Workshop GNSS Interferentie en

Op woensdag 31 januari 2018 vond een workshop plaats over de actuele problematiek rond interferentie en authenticatie van GNSS (Global Navigation Satellite Systems). Ruim 100 mensen bezochten de workshop in het historische Teylersmuseum in Haarlem. De organisatie was een samenwerking tussen de Hydrographic Society Benelux (HSB), het Nederlands Instituut voor Navigatie (NIN) en Geo-Informatie Nederland (GIN). Veel leden van deze verenigingen hebben als hydrograaf, navigator te land, ter zee of in de lucht of als landmeter steeds vaker te maken met verstoringen die het gebruik van GNSS voor hun beroep bemoeilijken. Dagvoorzitter was John Loog van de Hydrografische Dienst van de Marine. Maar liefst vijf sprekers kwamen aan het woord om hun expertise te delen met de aanwezigen.

Introductie Radio Interferentie

Jaco Verpoorte van het NLR gaf als eerste spreker een inkijkje in de algemene oorzaken van radio-interferentie en wat je er aan kunt doen. Het radiofrequentiespectrum in Nederland en de wereld is overvol. Er hoeft maar weinig te gebeuren of je zit in iemand anders zijn frequentieruimte. Regulering en controle zijn dus belangrijk. Niet alleen voor navigatie en plaatsbepaling zijn we afhankelijk van GNSS. Ook banken en telecombedrijven gebruiken GNSS, bijvoorbeeld als nauwkeurige klok voor het synchroniseren van hun processen. GNSS signalen zijn zeer zwak door het beperkte zendvermogen van de satellieten plus de enorme afstand van ruim 20.000 km tot de aarde. Niet alle verstoringen zijn afkomstig van de mens. Ook zonneactiviteit kan GNSS ontvangst belemmeren. En niet alle door de mens veroorzaakte interferentie is moedwillig. Slechte schakelingen of povere afschermingen kunnen onbedoeld tot signalen in de GNSS frequentiebanden leiden. Verstoringen die expres worden veroorzaakt zijn in twee typen te onderscheiden: jamming en spoofing.

Bij jamming wordt er een sterker signaal op of in de buurt van een GNSS frequentie uitgezonden waardoor de GNSS ontvanger het GNSS signaal niet meer kan vinden. Hierbij ontzegt men, net als bij een DDoS aanval, iemand het gebruik van GNSS. Geavanceerder wordt het bij spoofing. Hierbij zendt men signalen uit die afkomstig lijken te zijn van GNSS satellieten en die de GNSS ontvanger ergens anders uit laten komen, dan waar deze werkelijk is. Dit lijkt meer op hacken / overnemen van de plaatsbepaling. Jammers zijn op internet zeer goedkoop te verkrijgen en worden vaak eufemistisch 'Personal Privacy Devices' genoemd. Mensen die niet gevolgd willen worden door hun werkgever of door de politie, maken hier gebruik van.

Richard Gutteling Novatel spreekt de zaal toe.

Men kan moedwillige verstoringen tegengaan door onder andere het gebruik van multi-constellatie / multi-frequentie GNSS, het afschermen van antennes, gebruik te maken van additionele sensoren, zoals traagheidsnavigatie en wielsensoren, slimme filters in te bouwen in ontvangers of zelfs compleet andere systemen dan GNSS als back up te gebruiken.

Novatel OEM7 Interferentie Toolkit

Richard Gutteling van GNSS ontvanger fabrikant Novatel (onderdeel van Hexagon) gaf de aanwezigen vervolgens een inkijkje in de standaard mogelijkheden van een Novatel OEM7 GNSS board. De Interferentie Toolkit (ITK) beschikt over een spectrum analyzer, zodat grafisch te zien is waar de interferentie zich bevindt in de band. Bij het gebruik van meerdere ontvangers is het zelfs mogelijk de bron van de verstoring uit te peilen en dus te lokaliseren. Ook heeft het board de optie High Dynamic Range Mode (HDR). Door het echte signaal te versterken in de nabijheid van een sterk interferentiesignaal kan men toch doorwerken. Alleen interferenties die pal op de centrale GNSS frequentie zitten, zijn niet weg te halen. Bij filteren haal je dan namelijk het echte signaal ook weg. De werking van de ITK werd vervolgens op video gedemonstreerd door een VHF radio (die met zijn tiende harmonische frequentie als stoorbron op de L1 frequentie fungeert) dichtbij een Novatel ontvanger te houden. Veel toepassingen, waaronder RTK, werkten na ingrijpen van IKT gewoon door met nauwelijks kwaliteitsverlies.

Interferentie en spoofing tegenmaatregelen in Septentrio ontvangers

Tom Willems van GNSS leverancier Septentrio uit Leuven was de derde spreker. Septentrio is onder andere partner van ESA en gespecia-

Authenticatie

Alle 5 sprekers bedankt.

Dagvoorzitter John Loog.

liseerd in 'Precieze Positie en Tijd'. Septentrio ontvangers beschikken over geavanceerde filters om verschillende soorten jamming tegen te gaan, zowel smalbandige als breedbandige interferentie. De filters detecteren zelfs het variabele gedrag van jammers, waardoor deze in de praktijk minder problemen geven.

Ook voor spoofing bestaan tegenmaatregelen. Spoofing is in korte tijd heel populair geworden door het spelletje Pokémon Go. Door de GPS van je eigen telefoon te spoofen kan het spel denken dat je op plaatsen bent waar je anders nooit zou komen en kun je in korte tijd veel punten met het spel verzamelen. De mensen van Septentrio lieten zien dat, met wat gratis software plus wat simpele hardware, het voor een paar honderd euro mogelijk is een iPhone 6 op de Mount Everest neer te zetten. Spoofing kan echter ook door criminelen of door kwaadaardige regimes worden ingezet. Septentrio heeft onder andere spectrum en signaal-ruis monitoring voor het detecteren van spoofing. Ook is er Receiver Autonome Integriteit Monitoring (RAIM) en Multi band Redundantie. Spoofing vindt vaak alleen plaats op de L1 frequentie van GPS en de Septentrio ontvangers kunnen dan met alleen L2 en L5 signalen alsnog hun positie bepalen.

Galileo Open Service Navigation Message

Stefano Binda van de ESA startte zijn presentatie met een kort overzicht van de huidige status van Galileo. Op dit moment zijn er al 22 satellieten in de ruimte, waarvan 14 operationeel. Vier recent gelanceerde satellieten zullen binnenkort ook officieel bruikbaar zijn. Met enig trots liet hij zien dat de kwaliteit van de Galileo satellieten op dit moment die van GPS overstijgt door betere klokken en betere satellietbanen. Daarnaast wordt een grote rol voorzien voor Galileo bij autonoom rijden, vooral in combinatie met GPS en GLONASS.

Galileo wil zich graag onderscheiden door robuuste en betrouwbare plaatsbepaling en timing. Hiervoor zijn verschillende authenticatie maatregelen in ontwikkeling om de eindgebruiker te beschermen tegen bedrog en namaak. Eén daarvan is NMA: Navigation Message Authentication. NMA is een open source techniek die werkt met cryptosleutels en in elke ontvanger geïmplementeerd kan worden. Verwacht wordt dat NMA vanaf 2019 kan worden ingezet.
Nog in ontwikkeling is een tweede techniek genaamd Code geBaseerde Authenticatie (CBA). Deze techniek wordt mogelijk in de tweede generatie Galileo satellieten ingebouwd.

Authenticatie oplossingen

Als laatste spreker van de middag kwam Daan Scheer van Fugro aan het woord. Fugro is zich, als wereldwijde aanbieder van correctiediensten voor nauwkeurige plaatsbepaling, heel bewust van de toenemende dreiging van hacking en spoofing. Fugro vindt dat Positiebepaling integer moet zijn en werkt daarom ook aan bijvoorbeeld Navigation Message Authenticatie. Daan Scheer haalde als voorbeeld taxichauffeurs aan van Uber, die hun GPS positie spoofen op het lokale vliegveld, zodat ze eerder een passagier toegewezen krijgen, zonder daar eerst te moeten wachten. Ben je echter als professionele gebruiker in de buurt van zo'n taxi, dan zal je eigen GNSS positie ook niet juist zijn.
Fugro beveelt vooral een fusie aan tussen verschillende systemen voor "maximale robuustheid": Navigation Message Authenticatie, externe sensoren zoals IMU, radar en Lidar, andere signalen (WIFI, Bluetooth), Map Matching en natuurlijk GNSS augmentatie.

Met dank aan John Loog (Ministerie Van Defensie) en Hans Visser (Fugro), als organisatoren, en Jaco Verpoorte (NLR), Richard Gutteling (Novatel), Tom Willems (Septentrio), Stefano Binda (ESA) en Daan Scheer (Fugro) als sprekers.

Jean-Paul Henry
info@06-gps.nl