DE KEUS VAN INGENIEUR TEUS

ir. Teus van der Plaat

GPS SPOOFING SYMPTOOM VAN HET CYBER GEVECHT TUSSEN STATELIJKE ACTOREN

Op verzoek van de redactie buig ik me deze keer over de status van de GPS-systemen, waarvan er momenteel vier actief zijn. De praktijk is dat GPS-systemen in toenemende mate worden gestoord. Allereerst een overzicht en korte geschiedenis van de diverse actieve systemen.

Beschikbare systemen

In de eerste plaats is er het aloude GPS dat ontworpen en beheerd wordt door het Pentagon. Men begon in 1978 met de lancering van de eerste van de 32 satellieten die het systeem nu heeft.
Aanvankelijk alleen voor militaire toepassingen met grote nauwkeurigheid en encryptie, maar tijdens de Golfoorlog in 1990, toen de Amerikanen Koeweit binnenvielen waren er te weinig crypto-apparaten beschikbaar en heeft het US-commando besloten de encryptie (tijdelijk) te verwijderen waardoor naast de militairen ineens voor iedereen een veel hogere precisie beschikbaar kwam .

Al heel snel gingen de voertuignavigatiesystemen (opkomst van Tom Tom) dit gebruiken en werden later de chips die dit ondersteunen opgenomen in de mobiele telefoons. Het eind van het liedje was dat de encryptie er af bleef voor civiel gebruik en we nu allen dagelijks gratis gebruik maken van dit GPS-systeem. Zowel de EU (Galileo) als de Russen (GLONASS) en Chinezen (BeiDou) vonden en vinden het niks dat de hele wereld afhankelijk is van een door de US militairen beheerd systeem, waarmee ze in principe alles kunnen doen wat ze willen.
Vooral de EU zet sterk in op een alternatief systeem, genaamd Galileo. Dit systeem is in 2020 nagenoeg volledig operationeel (30 satellieten) en is in sommige aspecten beter dan het US GPS-systeem. Galileo is expliciet een niet militair systeem en de totale investeringskosten zijn ca. 10 miljard euro. De nauwkeurigheid is ca. 20% beter dan GPS en de dekking in noordelijke gebieden is kwalitatief beter. Daarnaast komt er een betaalde service die een nauwkeurigheid van ca. 20 cm moet kunnen halen. Er is ook een Search and Rescue faciliteit bij Galileo. Er kan een noodsignaal vanaf de aarde ontvangen worden door de satelliet, de positie wordt bepaald en het signaal wordt doorgezonden. De zender van het noodsignaal krijgt een respons dat de noodoproep is ontvangen, zodat men kan weten dat er hulp onderweg is.

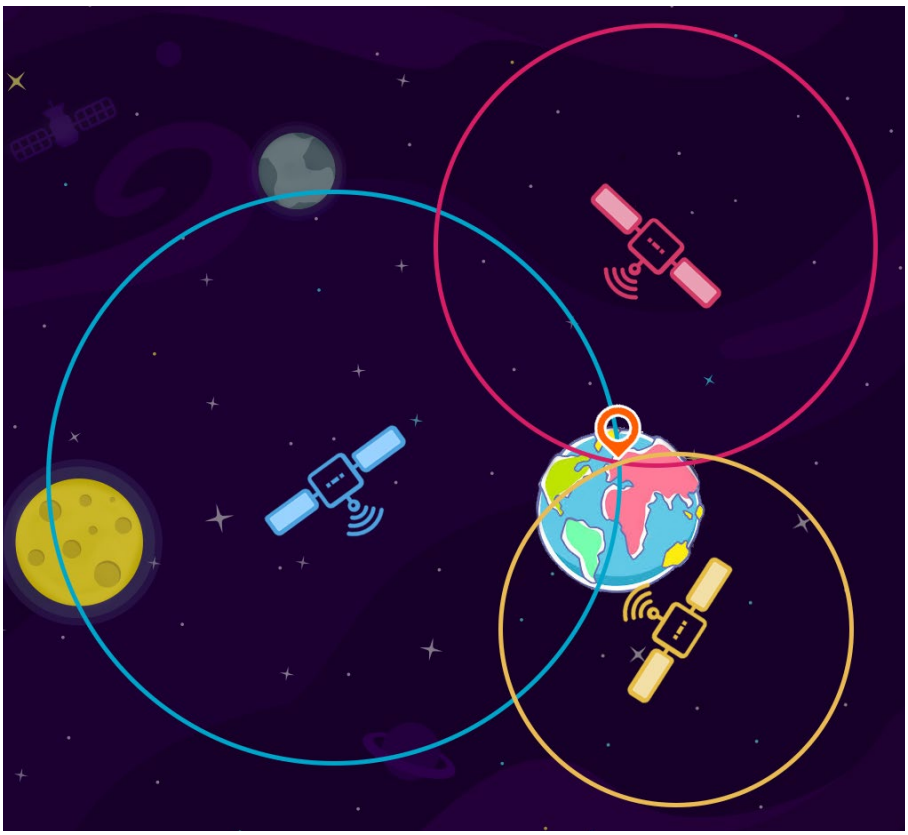
Inmiddels gebruiken alle nieuwe smartphones naast GPS ook Galileo. Van de ca. 7 miljard smartphones op de wereld kunnen al 1 miljard devices naast GPS ook werken met Galileo. Door combinatie van de systemen wordt de behaalde nauwkeurigheid van de plaatsbepaling groter. Ook het Chinese BeiDou en Russische Glonass kunnen

gebruikt worden door bijna elke nieuwe smartphone (Android en Apple).
Zo is bekend dat Google-maps probeert alle beschikbare plaatsbepalingssystemen te gebruiken om de positie zo goed mogelijk te bepalen.

Storingsgevoeligheid van GPS-systemen

De frequenties die gebruikt worden voor alle vier systemen liggen tussen de 1200 en 1600Mhz. Dit zijn frequenties die gemakkelijk opgewekt kunnen worden met draagbare devices en kleine antennes. Een bekende GPS-hack gebeurde toen Poetin de brug naar de Krim opende. In de stoet auto's die hem begeleidde reed een auto mee die ter plekke alle GPS stoorde, e.e.a. uit angst dat er een aanslag op Poetin gepleegd zou worden. Op dat moment kwam het bericht van wel 24 schepen die in de buurt lagen dat hun plaatsbepalingssystemen meldden dat ze met het schip 60 km verderop op het land lagen. De Russen zijn sindsdien zeer actief met GPS-spoofing en -hacking. In totaal zijn wereldwijd al meer dan 10.000 rapportages geweest van verstoring van plaatsbepalingssysteem door waarschijnlijk moedwillige acties. De kosten om een hacking device te maken zijn inmiddels gedaald naar ca. 300 dollar.
We kunnen dus constateren dat we als maatschappij in het geheel en defensie in het bijzonder een flink probleem hebben.

In het algemeen wordt aangenomen dat de veroorzaakte storingen grotendeels gecreëerd worden door de zogenaamde statelijke actoren, ofwel inlichtingendiensten en/of militaire organisaties. In een recente zeer boeiende uiteenzetting in Brussel over security in 5G door de directeur van de denktank Epice, Hosuk Lee-Makiyama (adviseur van de EU over politiek en technologie) en de Noorse professor Olav Lynse (adviseur Noorse regering) werd geconstateerd dat het huidige veiligheidsdilemma uiteindelijk in feite maar één oorzaak heeft : "Zolang overheden elkaar niet vertrouwen is en blijft er een security dreiging waar we



ons nauwelijks tegen kunnen wapenen". Deze vraag speelt momenteel sterk bij de selectie van de 5G-netwerkapparatuur. Bij de geconstateerde verstoringen van GPS is dit probleem in mijn visie hierdoor nagenoeg onoplosbaar gezien de enorme technologische mogelijkheden van de statelijke actoren.

Hoe wapenen tegen verstoring GPS?

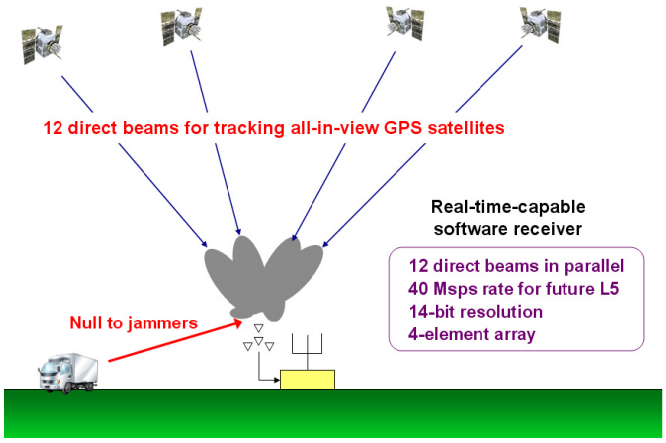
De vraag is hoe we dit toch kunnen voorkomen, of hoe maken we ons minder kwetsbaar voor verstoringen?
Als radiopropagatie- en antenneliefhebber is er in mijn visie een aantal maatregelen te nemen die verstoringen kunnen verminderen danwel voorkomen. Allereerst is het zaak alle beschikbare systemen continu met elkaar te vergelijken. Zodra er een flinke afwijking is op een van die systemen zou die automatisch genegeerd moeten worden.

Voorkomen dat er met sterke zenders op die frequenties gestoord wordt is moeilijk, zeker gezien de zeer lage kosten waarmee stoorzenders gemaakt kunnen worden, echter bij gebruik van alle systemen moet er tegelijk op een groot aantal frequenties gestoord worden, hetgeen lastiger wordt. De te storen frequenties zijn in hoge mate 'directzicht'- frequenties zodat er een fors stoorsignaal en een directzichtverbinding moet zijn naar het te storen object. Als er een paar betonnen muren tussen zitten zwakt het stoorsignaal al sterk af. Door het principe van de beveiliging van het Israëlische Iron Dome toe te passen moet de stoorzender oppassen want anders volgt er heel snel een voltreffer.

Een andere belangrijke maatregel is het gebruiken van pencil beam richtantennes, die dynamisch de satellieten kunnen volgen. Als de gain van dergelijke antennes hoog genoeg is, wordt het veel moeilijker om de ontvangst te storen omdat de stoorzender dan uit de richting van de satelliet zou moeten komen. Smartphones hebben een omnidirectionele antenne en zijn dus veel meer kwetsbaar voor stoorsignalen.

Bied 5G een oplossing?

Het toepassen van 5G-technieken biedt nieuwe mogelijkheden op het vlak van plaatsbepaling.
In de 3GPP 5G-standaarden is er spra-



ke van de zogenaamde coöperatieve positiebepaling. Hierbij wordt de positie enerzijds bepaald door driehoeksmetingen tussen de vele basisstations, maar anderzijds ook via device to device communicatie kan de positie van naburige devices gebruikt worden. Omdat 5G zich potentieel kan uitstrekken over bijna alle thans gebruikte frequenties tussen de 700 Mhz en de 3,5 Ghz wordt het voor mogelijke hackers steeds moeilijker alle frequenties tegelijkertijd te storen. Daarnaast zijn door het gebruik in 5G van spreadspectrumtechnieken devices minder gevoelig voor storingen.
Hoewel technisch complex komt het erop neer dat het juiste signaal nog steeds gedetecteerd kan worden ondanks een zeer hoog ruisniveau. Deze vorm van positiebepaling in 5G is vooral ontwikkeld om in gebouwen en stedelijke gebieden bij afwezigheid van GPS signalen toch nauwkeurig de positie te kunnen bepalen.

Verder is het natuurlijk altijd handig om ook andere bronnen te gebruiken om je positie te bepalen. Gebruik de methoden die sinds de VOC gebruikt zijn in de scheepvaart (zon, maan en sterren).De recent geïntroduceerde methode van augmented reality in combinatie met de positie, zoals deze door Google is geïntroduceerd, biedt in stedelijk gebieden ook mogelijkheden. Aan de hand van de positie en vooraf opgenomen beelden van de omgeving (streetview) is vast te stellen of men de juiste positie heeft. Daarnaast denk ik dat met Artificial Intelligence methoden op basis van veel data heel goed vastgesteld kan worden of een storing waarschijnlijk is of niet. Een plotselinge verandering van locatie wordt hierdoor zeker opgespoord!

Kortom er zijn in mijn visie best wel een aantal methoden om de positie veilig te stellen in situaties waarin er gestoord wordt, maar makkelijk is het niet. Recent kwam het bericht dat de US army nieuwe anti-jam GPS-devices (MAPS) had gemonteerd in een aantal voertuigen. Hoe deze exact werken is mij onbekend, maar in de berichten werd wel gewag gemaakt van speciale antennes, hetgeen zou kunnen duiden op de eerder genoemde pencil beam ontvangst.

Het lijkt er op dat er een race aan de gang is waarbij het enerzijds steeds makkelijker en goedkoper wordt om te jammen, maar aan de andere kant door technologische maatregelen de gevoeligheid voor jamming weer knap gereduceerd kan worden. De race is aan de gang!
Wat dat betreft is er niets nieuws onder de zon, want dit kat en muis spel is al aan de gang sinds Hannibal met zijn olifanten 200 jaar voor Christus over de Alpen trok.