FFI Forsvarets forskningsinstitutt

FAKTA

Mars 2025 – Foto: David Jensen

Hva er jamming, spoofing og meaconing?

I dagens samfunn er vi stadig mer avhengige av å vite hvor vi er, og til hvilken tid. Men hva hvis noen tukler med systemene vi er avhengige av?

Nasjonal sikkerhetsmyndighet har definert posisjonsangivelse, navigasjon og tidsangivelse (PNT) som en av våre grunnleggende nasjonale funksjoner. Det vil si at helt eller delvis bortfall av PNT vil få konsekvenser for statens evne til å ivareta nasjonale sikkerhetsinteresser. PNT-forstyrrelser kan også ramme kommunikasjon, navigasjon og bruk av våpensystemer i militære operasjoner.

Det finnes ulike kilder for PNT-informasjon. Den kanskje aller mest kjente er det amerikanske systemet GPS (Global Positioning System), som blant annet finnes i treningsklokker, mobiltelefoner og kjøretøy. GPS er en av fire globale satellittnavigasjonssystemer (GNSS) som gir global PNT-informasjon. De andre er det russiske GLONASS, europeiske Galileo og kinesiske BeiDou.

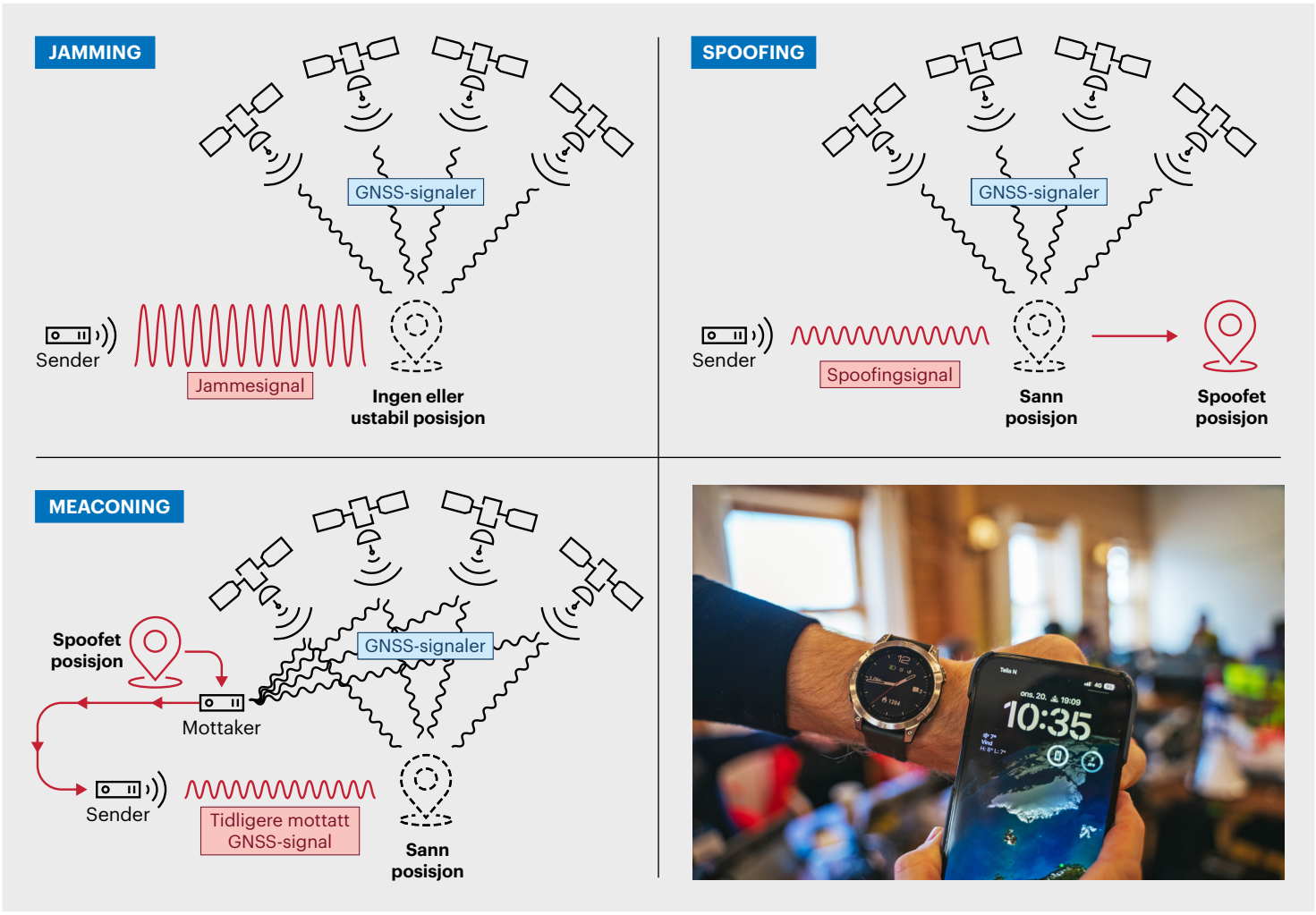
Alle disse satellittnavigasjonssystemene baserer seg på utsendte radiobølger (trådløse signaler) fra satellitter. Disse radiobølgene har kjente signalformer og svært lav energi når de når frem til bakken. Dermed er de svært utsatt for forstyrrelser eller interferens av andre radiobølger (*radio frequency interference* – RFI).

Disse forstyrrelsene (RFI) kan deles inn i tilsiktede og utilsiktede. De tilsiktede er laget for å forstyrre. Utilsiktede forstyrrelser kan komme av feil på utstyr og atmosfæriske forstyrrelser.

Tilsiktede forstyrrelser av GNSS kan deles opp i jamming, spoofing og meaconing.

Jamming
Jamming av GNSS-signaler vil si å sende ut støy for å hindre en GNSS-mottaker i å virke som den skal. Dette kan for eksempel bety at GNSS-mottakeren ikke klarer å beregne egen posisjon, eller at posisjonen som beregnes, er unøyaktig. Hvor effektiv jammingen er avhenger av utstrålt effekt, om det er fri sikt mellom jammeren og mottakeren, og formen på jammesignalet. For at jammingen skal være effektiv, må jammesignalet benytte samme frekvensbånd som benyttes av de GNSS-signalene jammesignalet skal forstyrre.

Spoofing
Spoofing er en forstyrrelse av GNSS for å få påvirkede GNSS-mottakere til å beregne feil posisjon eller tid. Spoofing kalles også for narring eller villedning.



De tre illustrasjonene viser forskjellen på jamming, spoofing og meaconing. Bildet til høyre: Mange moderne dingser henter info om tid og posisjon fra satellitter. Klokka til venstre går riktig. Telefonen til høyre blir lurt av spoofing fra Justervesenet. Foto: David Jensen

I et vellykket spoofingforsøk kan den som genererer de falske satellittsignalene, bestemme hvilken posisjon og tid mottakerne som blir spoofet, skal beregne. For eksempel kan et spoofingsignal gjøre at en GNSS-mottaker i Norge 1. januar 2025 kl. 10:00, tror at den befinner seg i Australia 1. juni 2023 kl. 20:00.

Meaconing

Meaconing, også kalt repeaterjamming, er et oppsett bestående av en mottakerantenne og en senderantenne for å re-transmittere satellittsignaler. Mottakerantennen mottar først de ekte GNSS-signalene for deretter å sende disse signalene ut igjen med en senderantenne, på et annet sted og til en annen (forsinket) tid. GNSS-mottakere som tar imot disse signalene vil tro at de befinner seg i samme posisjon som mottakerantennen til meaconingoppsettet, og tiden de beregner, vil ha en tidsforsinkelse lik forsinkelsen i meaconingoppsettet. På denne måten blir GNSS-mottakeren spoofet (narret) til en annen posisjon og til et annet tidspunkt.

Hva kan vi gjøre – mulig mottiltak?

Det finnes en rekke tiltak for å gjøre en GNSS-mottaker mer motstandsdyktig mot jamming, spoofing og meaconing. Siden alle disse forstyrrende signalene trenger fri sikt til mottakeren, kan man benytte bygninger eller terrenget for å skjerme sin egen mottaker. I tillegg kan man benytte antenner som tar inn signaler der hvor satellittene er (oppover), og reduserer signalet i andre retninger. Avanserte antennesystemer med flere antenneelementer kan kraftig redusere (nulle ut) signaler fra de retningene som de forstyrrende signalene kommer fra. Dette blir ofte kalt antijammeantenner, nullstyringsantenner eller Controlled Reception Pattern Antenna (CRPA).

For å beskytte seg mot de falske spoofingsignalene vil mottakere som utnytter krypterte signaler fra satellittene, være effektive, men dette er foreløpig begrenset til militære mottakere.

Man kan også gjøre tiltak i GNSS-mottakeren. For enkelte signaler kan filtrering av frekvenser være effektiv beskyttelse. Noen mottakere kan også benytte flere frekvensbånd. De vil da kunne overleve dersom ikke alle frekvensbåndene er forstyrret.

I tillegg til å gjøre antennene og mottakerne mer robuste, kan man bruke andre navigasjonssensorer som støtte til GNSS eller som alternative PNT-kilder. Eksempler her er treghetsnavigasjon, kamerabasert navigasjon, høydemåler og terrengnavigasjon.

Har du spørsmål, ta kontakt med:

Tonje Nanette Arnesen, forskningsleder
tonje-nanette.arnesen@ffi.no

Anders Rødningsby, sjefsforsker
anders.rodningsby@ffi.no

Kommunikasjonsenheten ved FFI
info@ffi.no

Mer informasjon om FFI og forskningen vår finner du på ffi.no