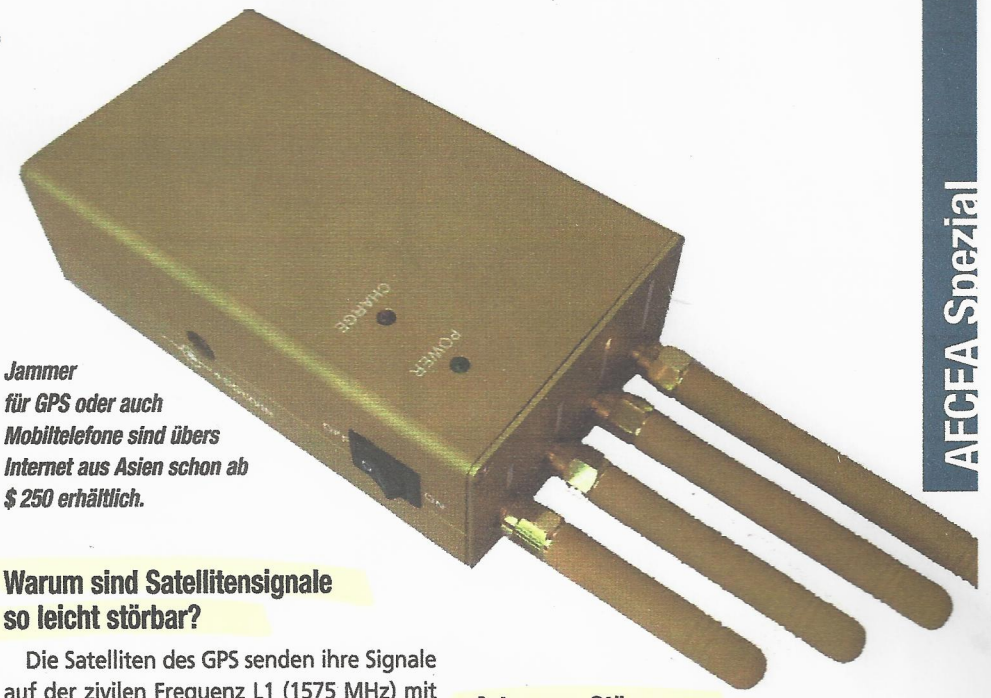
Willi Fink

Satellitennavigation – Wunderwerk der Technik oder Waffe zur elektronischen Kriegsführung?

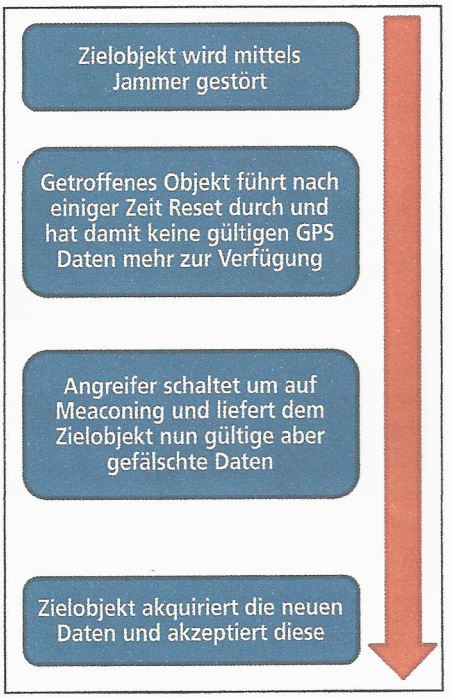
Ein roter Punkt auf weißer Fläche – wo bin ich? So wird manchmal die Aussage lauten, seit GPS-Systeme zur Positions- und Zeitbestimmung, ursprünglich militärischer Herkunft, auch auf dem zivilen Massenmarkt Einzug gehalten haben. Aber warum verlassen wir uns heute so sehr auf GPS oder GLONASS sowie in Kürze auch GALILEO? Welche Risiken können, mal abgesehen von Anwenderfehlern, damit verbunden sein? Seit Nordkorea regelmäßig den GPS-Empfang in der Nähe der Grenze zu Südkorea im Umkreis von 50-100 km stört oder GPS-Ortungssysteme durch einfache € 10 Handheld-Jammer deaktiviert werden, kommen Fragen nach Lösungen zu der Problematik des GPS Jamming immer wieder hoch. Was im zivilen Bereich unter dem Begriff GPS Jamming verbreitet ist, wird im militärischen Bereich mittlerweile als asymmetrische Kriegsführung unter dem Begriff „navigation warefare" bezeichnet. Aber warum sind unsere GNSS (Global Navigation Satellite System) so leicht störbar und wie kann man sich davor schützen? Dieser Beitrag soll einen kurzen Überblick geben. Der Autor ***Willi Fink*** *ist Geschäftsführer von* ***AuCon*** *in München, einem Systemhaus für GPS-Lösungen zur Signaldistribution für alle GNSS Bänder, wie GPS, GALILEO, GLONASS, OMNISTAR, BEIDOU und IRIDIUM. Die Signalverteilung kann drahtlos oder drahtgebunden erfolgen.*



Jammer für GPS oder auch Mobiltelefone sind übers Internet aus Asien schon ab $ 250 erhältlich.

Warum sind Satellitensignale so leicht störbar?

Die Satelliten des GPS senden ihre Signale auf der zivilen Frequenz L1 (1575 MHz) mit einer Leistung von rund 25 W (44 dBm), im militärischen L2 Band mit 4.5 W (37 dBm) aus. Aufgrund der großen Distanz von 20.000 km und der damit verbundenen Verluste in der Atmosphäre kommen die Signale auf der Erde mit nur ca. -136 dBm im L1-Band und -128 dBm im L2 Band an. GPS Empfänger müssen somit Signale erkennen und verarbeiten, deren Werte deutlich unterhalb des natürlichen Rauschens (ca. -108 dBm) liegen. Wird nun in diesem Frequenzbereich ein Störsender aktiv, kann das schwache Signal damit leicht überlagert bzw. vollkommen ausgelöscht werden. Eine Zeit- und Positionsbestimmung ist dann nicht mehr möglich.

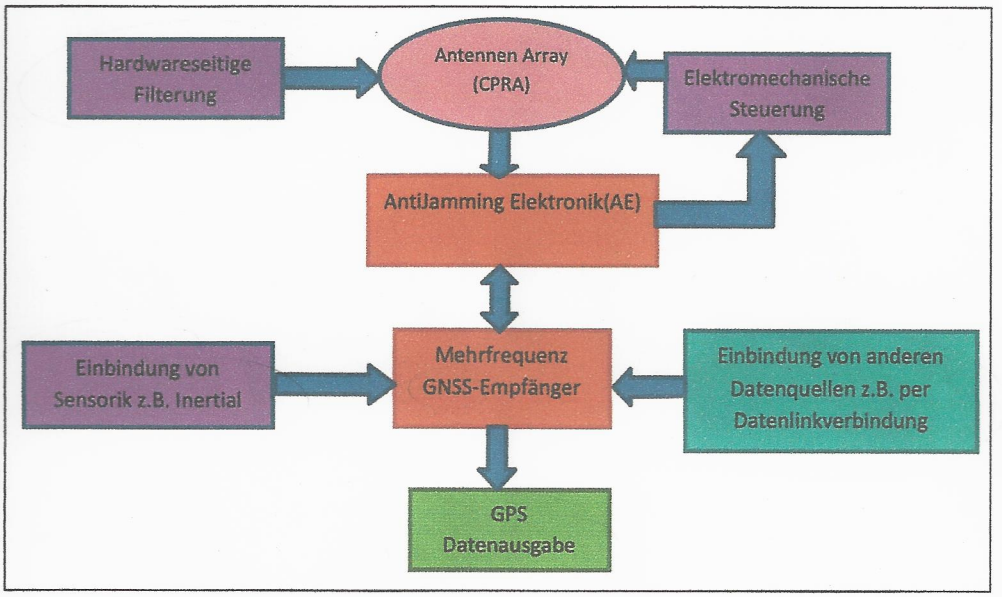


Mögliche Taktik der Störung und Täuschung (Grafik: AuCon)

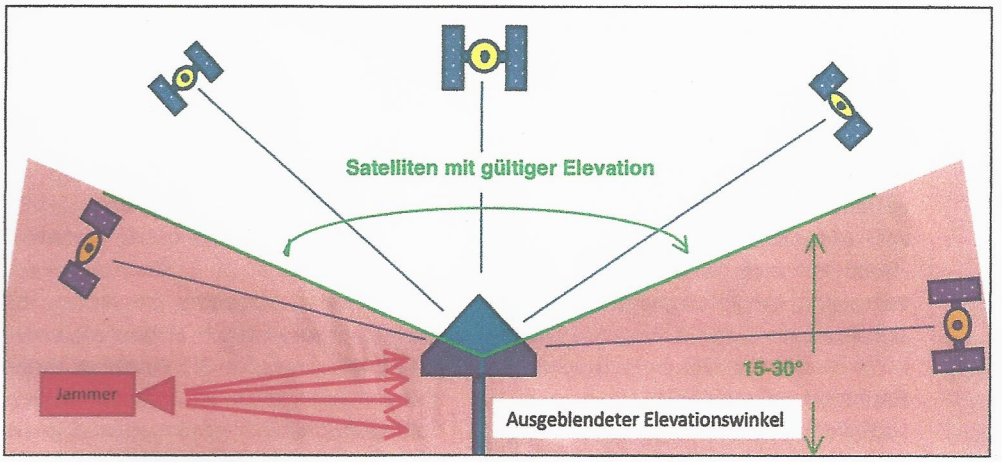
Arten von Störungen und wie sie entstehen

Die Interferenz ist eine häufig auftretende unbewusste Art von Funkstörung, verursacht durch Überlagerung von Wellen. FM oder TV Sendeanstalten können oft ungewollte Störungen des GPS-Empfangs verursachen. Aber auch Naturgewalten wie Sonneneruptionen können die Signale beeinflussen. Da diese Störungen jedoch nur temporär auftreten oder vom Nutzer beeinflusst werden können, geht hiervon keine ernsthafte Gefahr aus, lediglich die Detektion der Ursache ist nicht immer einfach, gerade dann, wenn keine hochempfindlichen Spectrum Analyser zur Verfügung stehen.

Jamming wird erzeugt von einfachen Handgeräten mit wenigen Metern Reichweite, die bereits für wenige Euro auf dem Schwarzmarkt erhältlich sind, bis hin zu mehreren Kilowatt „schweren" Jammern, die auf LKWs, Schiffen oder Flugzeugen verbaut werden und eine Reichweite von mehreren 100 km haben können. Ein zigarettenschachtelgroßer Jammer mit 1 mW Sendeleistung kann einen Umkreis von ca. 100 m stören, so dass hier für einen konventionellen zivilen GPS Empfänger kein GPS Empfang möglich ist. Der Ausfall bei einfachen L1 Band Empfängern kann entstehen, sobald der Abstand des natürlichen Signals zum Jammersignal größer als ca. 20 dB ist. Militärisch genutzte Empfänger haben bezüglich des J/S (Verhältnis Jamming to Signal) eine wesentlich höhere Immunität (J/S oft größer als 40 dB) gegen Jamming, was den Einsatz von teuren und leistungsstarken



Diese Grafik zeigt den Aufbau eines GPS Systems, das gegen Angriffe gut geschützt ist. (Grafik: AuCon)



Eine GPS Antenne dient zur Eliminierung von Signalen mit niedrigen Elevation (Grafik: AuCon)

Jammern voraussetzt. Diese befinden sich im Normalfall jedoch nicht in privater Hand und sind zudem leichter aufzuspüren.

Meaconing oder Spoofing ist das „anspruchsvollste" Verfahren und basiert auf der Manipulation gültiger Satellitensignale. Beim Meaconing/Spoofing werden gefälschte, aber gültige GPS Signale generiert und abgestrahlt. Der Einsatz dieser Systeme erfordert derzeit (noch) teure Hardware und gute Kenntnisse der GNSS Technologien.

Welche Gefahren sind damit verbunden?

Wird ein Jammer eingesetzt, um das natürliche Signal zu unterdrücken, führt der zivile Empfänger in Folge fehlender Daten regelmäßig ein Reset (Kaltstart) durch, um eine gültige aktuelle Position zu finden und verliert somit auch meist die letzten gültigen Daten. Werden nun im zweiten Schritt per Meaconing gefälschte, aber plausible Daten an den GPS-Empfänger gesendet, wird dieser die Daten übernehmen, sofern keine weitere Logik externe Daten z.B. eines GPS unabhängigen Netzwerkes vergleicht. Sowohl Zeitdaten als auch Positionsdaten können hiervon betroffen sein. Zudem erfährt der Nutzer meist nicht, dass es sich um gefälschte Daten handelt, da der Receiver diese Daten auch verarbeitet und keine Fehlermeldung liefert, wie etwa beim Jamming.

Die Taktik beim Meaconing kann sehr vielfältig sein und ist meist umso effektiver, je besser die Kenntnis des gegnerischen GPS-Systems ist. Es können beispielsweise „richtige aktuelle Daten" mit falschen Positions- oder Zeitinformationen versehen werden oder es können neue logische Daten der Zukunft (Bahndaten der Satelliten sind bekannt) generiert und abgestrahlt werden. Meaconing ist im Vergleich zum Jamming jedoch mit hohem Kapitaleinsatz für Hard- und Software sowie mit guter Kenntnis der GNSS Technologie verbunden. Meaconing kann je nach ausgebildeter „Intelligenz des Empfangssystems" eines Objektes schwerwiegende Folgen mit sich ziehen, z.B. bei Luftfahrzeugen, die bei schlechter Sicht lediglich GPS beim Landeanflug nutzen. In zeitkritischen Anwendungen wie bei Zeitservernetzwerken von Energieversorgern (z.B. beim Zu- oder Abschalten von Stromnetzen) kann dies durch falschen Zeitabgleich zu Totalausfällen führen. Auch zahlreiche andere Anwendungen im zivilen Bereich wie z.B. bei Banken, Börsen oder generell Netzwerkbetreiber die GPS zur Synchronisation von Zeitnetzwerken verwenden, wären davon betroffen. Notfallfahrzeuge bekommen mittlerweile den Einsatzort per GPS-Koordinate auf das Navigationssystem mitgeteilt. Züge werden GPS-gestützt überwacht und gesteuert. Ein Ausfall oder eine Falschinformation könnte enorme Auswirkungen auf diese Anwendungen haben und eine Art Dominoeffekt auslösen.

Zivile GPS-Ortungssysteme, die zu Sicherheitszwecken in Fahrzeugen verbaut werden, können ebenfalls auf simple Weise gestört werden. Die Folge ist, dass Überfälle auf Geldtransporte bzw. Diebstähle von Fahrzeugen zunehmen könnten, da sich der Angreifer in Sicherheit wägt, weil die Position durch die Zentrale nicht mehr festgestellt werden kann. Zudem kann die einst so hoch geschätzte GPS-Ortung zur logistischen Optimierung und Koordination von Fuhrparks vom Fahrer mit einem GPS Jammer auf einfachste Weise deaktiviert werden.

Im militärischen Bereich ist die Problematik von Jammern (Störer) und Spoofern (Meaconing) mittlerweile häufig unter dem Begriff „navigation warfare" zu finden. Zwar ist die Immunität des militärischen L2 Bandes (1227 MHz/Y-Code) gegen leistungsstarke Störer im Vergleich zum zivilen L1 (1575 MHz/C/A-Code) wesentlich höher, aber auch hier ist kein 100% Schutz gegeben. Dies betrifft vor allem den Kaltstart oder den Reset von GPS-Geräten die sowohl C/A als auch P/Y Code zur Synchronisation verwenden.

Methoden gegen Jamming:

Eine Methode ist z.B. die Einbindung von externen Informationsquellen (z.B. Einsatz von Blue Force Tracking Networks (BFTN) bei der Luftwaffe) mit einem Datenlink zur Korrektur. Bei zeitkritischen Anwendungen empfiehlt sich zusätzlich die Einbindung

nicht GPS-gestützter Zeitnetzwerke. GSM, wo verfügbar, hilft zur Übermittlung der groben Standortbestimmung per Assisted GPS.

Einbindung von Gyrosensoren (inertial) in autonome GPS Geräte, die dem System zum Überbrücken zusätzliche Richtungs- und Beschleunigungsinformationen liefern. Dies hilft jedoch nur bei zeitlich sehr begrenzten Ausfällen des GPS Signals.

Ein sauberes Filtern der jeweiligen Nutzfrequenz durch den Einsatz hochwertiger Antennentechnik, die optimal auf den Receiver abgestimmt werden, hilft gegen Störer außerhalb der Nutzfrequenz. Softwaregesteuerte digitale Filterbanken können Störfrequenzen nach Bedarf ausblenden.

Choke-Ring-Antennen zum Schutz vor Multipatheffekten (z.B. für Referenzstationen auf Gebäuden) sind zumeist auch wirkungsvoll gegen Einflüsse von Jammern in niedrigen Elevationen also z.B. gegen bodengestütztes Jamming. Dies hilft jedoch nicht bei Jammern, die beispielsweise aus Flugzeugen abgeworfen werden oder per Heißluftballon relativ kostengünstig in den Luftraum gebracht werden können.

Anti-Jamming-Antennensysteme: Mehrere Antennenelemente in präziser geometrischer Anordnung sorgen mit der integrierten Anti Jamming Electronic für das Ausblenden bzw. Nullen des Störsenders durch z.B. Sperren fremder Wellenformen. Das richtungsabhängige Ausblenden des Störers (Beamforming) kann auch elektromechanisch erfolgen, d.h. die Antenne wendet sich von der direkten Strahlrichtung des Störers ab oder reflektiert gar das Signal zurück.

Mehrfrequenzempfänger zum Ausschalten von schmalbandigen Störern sorgen für weitere Sicherheit. Nicht nur GPS sondern auch GALILEO und GLONASS sollten künftig zur Erhöhung der Redundanz eingesetzt werden.

Durch den Einsatz von GPS-Repeatern in manchen Bereichen kann das natürliche Signal verstärkt werden, um so den „Signalabstand" zwischen dem Jammer und dem korrekten Signal zu vergrößern, z.B. in Fahrzeugen, Gebäuden oder Hangars. Der Einsatz mobiler Repeater hat sich auch bei GPS georteten Fluchtfahrzeugen bewährt, die von Kriminellen häufig nur noch mit GPS Jammern betreten werden. Durch die gezielte „Weiterleitung" des natürlichen GPS-Signals via Repeater kann das Fahrzeug auch weiterhin am Bildschirm verfolgt werden.

Die softwareseitigen Technologien sind ebenfalls vielfältig. Anti-Jamming-Software basiert auf Algorithmen, die von logischer Analyse und Vergleichen verschiedener Signale über eine höhere Bandbreite bis hin zu statistischen Auswertungen der Signale reicht. Beispielsweise kann schon eine einfache Logik plötzliche „große Sprünge" innerhalb eines kurzen Zeitraumes bei der Positionierung oder Zeitverschiebungen ausschließen (z.B. Kalman-Filter). Weiterführende Methoden sind u.a. das Wiener Filter Modell. Bei Lenkflugkörpern kann der Vergleich der gespeicherten Geländedaten mit den aktuellen Radar- oder Bilddaten für Zielsicherheit sorgen (s.a. DSMAC – Digital Scene Matching Area Correlation).

FAZIT

Nur ein optimal und aufeinander abgestimmtes GPS System kann eine hohe, wenn auch nicht 100%ige Immunität gegen Jamming und vor allem gegen Meaconing bieten. Eine Anti-Jamming-Antenne ohne Steuerung ist ebenso nutzlos wie ein Anti-Jamming-Receiver mit Standardantenne.

Bei militärisch eingesetzten Systemen raten Experten der US Navy generell darauf zu achten, das beim Kaltstart von GPS-Geräten zuerst das verschlüsselte L2-Band genutzt wird, da dies durch die geschützten Daten wesentlich schwerer durch Jamming oder Meaconing beeinflussbar ist als das zivile L1 Band. Alte L1/L2 Empfänger verwenden bisher den C/A Code zur Synchronisation und schalten dann zur exakten Positionsbestimmung auf den P/Y Code um. Leider hat die regelmäßige Änderung des P-Codes jedoch zur Folge, dass auf die Nutzung von L2 im täglichen Einsatz oft ganz verzichtet wird. Im zivilen Bereich bietet der Einsatz hochwertiger Receiver wie z.B. des Ublox6 mit AntiJamTechnologie, einen guten Basisschutz gegen einfache Jammer. Die Technologie blendet u.a. Signale mit sehr hoher Signalstärke aus der Berechnung aus.

Allerdings erfordern all diese neuen Technologien auch höhere Rechenleistungen, die entsprechend teuerer als konventionelle Empfänger sind.

AGR (Anti-Jamming-Receiver) werden von Herstellern wie **Thales** (DIGAR), **Rockwell Collins** oder **Novatel** angeboten. Anti Jamming Antennen (CRPA – controlled radiation pattern antenna) und GPS Repeater bietet AuCon für den stationären und mobilen Einsatz.

Einige Systeme können auf Basis COTS (Commercial of the Shelf) mit vergleichsweise geringem Aufwand auf den Einsatzbereich des Kunden abgestimmt werden.

Aufgrund der leichten externen Störbarkeit mit preisgünstigen Handgeräten sollte die Entwicklung eines leicht zu bedienendem Instruments zum Aufspüren von Störern gerade in Bereichen wie z.B. Flughäfen zeitnah erfolgen. Als Basistechnologie bieten sich hier konventionelle kostengünstige GPS Receiver an, da der Einsatz von Geräten zur Spektrumanalyse neben den hohen Kosten auch ein breites Basiswissen des Nutzers voraussetzt. Eine erfolgversprechende Applikation für Smartphones, die auf der J/S-Messung mittels GPS-Receiver beruht, wurde kürzlich von der Universität der Bundeswehr in Neubiberg bei München vorgestellt.

wt

http://www.miltechmag.com

Follow us on twitter: http://twitter.com/miltech1

Join us on LinkedIn: MILITARY TECHNOLOGY