L1	65
11.3 Test 1.2.4 - Continuous wave jamming on L1,G1,L2,L5	68
11.4 Test 1.3.5 - Sweep jamming on L1	70
11.5 Test 1.3.8 - Sweep jamming on L1,G1,L2,L5	71
11.6 Test 1.4.1 - PRN-code jamming on L1	73
11.7 Test 1.4.4 - PRN-code jamming on L1,G1,L2,L5	75
11.8 Test 1.6.1 - PRN-code jamming on L1, with ramping power	76
11.9 Test 1.6.4 - PRN-code jamming on L1,G1,L2,L5, with ramping power	78
11.10 Test 1.8.1 - PRN-code jamming pyramid	80

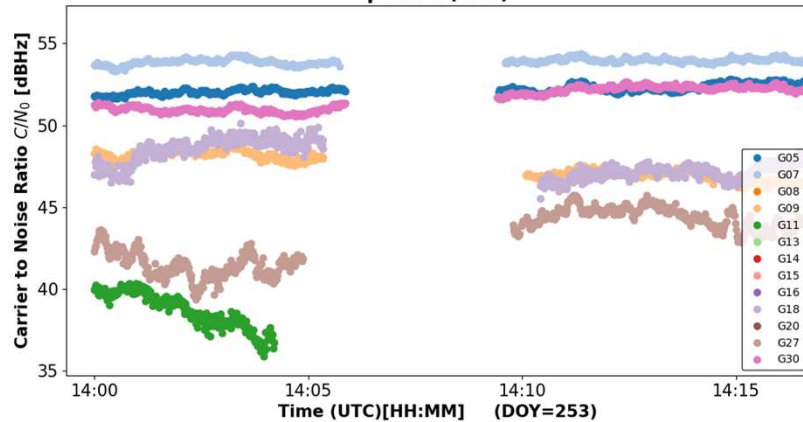
L2 avhenger av L1

- Svakheter ved mottager, eller uten betydning?

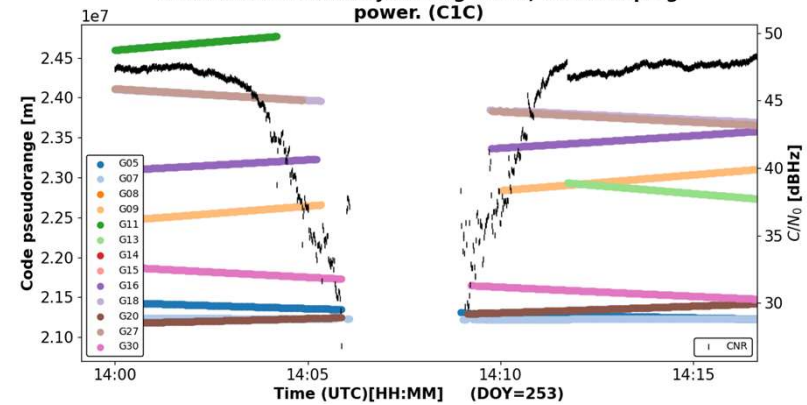
Test 1.6.1: PRN-code jamming on L1, with ramping power. (C1C)



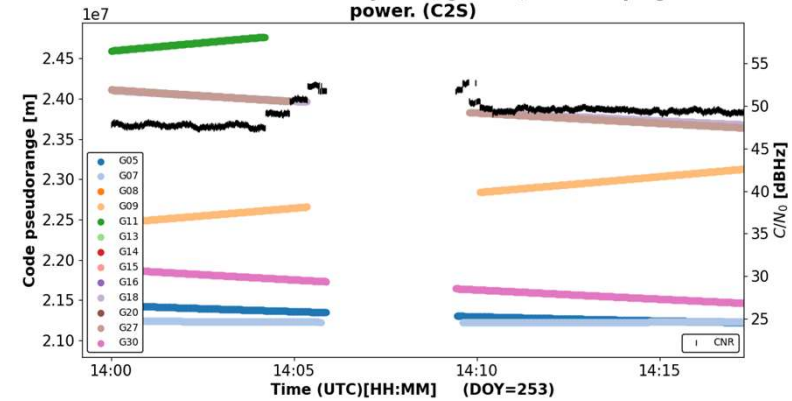
Test 1.6.1: PRN-code jamming on L1, with ramping power. (C2S)



Test 1.6.1: PRN-code jamming on L1, with ramping power. (C1C)



Test 1.6.1: PRN-code jamming on L1, with ramping power. (C2S)

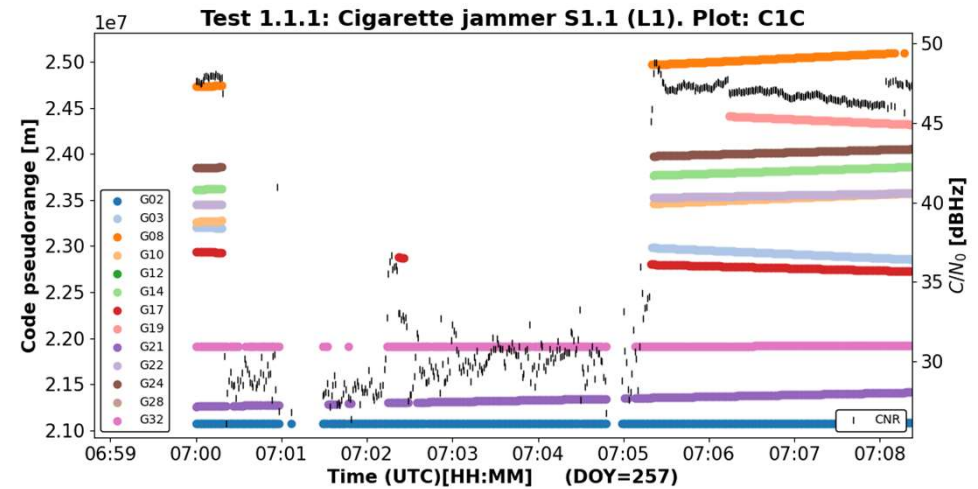
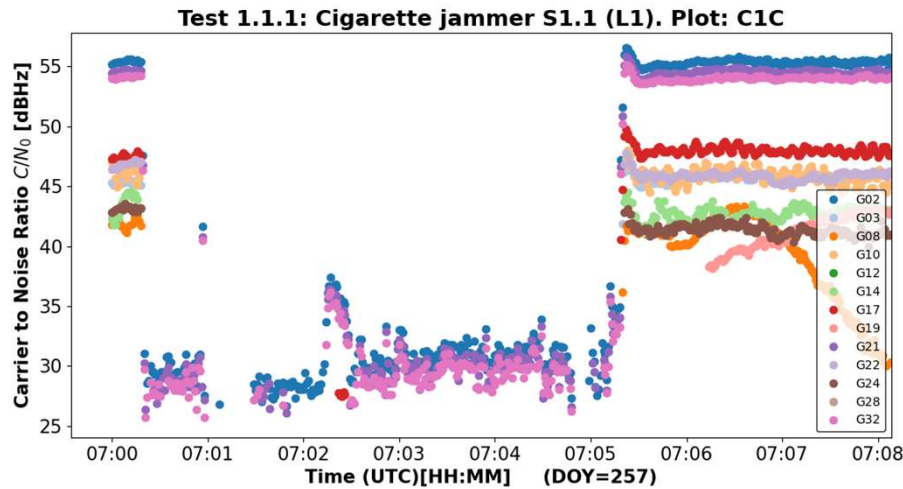


Jamming

- Realistisk jamming
 - = lav-effekt jamming med kommersielt tilgjengelig jammere
 - En sigaretttenner-jammer vil kunne være middels til veldig forstyrrende
- Høy-effekt jamming: Veldig forstyrrende
- Utilsiktet RFI: Høyeffekt - dermed veldig forstyrrende
 - Pseudoavstand-sporing av C1C stoppet når sentral frekvensen var 1575+-15 MHz

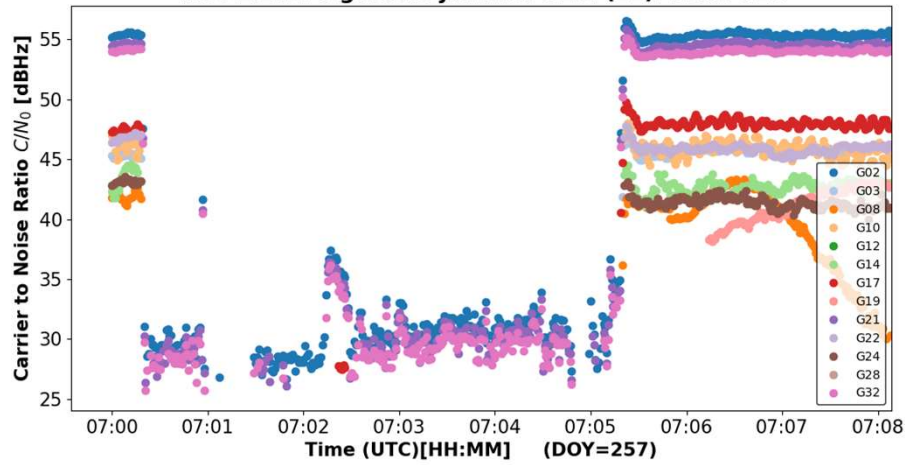
Realistisk jamming

No.	Test details	Test results
	Realistic jamming	
1.1.1-1.1.2	Sigarette jammer (S1.1), in close proximity(~100m)	Large (~25 dBHz) drop in CNR. Only pseudorange tracking of the highest CNR signals.
1.1.4-1.1.5	Sigarette jammer (S2.1), in close proximity(~100m)	Drop (~10 dBHz) in CNR. Pseudorange tracking for most of the satellites. - Sigarette jammers are not all the same.
1.1.8	USB jammer (U1.1), in close proximity(~100m)	Drop (~10 dBHz) in CNR. Pseudorange tracking for most of the satellites.
1.19.1-1.19.2	Three sigarette jammers (S1.1), two of them in close proximity(~100m),	Drop (~15 dBHz) in CNR. Pseudorange tracking for most of the satellites.
1.19.4-1.19.6	Three sigarette jammers (S2.1), two of them in close proximity(~100m-150m)	Same behavior as for the single jammer test, with 10dBHz drop in C1C CNR and tracking of most of the satellites.
1.19.10-1.19.11	Handheld jammers (H6.4), in close proximity(~100m)	Loss of tracking (for both C1C and C2S).
1.19.12	Handheld jammers (H6.4), in close proximity(~150m)	Large (~25 dBHz) drop in CNR. Only pseudorange tracking of the highest CNR signals.
1.19.13-1.19.15	Handheld jammers (H1.1), in close proximity(~100m), low power (-10dBm=0.1mW).	Small (1dBHz) drop in CNR. Normal code pseudorange tracking.
1.20.10-1.20.12	Handheld jammers (H1.1), in close proximity(~100m), high power (20dBm=0.10W).	Large (25 dBHz) drop in CNR. Only pseudorange tracking of the highest CNR signals.

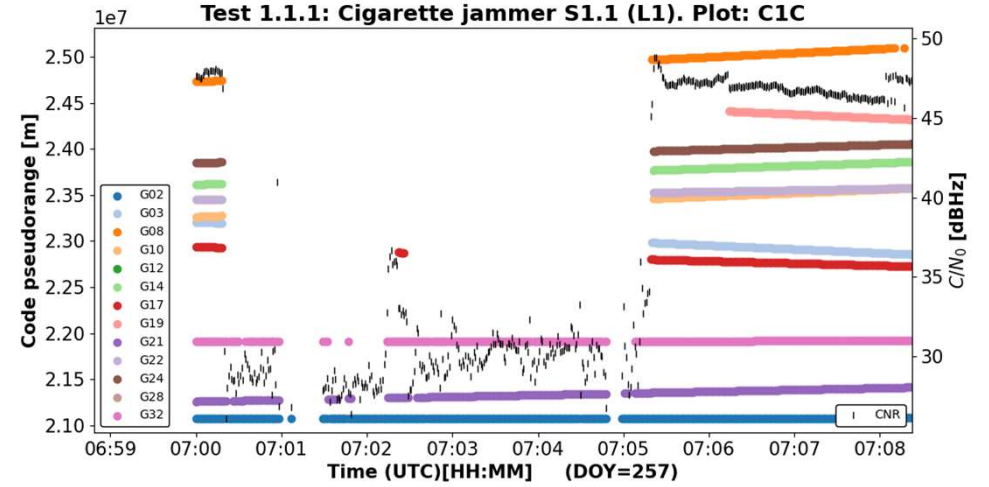


- Stort dropp i CNR
- IGS definisjoner
 - 30-35dBHz – grense for "god" sporing
- Generelt for GR50: faller CNR under 25dBHz, stopper sporing
- Tre satellitter spores fortsatt

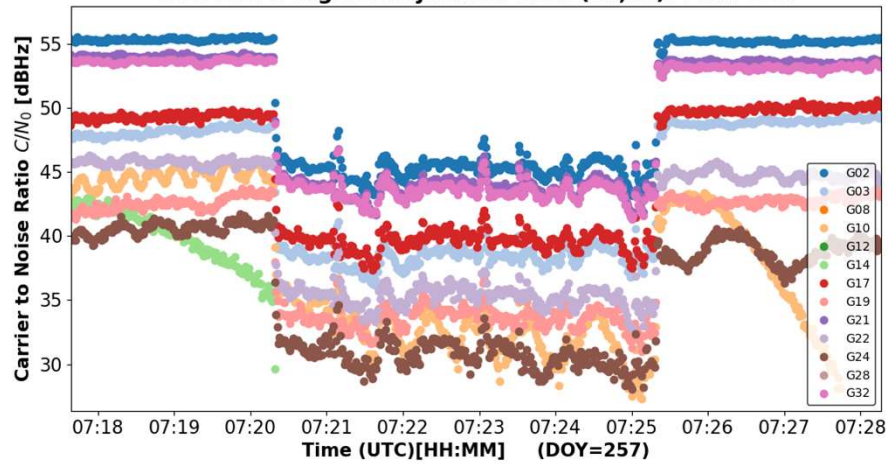
Test 1.1.1: Cigarette jammer S1.1 (L1). Plot: C1C



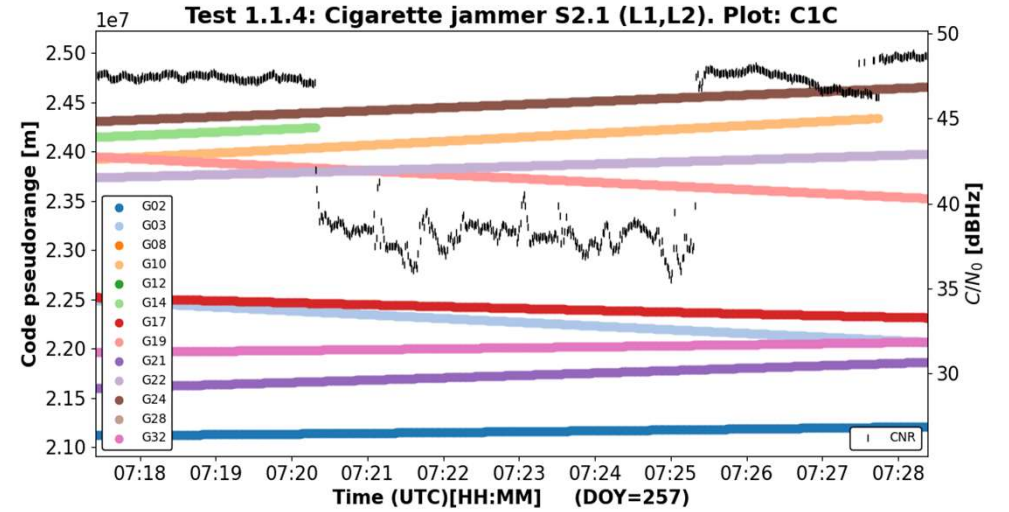
Test 1.1.1: Cigarette jammer S1.1 (L1). Plot: C1C



Test 1.1.4: Cigarette jammer S2.1 (L1,L2). Plot: C1C



Test 1.1.4: Cigarette jammer S2.1 (L1,L2). Plot: C1C

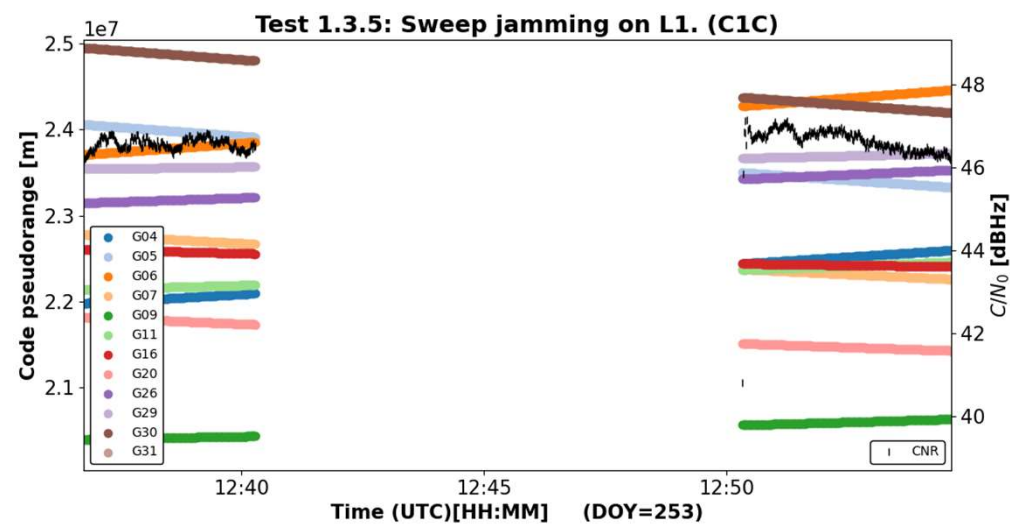
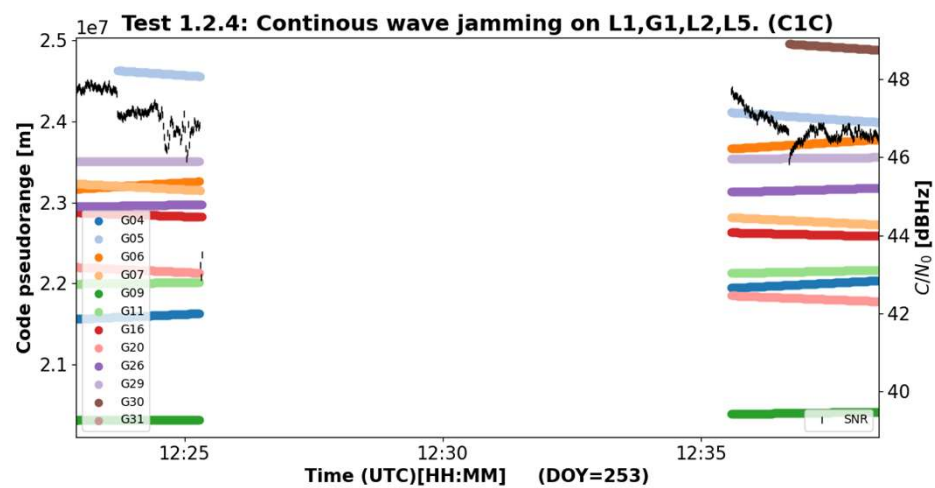


Høy-effekt jamming

- Effekten er høy (50 W): Sporing av pseudoavstand stopper

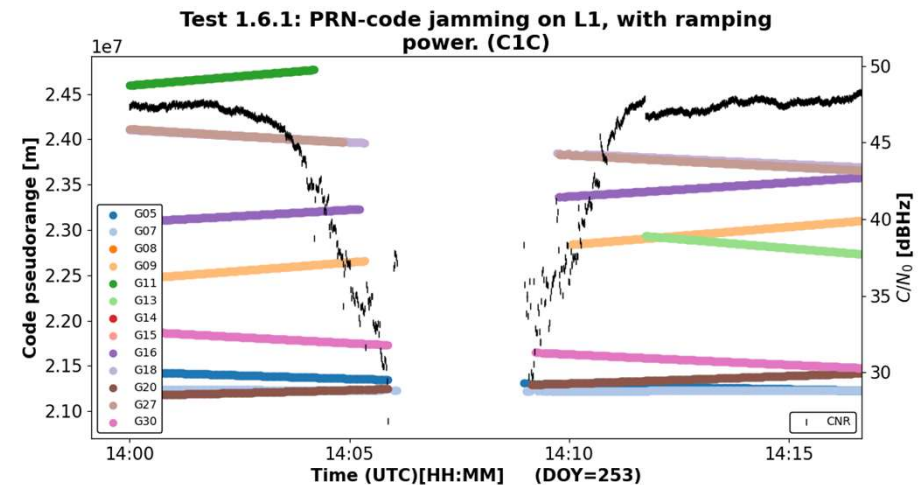
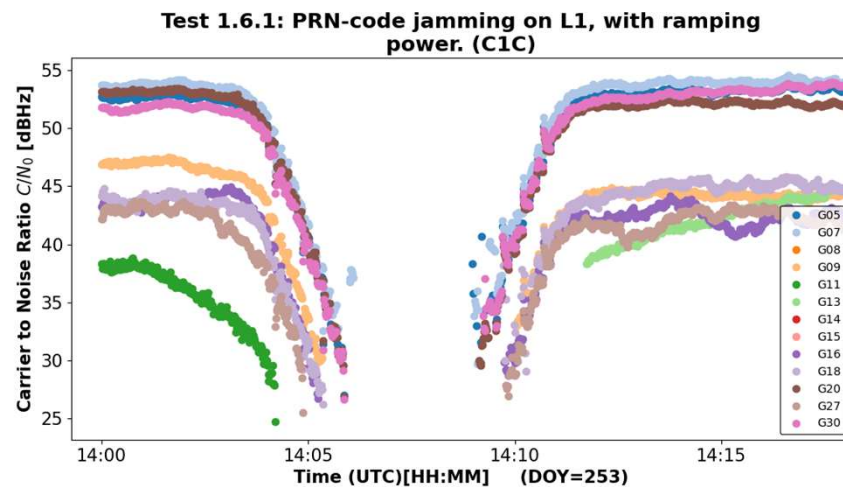
	High power jamming	Similar behavior for the different kinds of jamming. Power is so high that there is no tracking.
1.2.1	CW jamming, on L1, at a distance (~1.5km), high power (50W).	Loss of tracking (for both C1C and C2S).
1.2.4	CW jamming, on L1 and L2, at a distance (~1.5km), high power (50W).	Loss of tracking (for both C1C and C2S).
1.3.5	Sweep jamming, on L1, at a distance (~1.5km), high power (50W).	Loss of tracking (for both C1C and C2S).
1.4.1	PRN-code jamming, on L1, at a distance (~1.5km), high power (50W).	Loss of tracking (for both C1C and C2S).
1.4.4	PRN-code jamming, on L1 and L2, at a distance (~1.5km), high power (50W).	Loss of tracking (for both C1C and C2S).
1.6.1	PRN-code jamming, on L1, at a distance (~1.5km), power ramp.	CNR remains stable until around 10dBm (10mW), and drops below the 25dBHz threshold when jamming power is at 20-30dBm (0.1W-1W).
1.6.4	PRN-code jamming, on L1 and L2, at a distance (~1.5km), power ramp.	Similar behavior. (C2S is now also displaying the ramp behavior.)
1.8.1	PRN-code jamming, pyramid, at a distance (~1.5km), high power (50W).	Loss of tracking for C1C when jamming on B11 starts.

Høy-effekt jamming



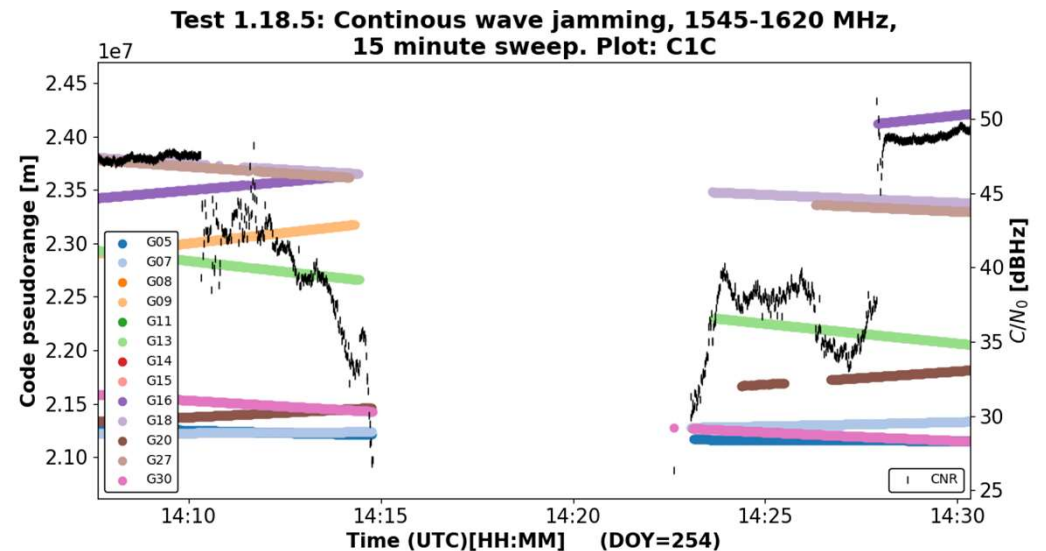
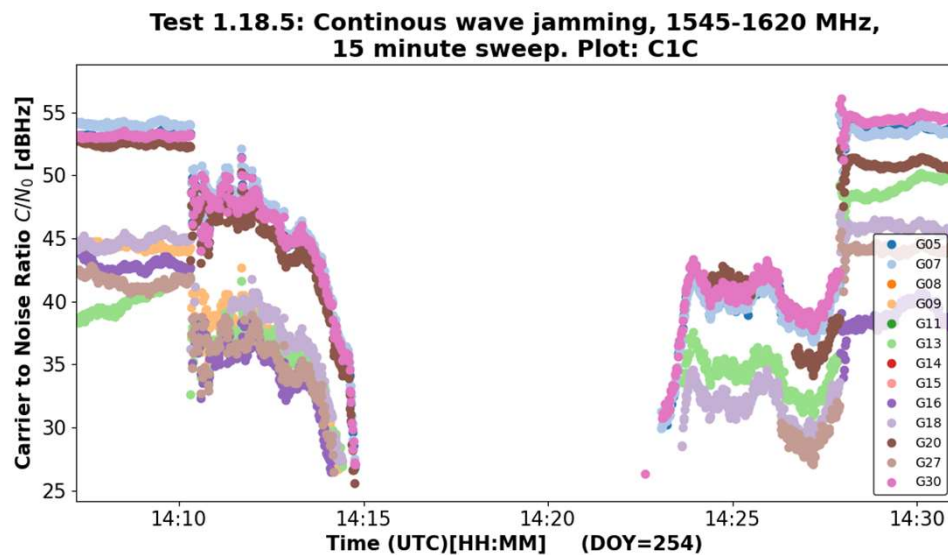
Høy-effekt jamming

- 10mW - CNR begynner å synke
- 0.1W-1W - CNR dropper under 25 dBHz og sporing stopper



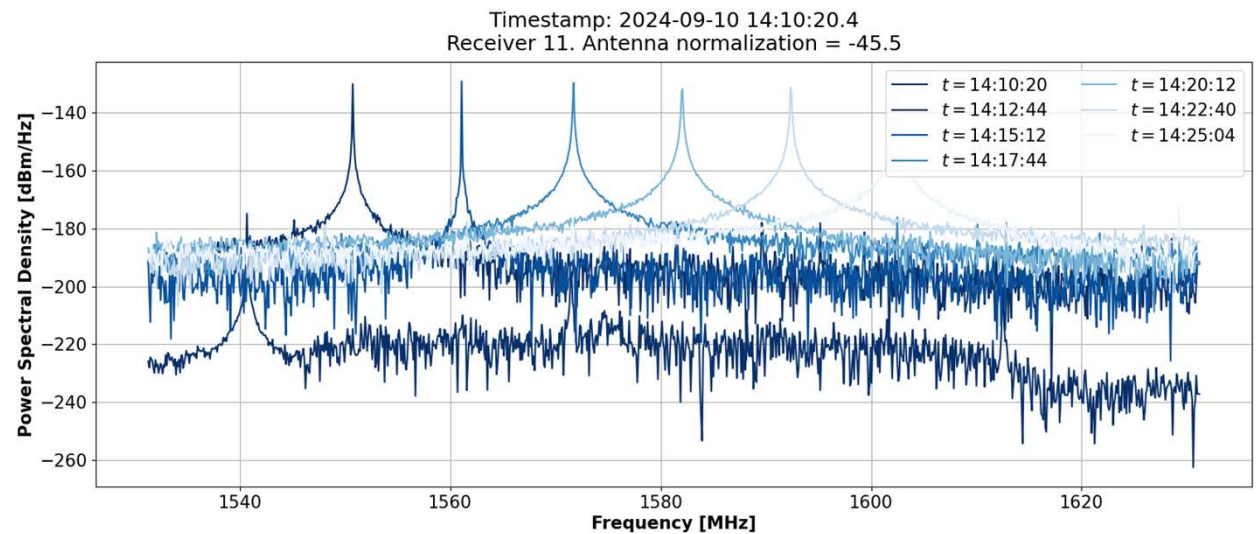
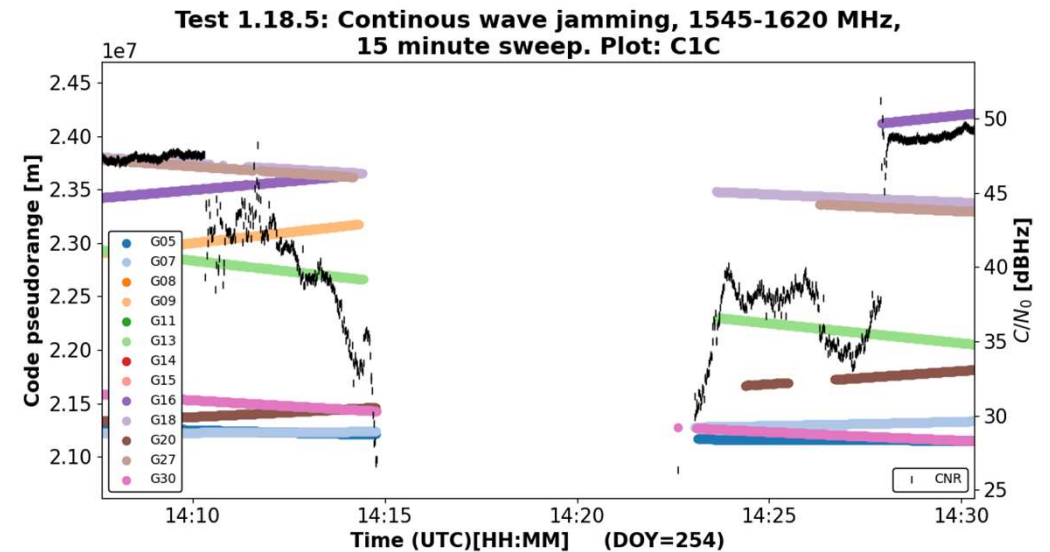
Utsikt RFI

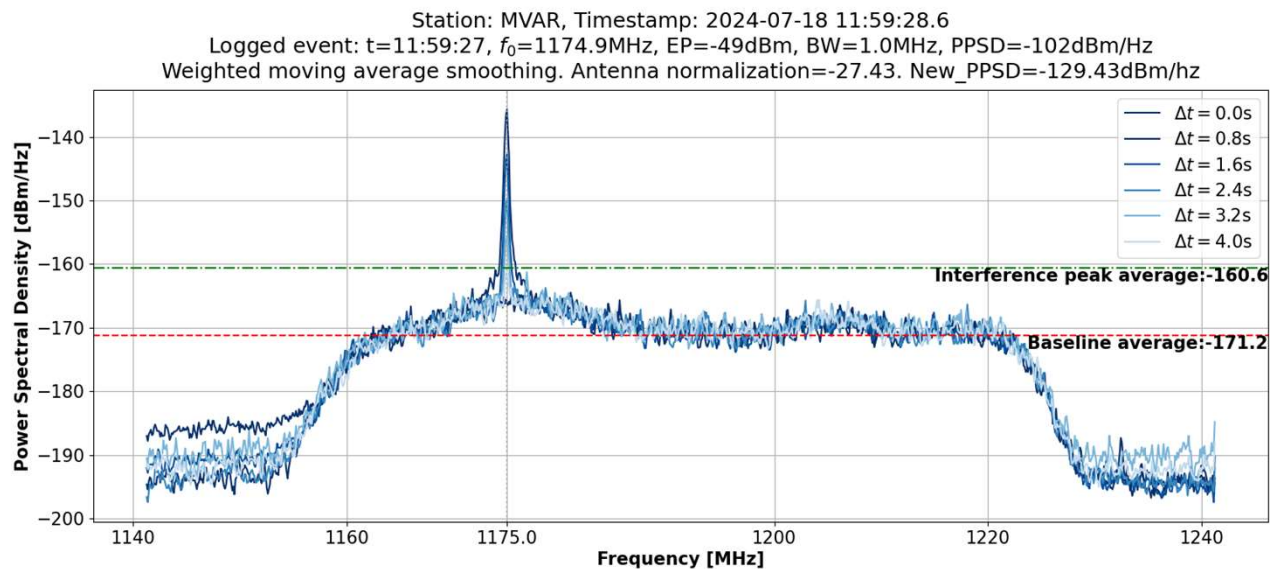
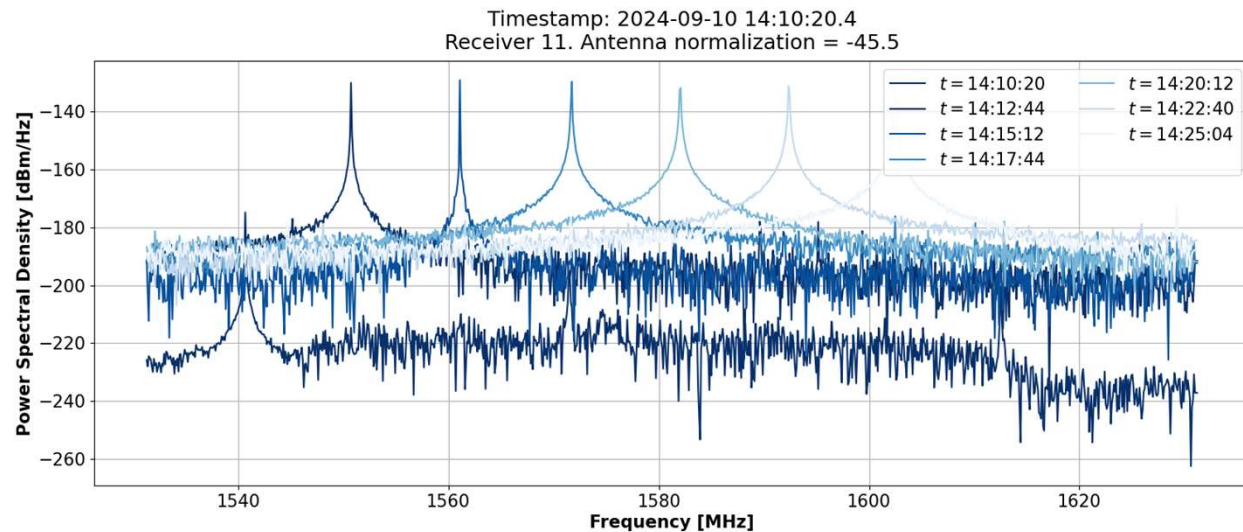
- Høy effekt – 50W
- Urealistisk høy effekt?



Utilsiktet RFI

- 14:15 – Central freq. = 1560 MHz
- 14:22 – Central freq. = 1590 MHz





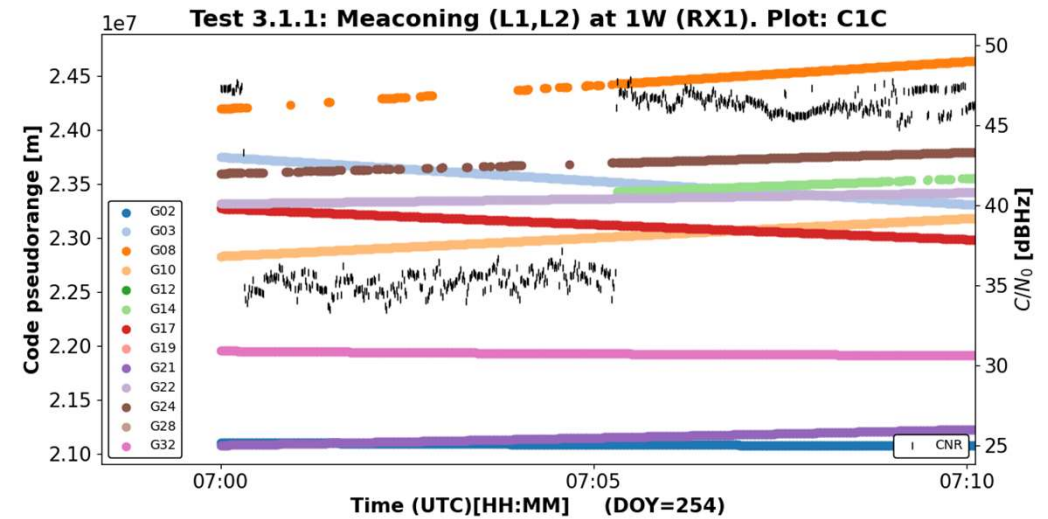
- Maks effekt-tetthet -130 dBm/Hz for begge
- Ulik normalisering
 - Antenne 29dB
 - Aktiv splitter 19dB
- Typiske verdier
 - Termisk støy -174 dBm/Hz
 - C1C
 - -130 dBm across 2MHz bandwidth
 - -193 dBm/Hz
- For test 1.2.4 ble dette logget
 - 12:30:01
 - Freq: 1602.04 [MHz],
 - Bandwidth: 0.81 [MHz],
 - Est. Power: -32.97 [dBm]
 - Highest est. power spec. density: -81.80 [dBmHz]

Meaconing

- Klarer meaconing å forvirre mottakeren?
- Meaconing = videresending av GNSS-signal, forsterket
- Meaconing-respons likner mye på jamme-respons
- Å jamme først gjør meaconing mer effektivt
- Med initiell jamming og høy nok effekt vil falsk pseudoavstand rapporteres
 - Mottaker skjønner at noe er galt – gir ikke posisjonsløsning.
- Mottaker tilbake til normalen når meaconing slutter

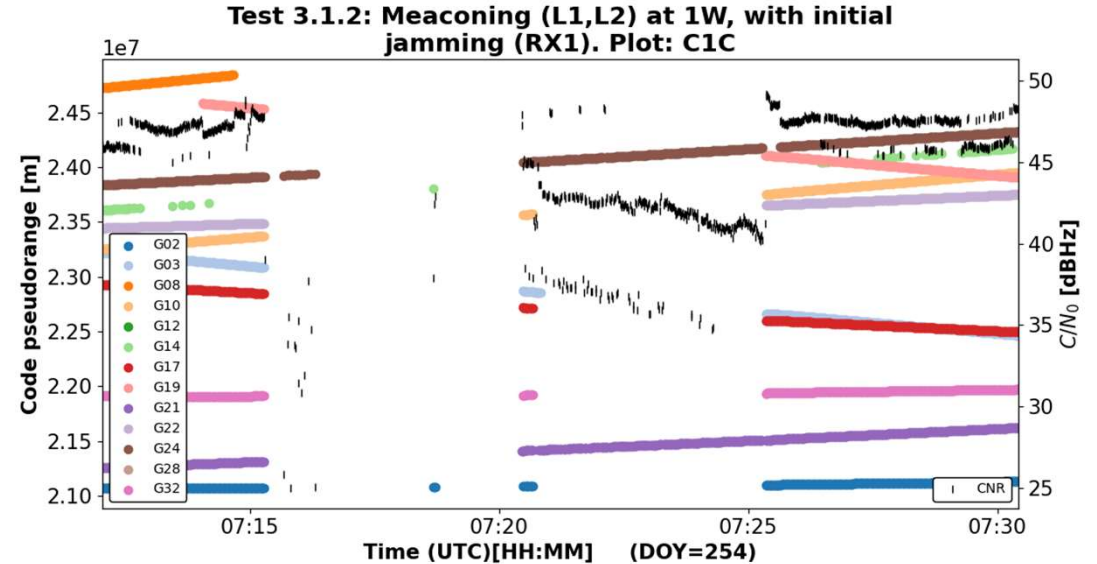
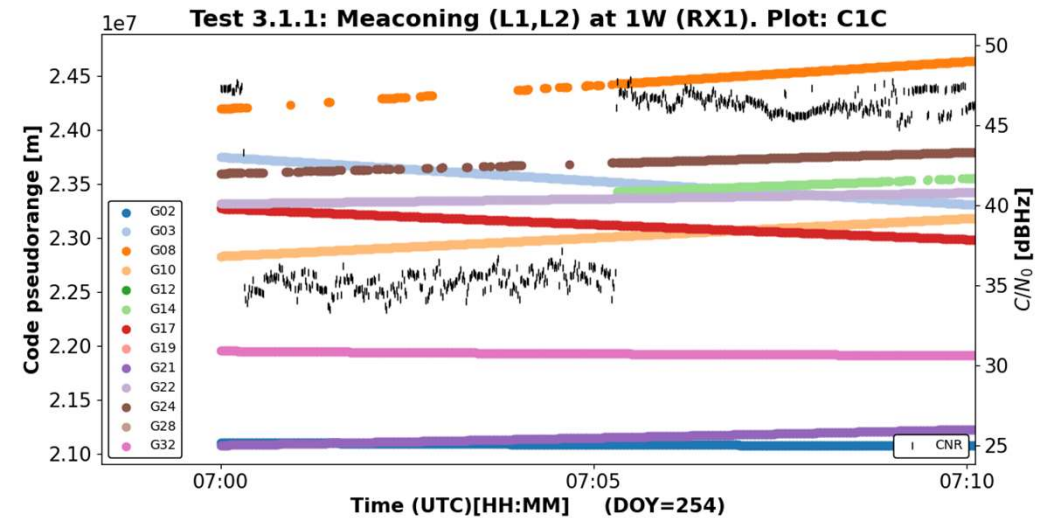
Meaconing

- Lav effekt 1W
 - Liten påvirkning



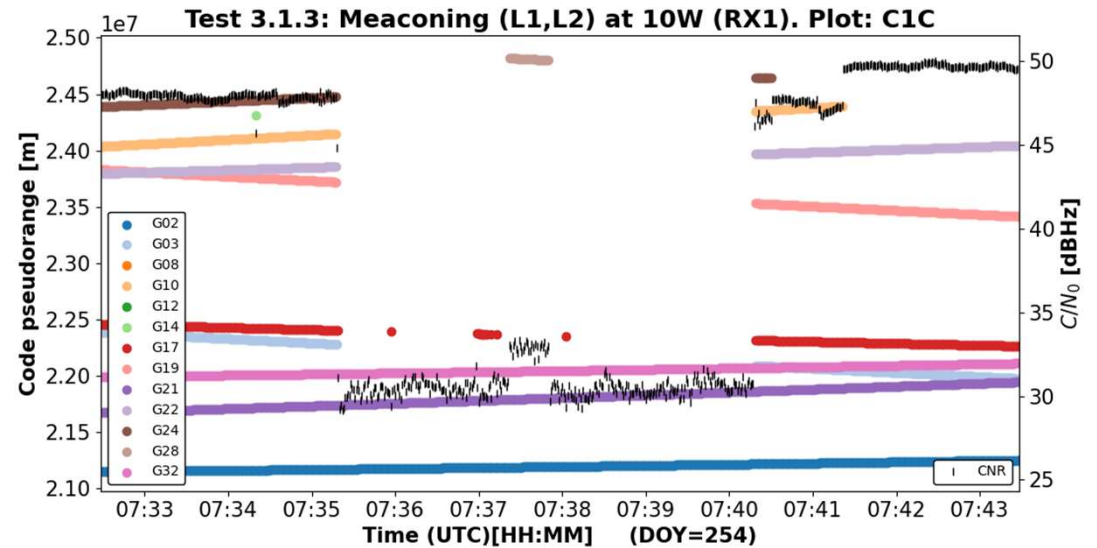
Meaconing

- Lav effekt 1W
 - Liten påvirkning
- Jamme først
 - Stor påvirkning - bare to satelitter



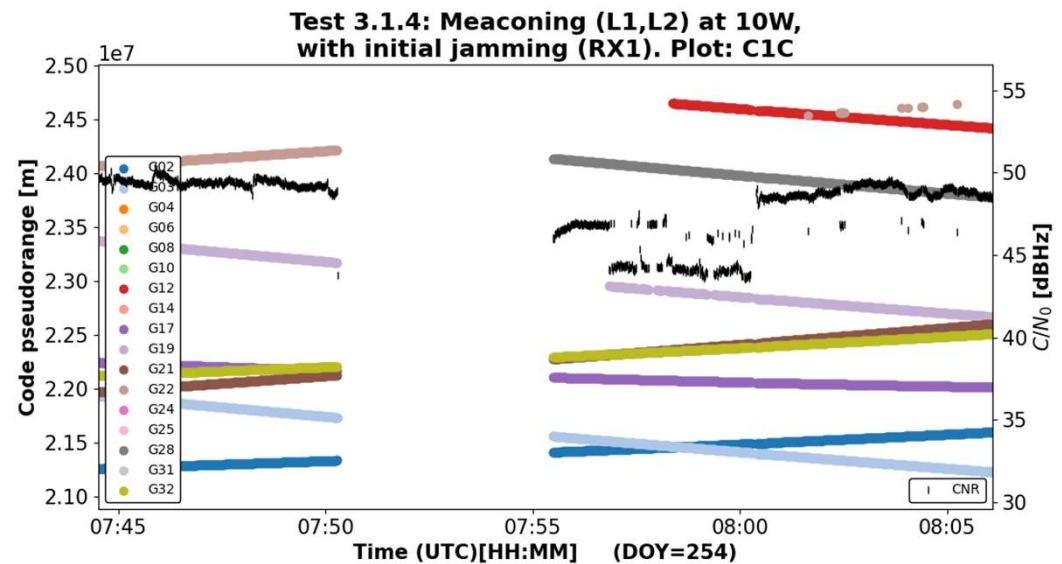
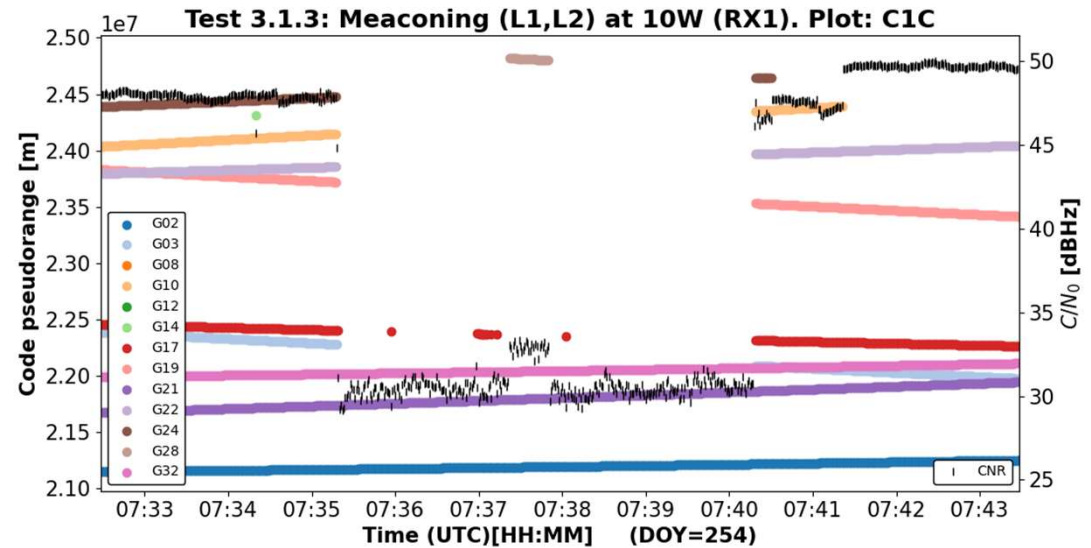
Meaconing

- Lav effekt 1W
 - Liten påvirkning
- Jamme først
 - Stor påvirkning - bare to satelitter
- Høy effekt 10W
 - Stor påvirkning

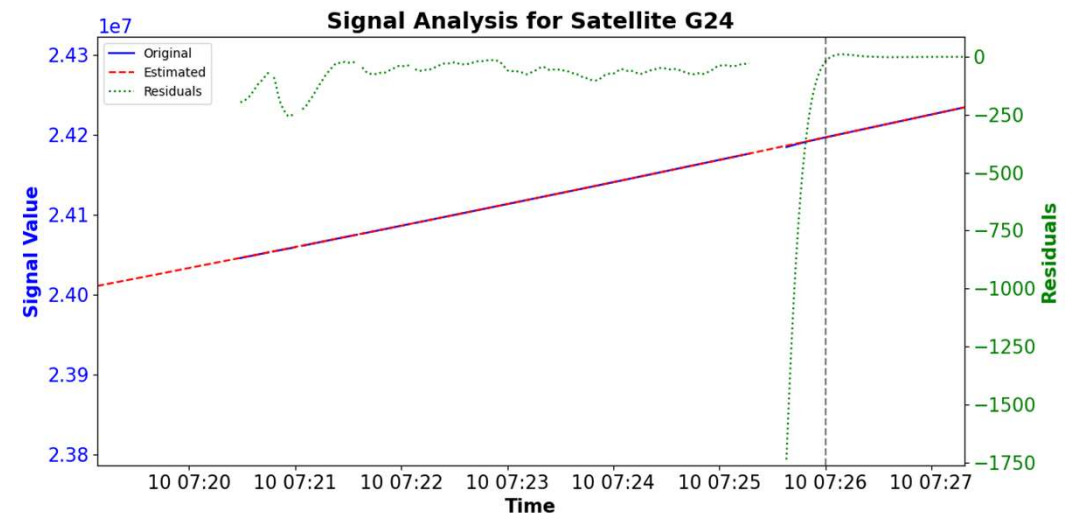


Meaconing

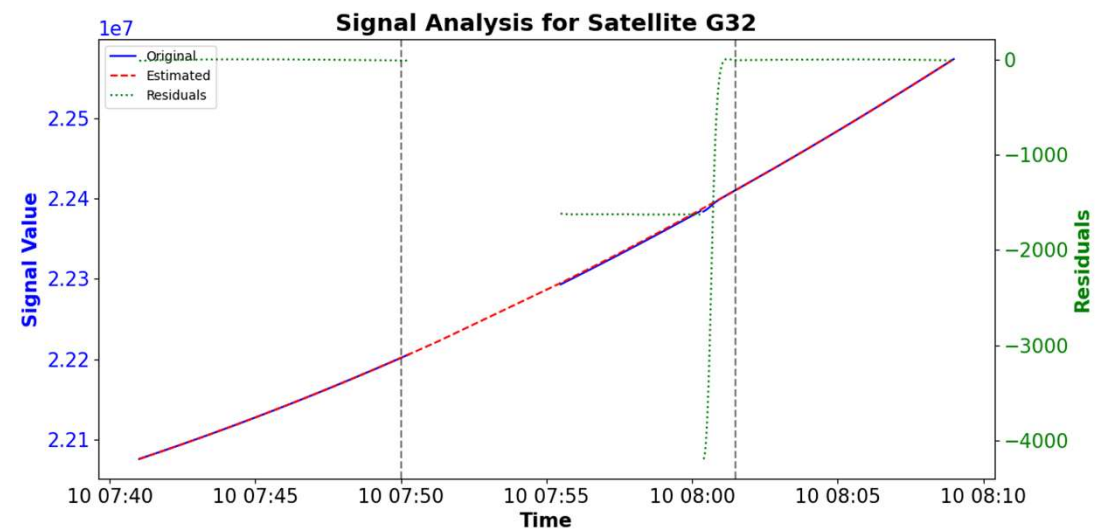
- Lav effekt 1W
 - Liten påvirkning
- Jamme først
 - Stor påvirkning - bare to satellitter
- Høy effekt 10W
 - Stor påvirkning
- Jamme først
 - Flere satellitter spores
 - Falsk pseudoavstand



- Test 3.1.2: lave residualer -> riktig pseudoavstand
- Stort avvik når meaconing rundt 07:25:40, ca. 20 sek etter meaconing er ferdig.



- Test 3.1.4 høye residualer



Spoofing

- **Ikke-koherent spoofing, falske efemerider:** Falske satelittbaner kan gi store avvik i pseudoavstand
- **Ikke-koherent spoofing, ekte efemerider:** Ved å lage en forsinkelse i kodene kan man andre registrerte pseudoavstander
- **Koherent spoofing:** Signalets fase er synkronisert med fasen til det ekte GNSS-signalet. Pseudoavstand manipuleres også her ved forsinkelse i kodene. PRN-koden kan forskives med x antal chips, eller hele kodelengder.

Spoofing

- Ofte falske pseudoavstander, men aldri falske posisjoner
- Ved høy nok effekt, kan ikke-koherent spoofing med falske efemerider være nok til å lure mottaker til å spore falske signaler
- To tester satte mottaker ut av spill, krevde manuell innblanding
 - Ikke-koherent spoofing med flaske efemerider, med høy effekt (1W)
 - Koherent spoofing med initiell jamming, med 0.1W spoofing-effekt
- Det finnes noen sikkerhetsmekanismer i Novatel-kortet.
 - Stor posisjonsendring kan føre til at målemotoren må reinitialiseres.

Spoofing

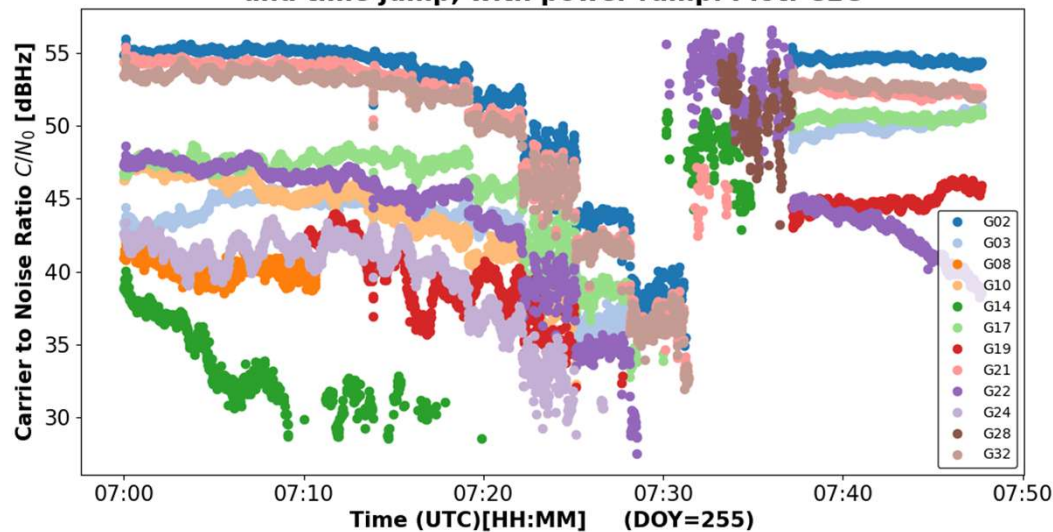
	Spoofing	
2.1.1	Incoherent spoofing, synthetic ephemerides, all signals, in close proximity(~20m), power ramp.	At maximum spoofing power (30dBm=1W) spoofed pseudoranges are tracked. Difficulty recovering: Measurement engine was reinitialized for receiver 1.1
2.1.2	Incoherent spoofing, synthetic ephemerides, L1, in close proximity(~20m), 0.316W.	Drop (~15 dBHz) in CNR. Only pseudorange tracking of the highest CNR signals.
2.1.4	Incoherent spoofing, synthetic ephemerides, L1 (and E1), in close proximity(~20m), 0.316W.	Drop (~20 dBHz) in CNR. Only pseudorange tracking of the highest CNR signals. One false pseudorange reported.
2.1.10	Incoherent spoofing, synthetic ephemerides, L1,L2,L5,E1,E5, in close proximity(~20m), 0.1W.	Drop (~15 dBHz) in CNR. Pseudorange tracking for many of the satellites. Receiver 1.2: False pseudoranges reported, followed by 45min oscillations after test.
2.2.3	Incoherent spoofing, true ephemerides, L1,L2,L5,E1,E5, in close proximity(20m), 0.1W.	Drop (~10 dBHz) in CNR for some satellites. And increased CNR for 4 satellites. Some true and some false pseudoranges reported. Receivers give correct navigated position!
2.3.3	Coherent spoofing, L1,L2,L5,E1,E5, in close proximity(~20m), 0.1W.	Drop (~10 dBHz) in CNR for some satellites. And increased CNR for 3 satellites. Some true and some false pseudoranges reported. Receivers give correct navigated position!
2.3.2	Coherent spoofing, L1,L2,L5,E1,E5, in close proximity(~20m), 0.1W. Initial jamming.	High and fluctuating CNR. False pseudoranges reported. Difficulty recovering: Intermittent tracking of C1C and no tracking of C2S, for both receivers, after test. By deactivating tracking of everything but GPS, receiver was able to regain position.
2.3.5	Coherent spoofing, L1,L2,L5, in close proximity(~20m), 0.1W.	Similar test as 2.3.3, and similar result, where it seem some satellite trackings are correct and others not.
2.3.11	Coherent spoofing, L1,L2,L5,E1,E5, in close proximity(~20m), 0.1W. Initial jamming.	Similar test as 2.3.2. False pseudoranges reported.

Spoofing

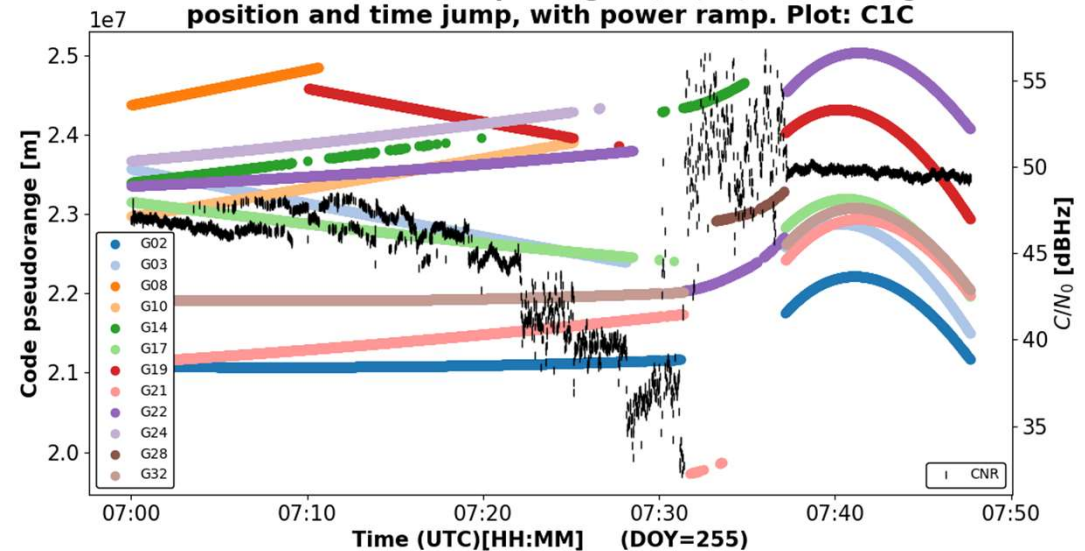
- 0.0316W -> 5dBHz drop in CNR
- 0.1W -> 10dBHz drop in CNR
- 0.316W -> 15dBHz drop in CNR
- 1W -> Spoofed pseudoranges tracked

- Feil pseudoavstand også etter testen
- Deretter ingen sporing
- Målemotor reinitialiseres

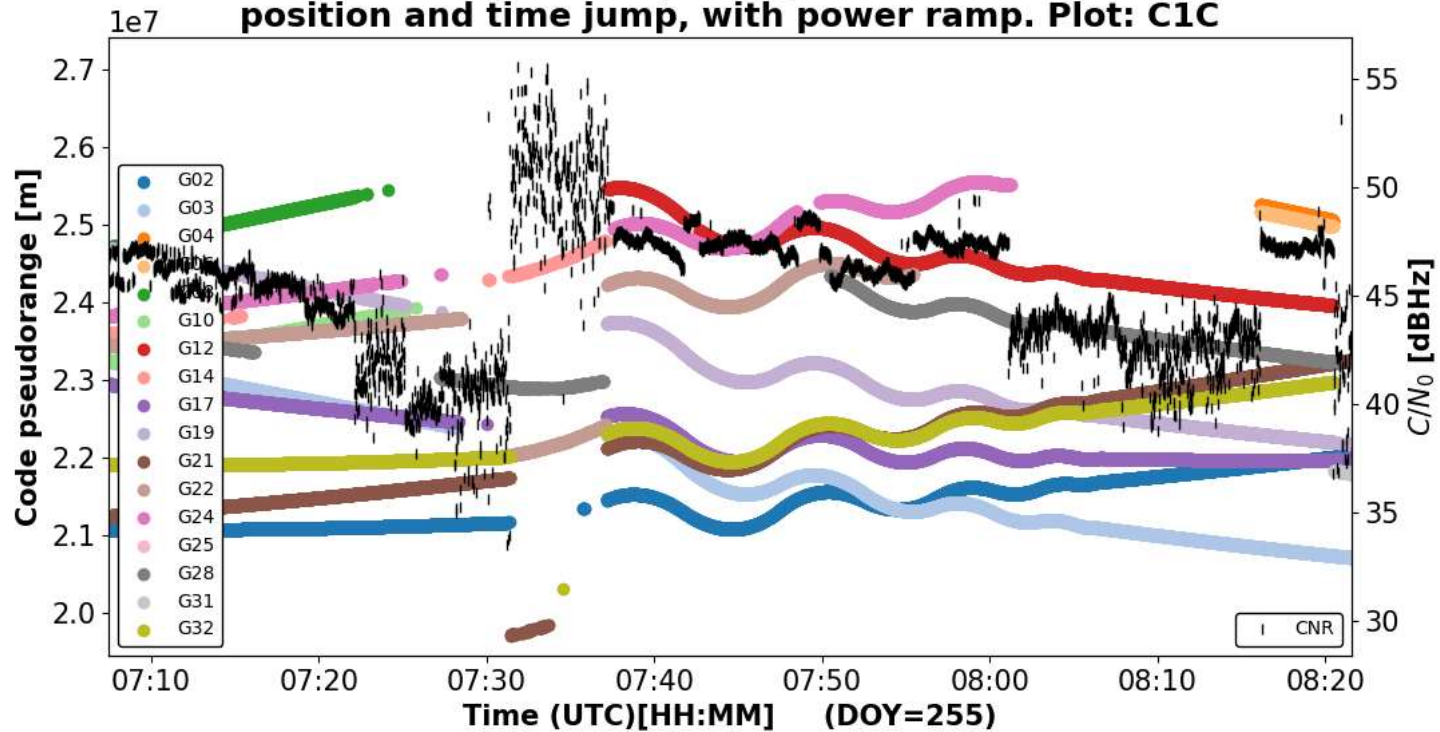
Test 2.1.1: Incoherent spoofing (L1,L2,L5,E1,E5)- Large position and time jump, with power ramp. Plot: C1C



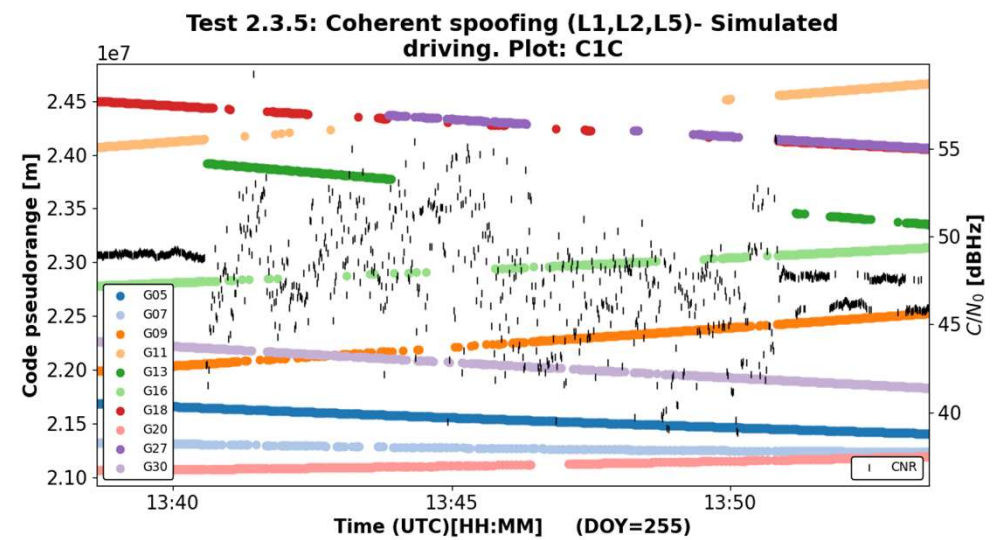
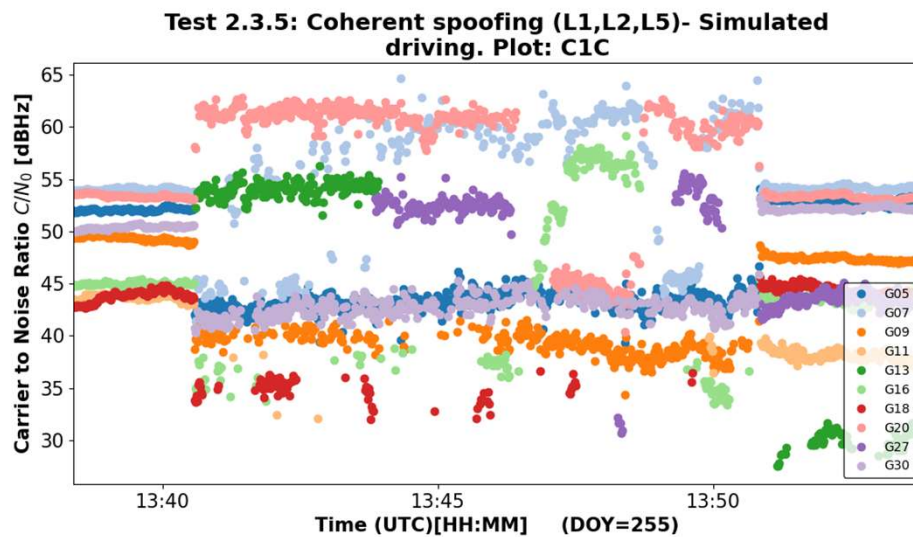
Test 2.1.1: Incoherent spoofing (L1,L2,L5,E1,E5)- Large position and time jump, with power ramp. Plot: C1C



Test 2.1.1: Incoherent spoofing (L1,L2,L5,E1,E5)- Large position and time jump, with power ramp. Plot: C1C



- Høyere CNR for noen satellitter – og falske pseudoavstander
- Lavere CNR for noen satellitter – og korrekte pseudoavstander



Test 2.3.5 - pseudoavstander for C1C

