PROGETTO “CRONOS”

Titolo

Progetto di ricerca tecnologica per lo sviluppo e la realizzazione di un sistema per la rilevazione dell’alterazione dei segnali GPS generata da azioni di spoofing.
Denominazione progetto “CRONOS” p/n: SPT- 0125” (CybeR-attack Outfight with Neural Operation System)

Campo di attività

Difesa elettronica dei siti e dei sistemi mobili di F.A. per contrasto “electronic warfare”.
- Tecnologie di rilevazione radiofrequenza per contromisura disturbo e neutralizzazione minaccia rilevata.
- Tecnologie di rilevazione elettronica per identificazione cyber-attacco.
- Contromisure Elettroniche per protezione dati di posizione, navigazione e timing (cyber security).

Azienda responsabile

MPM Telecommunication srl. di Civitavecchia con cooperazione
della Università “Sapienza” di Roma, Dipartimento di Ingegneria Informatica e Fondazione Anna Maria Catalano

VALIDITA’ TECNICO OPERATIVA DEL PROGETTO

Fino ad oggi, la maggiore preoccupazione per i sistemi basati su NAVSTAR GPS è un cyberattacco basato sul jamming, ovvero sovrapponendo i segnali satellitari tramite rumore e quindi annullando il rilevamento della posizione. Questo tipo di cyber-attacco, includibile nelle tecniche di “electronic warfare”, anche se può causare problemi, è abbastanza semplice da individuare. Un’insidia maggiore deriva da un attacco spoofing: falsi segnali satellitari trasmessi da stazioni di terra in grado di confondere i ricevitori e gli apparati connessi. Data la notevole evoluzione tecnologica degli ultimi anni e, conseguentemente la condivisione delle informazioni e delle conoscenze, i sistemi in grado di produrre questo tipo di cyber-attacco sono diventati di facile reperibilità con costi accessibili.
D’altro canto, l’incremento dell’utilizzo di apparati satellitari e Wi-Fi ha comportato, quasi automaticamente, un aumento del numero di hacker che si sono dedicati ad attaccare questi sistemi; gli attacchi condotti contro le moderne autovetture, dotate di reti senza fili a bordo, ne sono una prova.
Gli studi su questa possibilità di attacco hanno avuto avvio quando un drone americano è stato catturato, inducendolo ad atterrare in una zona controllata dai nemici. Dopo tale evento il Dipartimento della Sicurezza Nazionale degli Stati Uniti ha analizzato la possibilità di realizzare un trasmettitore di segnali GPS, che sono indistinguibili da quelli reali. Durante un esperimento condotto nel poligono militare di White Sands, nel Nuovo Messico, si riuscì ad ingannare un drone, facendo credere agli apparati di bordo che esso stava salendo in quota, mentre invece stava scendendo; il drone fu salvato l’ultimo istante, prima di precipitare nella sabbia del deserto, da un pilota che, disabilitando i controlli automatici, ne ha assunto il comando manuale.
Una possibile sperimentazione di questo tipo di attacco, che fino a pochi anni fa sembrava molto remoto, sembra essere stata già effettuato il 22 giugno 2017 alle 7:10 GMT nei pressi del Mar Nero. La US Maritime Administration ha pubblicato una “safety alert” per una possibile “interferenza GPS”.
In realtà i capitani di oltre 20 navi commerciali al largo del porto russo di Novorossiysk hanno notato che gli strumenti GPS rilevavano come posizione l’aeroporto di Gelendzhik, ad oltre 32 Km nell’entroterra. I ricercatori dell’università di Austin, Texas, suppongono sia stato un

test russo per provare un nuovo disturbatore.
L'alterazione del segnale GPS, e la conseguente errata rilevazione, ha effetti negativi su un'ampia varietà di applicazioni che fanno del GPS un apparato fondamentale per il proprio funzionamento; basti pensare, ad esempio, ai sistemi di movimentazione automatica di veicoli o velivoli, dove il GPS tiene conto della propria posizione per decidere il percorso o la rotta. Altro possibile malfunzionamento si potrebbe trovare in tutti quegli apparati che usano il ricevitore GPS per effettuare sincronie o usano la stringa NMEA per costruire chiavi di crittografia condivise (entrambe utilizzate nei sistemi di comunicazione ECCM).
Una possibile tecnica di protezione è basata sulla individuazione della direzione da cui arrivano i segnali dei satelliti: se la antenna che riceve i satelliti è di tipo direzionale, è possibile rendersi conto che il segnale in arrivo non proviene dalla posizione calcolata dei satelliti, ma questo tipo di elaborazione informatica richiede ore di calcolo e potenti disponibilità elettroniche; tale elevato tempo di analisi annulla i benefici del rilevamento della minaccia.
Un'altra possibile contromisura è basata sulla individuazione di un segnale distorto, ovvero, quando il segnale rilevato è diverso da quello ricevuto dalla costellazione satellitare, è possibile rivelare delle brevi anomalie che potrebbero indicare un tentativo di attacco. Per individuare questa distorsione temporanea bisogna utilizzare i segnali provenienti dai vari canali satellitari al fine di individuare queste brevi distorsioni.
Da tali presupposti scaturisce la necessità di sviluppare un vero e proprio sistema di difesa "intelligente" che si basi sull'uso di diversi ricevitori per l'acquisizione del segnale GNSS, tra cui i ricevitori satellitari per le differenti costellazioni (NAVSTAR GPS, Galileo, Glonass) e ricevitori radio (IEN e DCF-77).
In una condizione di uso normale e ottimale, tali ricevitori collimano tutti fra di loro e i segnali ricevuti sono coerenti.
Per contrastare attacchi jamming o spoofing ed estendere l'uso del sistema a siti non presidiati da personale, si intende studiare ed implementare, nell'apparato di rilevamento GPS prodotto da MPM, un sistema basato su reti neurali, per la scelta automatica della migliore sorgente tra quelle disponibili, scartando le non affidabili.
L'uso delle reti neurali nei problemi di classificazione e clusterizzazione è particolarmente indicato grazie alle capacità di generalizzazione dei sistemi di calcolo basato su questo tipo di architettura: la logica fuzzy permette di rappresentare e trattare concetti in forma qualitativa garantendo elevata robustezza in termini di reiezione di errori.
La rete neurale da sviluppare non solo risolverebbe i problemi legati alla specifica configurazione iniziale del sistema, dipendente dal luogo di installazione e allo scenario operativo, ma si adatterebbe in automatico agli attacchi elettronici e cibernetici, identificando le adeguate contromisure nel minor tempo possibile nel caso che questi cyber-attacchi si riproponessero, anche in modalità simili.

ESIGENZE TECNOLOGICHE DA SODDISFARE

L'esigenza tecnologica è quella di sviluppare le componenti hardware e software per soddisfare i seguenti requisiti tecnici:

- Rilevamento e comparazione dei segnali di posizionamento e timing rilevati da varie sorgenti;
- Comparazione dei segnali tramite rete neurale al fine di rilevare anomalie;
- Catalogazione e analisi della minaccia per successiva identificazione di attacchi simili;
- Distribuzione locale del segnale GPS e Timing esente da anomalie.

TEMA DELLO STUDIO

L'obiettivo del presente studio è la progettazione e realizzazione di un sistema complesso che risponda alle necessità di rilevamento, monitoraggio e neutralizzazione degli effetti di

attacchi elettronici jamming e spoofing su rilevatori GPS.
Data l'esperienza di MPM nel trattamento e nell'analisi delle informazioni satellitari, si prevede, come oggetto di studio, 3 tipi di attacchi elettronici ai dati satellitari. Questi attacchi di spoofing si possono identificare come:

1. Alterazione dei dati di posizione, forse la tipologia più nota, che impatta sui mezzi che usano i dati satellitari per tracciare rotte o identificare punti geografici;
2. Alterazione dei dati temporali, che interessa soprattutto gli apparati che usano un marcatore temporale per algoritmi di crittografia, per chiavi di accesso o per autenticazione di documenti;
3. Alterazione del PPS, ovvero del clock, che riguarda quegli apparati che usano il segnale GPS per sincronizzare i propri oscillatori interni.

La presa di coscienza per questo nuovo cyber-attacco è relativamente attuale, quindi in commercio non esistono dei prodotti COTS per la neutralizzazione della minaccia.
Lo studio che si intende portare avanti partirà dall'analisi dei limiti e delle vulnerabilità del protocollo che trasporta le informazioni GPS; in un secondo momento si analizzeranno anche le vulnerabilità e i limiti dei rilevatori GPS in commercio di più comune uso.
Si studieranno inoltre le sorgenti satellitari da cui si attingeranno le informazioni da analizzare (NAVSTAR, Galileo, Glonass, ecc.); si considererà anche la possibilità di affiancare, per la validazione dei dati rilevati, alcune sorgenti terrestri di diffusione temporale in aria (DCF-77, IEN).
Si passerà a studiare e sviluppare un modello di rete neurale adatta allo scopo, scegliendola tra la famiglia dei classificatori e usando una logica per rappresentare e trattare le informazioni in forma qualitativa (Fuzzy Logic). Tale rete, sia all'istate zero di accensione, sia in un processo di apprendimento successivo, si baserà sulle informazioni provenienti dalle sorgenti ed immagazzinate sull'apparato.
Altro punto su cui indagare è la possibilità, avendo già a disposizione una serie di campioni di dati GPS, effettuare una previsione del probabile dato futuro: questa informazione potrebbe essere inserita tra i dati in ingresso della rete logica in modo da avere un dato discriminante aggiuntivo.
La rete neurale avrà in ingresso tutti i dati provenienti dalle sorgenti disponibili e in uscita il dato GPS stimato come corretto. All'interno della stessa rete il processo decisionale prenderà provvedimenti appropriati a seconda della tipologia di minaccia rilevata. Per esempio, nel caso di rilevamento di alterazione dei dati temporali, il confronto coinvolgerà, oltre i dati satellitari, anche i dati provenienti dalle sincronizzazioni in aria.
Ultimo punto da verificare è l'analisi degli scostamenti naturali accettabili, non inducibili ad una tipologia di attacco, ovvero l'errore di posizionamento intrinseco all'interno del protocollo GPS, i ritardi di trasmissione dovuti alla propagazione della trasmissione del dato in aria, lo scostamento del PPS dovuto ad esempio a due ricevitori satellitari diversi. Questi scostamenti, pur con tutte le tecniche utilizzate per minimizzare gli stessi, come ad esempio l'uso di più satelliti per affinare la localizzazione, sono da tenere in conto al fine di evitare che la rete neurale possa essere affetta da "falsi positivi" ovvero combinazioni di dati coerenti e validi, interpretati però come non validi.

WP DEL PROGETTO

1 Analisi vulnerabilità

2 Identificazione tipologia di attacchi

3 Analisi scostamenti su un ambiente reale

4 Studio Rete Neurale

5 Validazione

6 Integrazione e realizzazione prototipica

7 Verifica Operativa

RISULTATI ATTESI
Si intende non finalizzare lo studio alla semplice raccolta dati e consigli costruttivi, ma si vuole raggiungere l'obiettivo di realizzare un sistema prototipale funzionante che soddisfi tutti i requisiti trattati nel capitolo precedente e sia possibilmente conveniente economicamente e di dispiegamento sul territorio.

PROFILO FINANZIARIO

Totale Costo: K€ 544,00

1. DURATA DEL PROGETTO

Mesi 20.