Detection and Localization of Attacks on Satellite-Based Navigation Systems

Kai Jansen

Kurzfassung

Die weltweite Abdeckung durch satellitengestützte Navigationssysteme, wie beispielsweise das GPS, ermöglicht die Lokalisierung und zeitliche Synchronisation. Orts- und Zeitbewusstsein sind wesentliche Bestandteile vieler Anwendungsbereiche, einschließlich Katastrophenschutz, autonomes Fahren und Luftfahrt. Die starke Abhängigkeit von GPS macht solche Anwendungen anfällig für Signalausfälle oder für eine vorsätzliche Manipulation. Letzteres beinhaltet sogenannte Spoofing-Angriffe, eine mächtige Angriffsklasse gegen GPS-abhängige Systeme, gegen die man sich nur schwer schützen kann. Darüber hinaus werden die für Angreifer verfügbaren Werkzeuge immer erschwinglicher und bieten mehr Funktionalität. Als Konsequenz sehen wir eine Diskrepanz zwischen den vorhandenen Schutzmaßnahmen kritischer Systeme und der Durchführbarkeit von Angriffen.

Um diese Diskrepanz zu überwinden, stellen wir Gegenmaßnahmen vor, um GPS-abhängige Systeme gegen Spoofing-Angriffe besser abzusichern. Dabei sind die strengen Anforderungen der relevanten Anwendungsbereiche, insbesondere der Luftfahrt, zu beachten, um längere (Re-)Zertifizierungsprozesse zu verhindern. Wir erfüllen die gegebenen Anforderungen, indem wir unsere Gegenmaßnahmen auf eine Realisierbarkeit mit kommerzieller Hardware oder der bereits vorhandenen Infrastruktur beschränken. Wir entwickeln beispielsweise effektive Gegenmaßnahmen zur Erkennung von Spoofing Angriffen. Darüber hinaus gehen wir auf das Problem der Spoofer Lokalisierung ein und stellen *Crowd-GPS-Sec* als ein System zur Eingrenzung möglicher Angreiferpositionen durch ADS-B vor. Weiterhin entwerfen wir ein Verifikationsschema basierend auf „Wireless Witnessing“, um die Glaubwürdigkeit von ADS-B Flugzeugnachrichten zu verifizieren.

Zusammenfassend evaluieren und implementieren wir unterschiedliche Sicherheitslösungen zur Detektion und Lokalisierung von Angriffen auf satellitengestützte Navigationssysteme. Wir analysieren die theoretische Realisierbarkeit unserer Ansätze und entwickeln Prototypen, die deren Wirksamkeit demonstrieren. Die von uns vorgestellten Lösungsansätze können zeitnah implementiert werden, um die Sicherheit von GPS-abhängigen Systemen zu verbessern.