Aspetti di sicurezza nell'utilizzo dei sistemi di navigazione satellitare

di Mauro Leonardi

Fig. 1 - Esempi di spoofer disponibili in commercio (Di Fonzo 2014).

I sistemi di navigazione satellitare sono sempre più utilizzati nel settore della geomatica (dal rilevamento, alla georeferenziazione, ai sistemi per la guida dei droni). Questa penetrazione nel mercato, però, non sempre ha tenuto conto dei relativi aspetti di sicurezza e delle conseguenti minacce per l'incolumità dell'uomo.

Negli ultimi anni si è assistito ad una sempre maggiore penetrazione delle tecnologie satellitari (ed in particolare di navigazione) in tutti i campi della Geomatica. Questa penetrazione, iniziata già molti anni fa, ha avuto una forte accelerazione grazie alla sempre maggiore disponibilità sul mercato di tecnologie a basso costo ed alte prestazioni. Oggi, l'uso dei sistemi di navigazione satellitare avviene sia per via diretta (ad esempio nel rilevamento topografico) sia per via indiretta (per la georeferenziazione di altri strumenti di misura come i Laser Scanner, o come strumento di navigazione per i velivoli autonomi).
In questo lavoro non ci si concentrerà sulle nuove opportunità aperte dai sistemi satellitari, o sulle loro prestazioni di misura, ma su un aspetto che spesso è trascurato: la gestione della sicurezza durante il loro utilizzo.
E' importante chiarire cosa si intenderà per sicurezza. Si parla di sicurezza ogni qualvolta ci si riferisce alla salvaguardia della vita umana. Sicurezza, però, vuol dire anche capacità di proteggere qualcosa o qualcuno. Nel primo caso si usa il termine inglese *safety,* nel secondo si usa il termine *security*. Questa distinzione diviene molto chiara se si risale all'origine delle due parole: safe viene dal latino Latino "salvum", dalla stessa radice di "salus" che significa 'salute'; secure, viene dal latino securum, 'tranquillo, senza preoccupazioni'. Comunemente si pensa alla security come un mezzo per raggiungere la safety: il *sistema di sicurezza* (security) costituisce una barriera a protezione dell'incolumità personale (safety). Nelle attuali applicazioni tecnologiche questa visione è riduttiva in quanto: (a) non necessariamente un sistema di sicurezza è a protezione della salute dell'uomo (si pensi ad esempio alla cyber-security, alla protezione dei dati sensibili ecc.); (b) la security non è condizione necessaria (ne sufficiente) a garantire l'incolumità dell'uomo (si pensi, ad esempio agli incidenti, ed ai malfunzionamenti).
Nelle seguito, dopo un breve introduzione sull'evoluzione dei sistemi di navigazione satellitare (chiamati genericamente Global Navigation Satellite System - GNSS) e sulle tendenze di utilizzo future, saranno analizzati i relativi rischi di sicurezza ed alcune possibili contromisure.

Evoluzione dei sistemi GNSS

Il primo sistema di navigazione satellitare operativo fu il sistema *Transit*, era utilizzato dalla Marina Statunitense per avere informazioni precise sulla posizione dei suoi sottomarini e dei missili balistici.
Il *Transit* ha fornito un servizio di navigazione continuo fin dal 1964 e, successivamente, è stato reso disponibile anche per uso civile**.**
Durante la guerra fredda, furono sviluppati i due sistemi più noti: il *GPS* (Stati Uniti) ed il *GLONASS* (Unione Sovietica). I due sistemi, con differenti soluzioni tecniche, sfruttano lo stesso principio di funzionamento per fornire la posizione: il ricevitore misura la propria distanza da almeno 4 satelliti (contemporaneamente visibili), ricavando poi la propria posizione come il punto di intersezione di sfere aventi come centro i satelliti e come raggio la distanza misurata. Questo principio è, di fatto, diventato lo standard di riferimento per la navigazione satellitare e, dato l'abbandono per lungo tempo del sistema GLONASS, il GPS è stato l'unico sistema utilizzato in occidente.
Recentemente, la situazione è molto cambiata: oltre alla piena operatività (ritrovata nel 2012) del sistema GLONASS, nuovi sistemi di navigazione satellitare sono diventati operativi ed altri sono pianificati per il futuro. Si possono qui menzionare l'europeo *Galileo*, dichiarato in *"Initial Operational Capability* a dicembre 2016, ed il cinese *Beidou*, che con il lancio del 12 Febbraio 2018 ha raggiunto un totale di 22 satelliti in orbita sui 35 previsti. A questi sistemi di navigazione globale si affiancano i sistemi regionali (dove per regioni si intendono scale nazionali o continentali) di posizionamento autonomo (come il *NAVIC* indiano) o di supporto (per il miglioramento delle prestazioni dei sistemi esistenti,

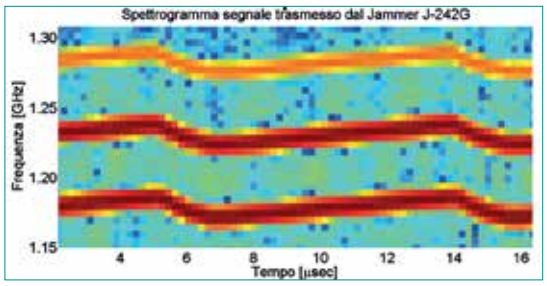

Fig. 2 - Occupazione spettrale del segnale trasmesso da un jammer in grado di disturbare contemporaneamente le bande L2, L4 e L5 del GPS.

come il *WAAS* americano o l'*EGNOS* europeo) e, infine, sistemi locali o terrestri (ad.es. il *GBAS*, le reti *DGPS*, le reti *RTK* ecc.) per i più disparati utilizzi (dall'atterraggio di precisione, al monitoraggio dei movimento tettonici, al rilevamento topografico).
Data questa forte evoluzione, le attuali prestazioni di accuratezza sulla misura di posizione variano dai pochi metro (utilizzando i soli sistemi di navigazione satellitare) fino ai centimetri (o sotto) con l'aiuto dei sistemi di supporto (stazioni differenziali, stazioni RTK, reti RTK ecc.) e lunghi tempi di osservazione. Essendo i sistemi GNSS interoperabili, l'utilizzo contemporaneo di più costellazioni (ricevitori multi-costellazione) ha consentito, infine, anche un aumento della continuità e della disponibilità dei servizi (Galati 2009).
Anche il lato utente (cioè il ricevitore da esso usato) ha subito un evoluzione con la produzione di ricevitori GNSS sempre più performanti ed a basso costo. La grande diffusioni di terminali mobili multimediali (smartphone) con ricevitori GNSS integrati, ha, inoltre, aperto la strada all'uso di questi device anche nelle applicazioni professionali in cui le performance di accuratezza richieste sono elevate. Ulteriore spinta in questa direzione sarà data dalla possibilità di accedere direttamente ai dati di misura GNSS negli smartphone di ultima generazione (da Android N in poi).
La diffusione pervasiva di questi terminali cambia completamente l'approccio nell'uso dei sistemi GNSS per applicazioni professionali. Il paradigma di utilizzo, che prima era basato sull'utilizzo di tecnologie ad-hoc ed ottimizzate per la specifica funzione da svolgere, sarà sempre più basato su soluzioni con hardware distribuito (sempre più apparati comunicanti tra loro) e funzioni concentrate (sempre maggiore sovrapposizione delle funzioni di elaborazione, comunicazione e navigazione).
Questa redistribuzione delle "competenze" produce molti vantaggi (abbattimento dei costi, prestazione di misura elevate, dati sempre disponibili, maggiore semplicità di utilizzo ecc.) ma non bisogna dimenticare che ogni volta che si introducono nuove tecnologie o nuovi servizi se ne devono considerare anche i limiti.
In particolare, oggi, per la stragrande maggioranza delle applicazioni commerciali, i ricevitori GNSS non forniscono nessuna garanzia di servizio agli utenti e, per varie ragioni, le loro prestazioni di accuratezza (seppur normalmente molto elevate rispetto al passato) si possono degradare molto e molto rapidamente (ad esempio per condizioni di propagazione del segnale anomale o per malfunzionamenti nei satelliti). Inoltre, come ogni sistema basato sulle telecomunicazioni wireless, il servizio di localizzazione può essere negate o degradato intenzionalmente utilizzando degli appositi apparati di disturbo: solitamente si parla di *Jamming* come l'atto di disturbare volutamente le comunicazioni radio trasmettendo sulla stessa frequenza del segnale che si vuole disturbare, o di *Spoofing* quando si intende la trasmissione di falsi segnali, del tutto simili a quelli nominali, contenenti informazioni fuorvianti per ingannare il ricevitore d'utente (ad esempio facendogli credere di trovarsi in posto diverso da quello in cui realmente si trova).
A questi limiti, va aggiunta un considerazione generale: è sempre più frequente, nei sistemi complessi, l'uso di metodi automatici o autonomi di decisione (comunemente noti come intelligenza artificiale). Questi metodi introducono un ulteriore strato di mediazione tra le misure GNSS e l'uomo, trasformandolo, di fatto, in una componente (a volte marginale) dell'intero sistema. L'utilizzatore finale, di conseguenza, non ha ne il pieno controllo, ne la piena conoscenza di quanto sta avvenendo.

Sicurezza nelle applicazioni geomatiche

I suddetti limiti influiscono direttamente sulla sicurezza (safety e security), infatti: (a) essendo lo scopo principale dei sistemi di navigazione il governo dei mezzi mobili (dalle automobili, alle persone, dagli aerei ai droni), se mal governati per malfunzionamento del sistema di localizzazione, essi possono arrecare danno all'uomo (incidenti) o ai sui beni (perdite economiche); (b) attraverso l'utilizzo dei GNSS si generano dati come, ad esempio, cartografie o rilievi topografici che, se errati possono essere dannosi; (c) può essere di interesse, per un soggetto terzo, provocare malfunzionamenti o impedire il corretto (o sicuro) svolgimento delle attività in cui è previsto l'uso di apparati GNSS; (d) non è nulla la probabilità di trovarsi in condizioni avverse (ad esempio per presenza di interferenze o malfunzionamenti) che degradano le prestazioni del sistemi in uso; (e) non è nulla la probabilità di essere in presenza di una degradazione intenzionale delle prestazioni non direttamente rivolta al nostro ricevitore ma ad altri nelle vicinanze.
Molti dei casi esposti sono già accaduti in passato e se ne riportano qui alcuni esempi significativi.
Molto diffuso (seppur illegale) è l'utilizzo di apparati di disturbo

Fig. 3 - Esempio di disturbo attraverso spoofer. La traccia blue rappresenta la sequenza di posizioni (errate) calcolate da un ricevitore (in posizione fissa) in presenza di spoofer che invia falsi segnali di navigazione (Jones 2017).

per inibire il funzionamento del sistema di navigazione installato a bordo del proprio veicolo (normalmente per disturbare il sistema di controllo della flotta aziendale o per disturbare il sistema GNSS installato ai fini assicurativi).
Qualche anno fa si è verificato il primo provvedimento sanzionatorio a riguardo: un uomo del New Jersey è stato scoperto ad utilizzare un jammer sul proprio mezzo per impedirne la localizzazione da parte della sua azienda. Passando regolarmente nelle vicinanze dell'aeroporto di Newark ha disturbato i test per l'installazione di un sistema di navigazione nell'aeroporto stesso e, una volta scoperto, è stato licenziato e multato per circa 32.000 dollari dalla Federal Communications Commission.
Cambiando ambito di applicazione, nel 2013, un team di ricercatori statunitensi ha dimostrato che era possibile mandar fuori rotta uno yacht (del valore di 80 milioni di dollari) attraverso semplici dispositivi di spoofing (Jones 2017).
La questione diventa importante quando queste pratiche diventano diffuse: nel luglio 2016 è salito alla ribalta delle cronache il gioco per smartphone *Pokémon Go*. Il gioco utilizza il GNSS del dispositivo mobile per individuare, catturare, combattere e addestrare i Pokémon, creature virtuali, (posizionate nel mondo reale) che appaiono sullo schermo del giocatore solo quando esso si trova nelle loro vicinanze. La difficoltà di trovarsi in luoghi specifici ha fatto nascere nei giocatori la voglia di trovare una soluzione più facile: ingannare il gioco facendogli credere di trovarsi nel posto giusto al momento giusto. Molti utenti hanno, quindi, installato nel proprio device applicazioni in grado di sostituire i dati di localizzazione con dati falsi (auto-spoofing). Pokemon-Go ha cosi contribuito a far conoscere al grande (e giovane) pubblico lo spoofing dei sistemi GNSS.
Ultimo evento significativo: tra il 22 e il 24 giugno 2017, alcune navi nel Mar Nero hanno riportato anomalie nel calcolo della loro posizione, risultando posizionate all'interno di un aeroporto a chilometri di distanza. E' abbastanza probabile che i segnali GPS di quella zona siano stati falsificati da un sistema di difesa anti-drone.
Molti droni commerciali hanno, infatti, regole di *geofencing* che ne impediscono il volo su aeroporti e altre aree ristrette: facendo credere al drone di trovarsi sopra un aeroporto lo si costringe ad eseguire l'immediato atterraggio o il ritorno al punto di lancio (Jones 2017).
Quanto esposto è possibile poiché, come menzionato precedentemente, la stragrande maggioranza dei ricevitori GNSS commerciali nel mondo si basa esclusivamente sui segnali non crittografati ed aperti a tutti. In più, la diffusione delle Software Defined Radio (SDR - Ricetrasmettitori programmabili a basso costo) ha aperto la strada allo "spoofing per tutti". Equipaggiate con software di simulazione GPS (open source!) le SDR posso trasformarsi in ottimi spoofer.
Considerando quanto esposto è chiaro che la sicurezza dovrebbe essere attentamente considerata anche nelle applicazioni di Geomatica, per fare alcuni esempi:

- in caso di uso di droni per ogni tipo di rilevamento: il mancato controllo del drone a causa di un errore di posizione elevato o una negazione del servizio può comportare un danno per l'uomo; l'uso di disturbatori può consentirne la cattura, l'abbattimento o il furto;
- errori di misura (diretti o indiretti) possono vanificare campagne di misura anche lunghe e costose;
- utenti o fruitori non collaborativi possono cercare di impedire i rilievi attraverso la negazione dei servizio di localizzazione (ad esempio nei casi di censimenti, monitoraggio di abusi edilizi etc.);

Fortunatamente molte tecniche di difesa sono già note e l'argomento è continuo oggetto di ricerca da anni in tutto il mondo.
Normalmente possiamo utilizzare almeno tre contromisure per mitigare i rischi di sicurezza legati all'uso di un sistema di navigazione satellitare: l'*integrità*, la *protezione* e la *consapevolezza*.

Integrità
L'integrità è la capacità di fornire opportuni allarmi agli utenti quando il sistema di navigazione non sta funzionando in modo corretto o comunque non sta rispettando le specifiche richieste. E', quindi, la capacità di rilevare degradazioni nella accuratezza oltre una determinata soglia e di segnalarlo entro un tempo definito. In questo modo l'utente, consapevole che il sistema è degradato nelle sue prestazioni, può smettere di utilizzarlo.
Possono essere utilizzate varie tecniche per fornire questo servizio; tutte quante sfruttano la ridondanza delle informazioni (provenienti dal sistema stesso o da sistemi di localizzazione terzi) per scovare il malfunzionamento.
Generalmente si distinguono le seguenti categorie di algoritmi di integrità:

- *AIM (Autonomous Integrity Monitoring)* in cui l'utente confronta più sistemi di navigazione a suo disposizione per rilevare un anomalia nei dati di posizione;
- *RAIM (Receiver Autonomous Integrity Monitoring)* in cui l'utente sfruttando la sovrabbondanza di satelliti di navigazione in visibilità riesce a rilevare la presenza di misure anomale;
- *Monitoring*: i segnali provenienti dai satelliti del sistema di navigazione vengono monitorati da un rete di ricevitori a terra che verificano la loro "congruità" e se necessario lanciano un allarme. Per diffondere l'allarme può essere utilizzato un data-link di tipo terrestre o di tipo satellitare.

Esistono vari esempi di servizi di integrità già operativi (solitamente

per applicazioni aeronautiche) come quelli forniti dai sistemi *WAAS* ed *EGNOS* precedentemente citati. Essi monitorano i segnali GNSS attraverso una rete di sensori a terra e diffondono su scala continentale informazioni di integrità utilizzando i satelliti geostazionari (EGNOS, ad esempio, è in grado di fornire un allarme entro 6 secondi se si verifica una degradazione dell'accuratezza superiore ai 40-50 metri).
Con sistemi di tipo locale si ottengono prestazioni migliori sia per quanto riguarda il tempo di allarme che il livello di protezione (soglia di accuratezza oltre la quale esso scatta). Sempre nel settore aeronautico, sono stati introdotti e si stanno sviluppando i sistemi *GBAS* (Ground Based Augmentation System) pensati per essere installati presso gli aeroporti e consentire alcuni tipi di atterraggi strumentali (tipicamente con tempi di allarme inferiori al secondo e livelli di protezione sotto ai 10 metri).
Infine le tecniche RAIM e AIM sono già ampiamente utilizzate per la navigazione aerea in rotta senza l'ausilio di infrastrutture terrestri (Galati 2009).
Molte altre tecniche sono allo studio, ad es. per sfruttare la presenza di multi-costellazioni (Gargiulo 2010)(Viola 2012), e tutte, così come sono o con alcune modifiche, potrebbero essere introdotte anche nelle applicazioni di geomatica.

Protezione
Seppur la funzione di l'integrità consente di rilevare un malfunzionamento, da sola non è sufficiente. La presenza di un disturbo intenzionale, ad esempio, può, a volte, essere difficile da rivelare e comunque inibirebbe localmente l'uso del sistema. Lo Spoofing, inoltre, generando segnali del tutto analoghi a quelli dei satelliti, potrebbe essere completamente trasparente ai sistemi di integrità.
Il ricevitore di navigazione satellitare deve essere quindi protetto da questi attacchi. Questo problema è noto fin dall'origine dei sistemi di navigazione satellitare ed infatti tutti i sistemi oggi operativi, oltre ai segnali per uso civile (e liberamente fruibile), trasmettono anche segnali ad accesso controllato, tipicamente ad uso militare, che grazie all'impiego di tecniche di crittografiche e di autenticazione sono robusti rispetto ai disturbi. Caso particolare è il sistema Galileo che prevede queste peculiarità anche per gli utenti civili (con il futuro servizio denominato *Safety of Life*) (Galati 2009): sarà pertanto possibile proteggersi selezionando accuratamente il servizio di navigazione più adatto alle esigenze.
Anche nel caso non sia possibile utilizzare i segnali e i servizi appositamente concepiti per essere immuni ai disturbi, sono comunque disponibili delle tecniche di mitigazione. Sono note, e oggetto di ricerca, tecniche in grado di rivelare la presenza di un segnali interferenti e mitigarne gli effetti attraverso introduzione di algoritmi avanzati di Signal Processing direttamente nel ricevitore d'utente o sfruttando antenne adattative (Lo presti 2006)(Di Fonzo 2014).

Consapevolezza
Può sembrar banale, ma il primo passo per gestire un rischio è sempre la consapevolezza della sua esistenza e delle sue potenzialità. Introdurre la cultura della sicurezza nell'uso di apparati di navigazione satellitare anche in settori applicativi in cui non si ci si occupa direttamente del trasporto delle persone è un passo fondamentale. Fortunatamente la cultura della sicurezza è già ben presente in vasti settori della geomatica (si pensi alle norme di sicurezza nei cantieri); essa dovrebbe essere estesa anche ai nuovi strumenti basati sui GNSS. Conoscere i limiti dei propri strumenti (seppur considerati solo apparati di misura) consente già una mitigazione del rischio.
Fondamentale è, quindi, incrementare le competenze di navigazione satellitare degli operatori del settore attraverso una formazione permanente. Sarà necessario, infine, sviluppare nuovi modelli e piani di sicurezza che tengano presente le specificità di questi sistemi tecnologici.

Conclusioni
In conclusione, seppur oggi la cultura e la gestione della sicurezza dei sistemi di navigazione satellitare non è al primo posto nei pensieri del professionista, lo potrà diventerà ben presto, così come già dimostrato in altri settori delle telecomunicazioni (si pensi ad esempio alla cyber security nelle reti di telecomunicazioni). Bisognerà, allora, farsi trovare pronti avendo ben presente i limiti dei sistemi GNSS, conoscendo le possibilità messe a disposizione dagli odierni (e futuri) sistemi di navigazione e, quando necessario, sviluppando nuove tecniche di integrità e protezione.

ABSTRACT
G. Galati, M. Leonardi (2009) SISTEMI DI RILEVAMENTO E NAVIGAZIONE, TexMat Libreria Universitaria
M. Jones (2017) Spoofing in the Black Sea: What really happened? gpsworld.com, http://gpsworld.com/spoofing-in-the-black-sea-what-really-happened/
G. Gargiulo, M. Leonardi,M. Zanzi, G. Varacalli (2010) Integrity and protection level computation for vehicular applications Proceedings of 16th Ka and broadband communications navigation and earth observation conference, Pages:2968 – 2977
S. Viola, M. Mascolo, P. Madonna, L. Sfarzo, M. Leonardi (2012) Design and Implementation of a Single-Frequency L1 Multiconstellation GPS/EGNOS/GLONASS SDR Receiver with NIORAIM FDE Integrity, Proceedings of the 25th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2012)
L. Lo Presti, B. Motella, M. Leonardi (2006) A Technique of Interference Monitoring in GNSS Applications, Based on ACF and Prony Methods, Proceedings of the 19th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2006)
A. Di Fonzo, M. Leonardi; G. Galati, P. Madonna, L. Sfarzo (2014) Software-Defined-Radio techniques against jammers for in car GNSS navigation, IEEE International Workshop on Metrology for Aerospace 2014

PAROLE CHIAVE
GNSS; SICUREZZA; GEOMATICA

ABSTRACT
Satellite navigation systems are more and more used in geomatics. This penetration has not always taken into account the relative safety and security aspects and the consequent threats to the humans. This work focuses on these aspects that are often overlooked in geomatics. After a brief introduction on the evolution of satellite navigation systems and on future trends, the related safety and security risks are analyzed and possible countermeasures (Integrity, Awareness, and Protection) are discussed.

AUTORE
MAURO LEONARDI
MAURO.LEONARDI@UNIROMA2.IT
DIPARTIMENTO DI INGEGNERIA ELETTRONICA
UNIVERSITÀ DI ROMA TOR VERGATA.