

Simulerade ADS-B OCH CPDLC ATTACKER

Experiment i testmiljö med hjälp av mjukvarubaserad radio

Bakgrund

- ✓ Controller-Pilot Link Communications (CPDLC) används för text-kommunikation mellan flygplan och flygplanstorn.
- ✓ Automatic Dependent Surveillance-Broadcast (ADS-B) används för att bestämma flygplanets position.
- ✓ Säkerhet inom flygkommunikation, med dessa tekniker är just nu bristfällig.
- ✓ Okrypterade meddelanden skickas just nu i luftrummet.
- ✓ Detta gör tekniken sårbar.
- ✓ Experiment har visat att obehöriga kan skicka meddelanden med båda teknikerna med hjälp av billig radioutrustning.



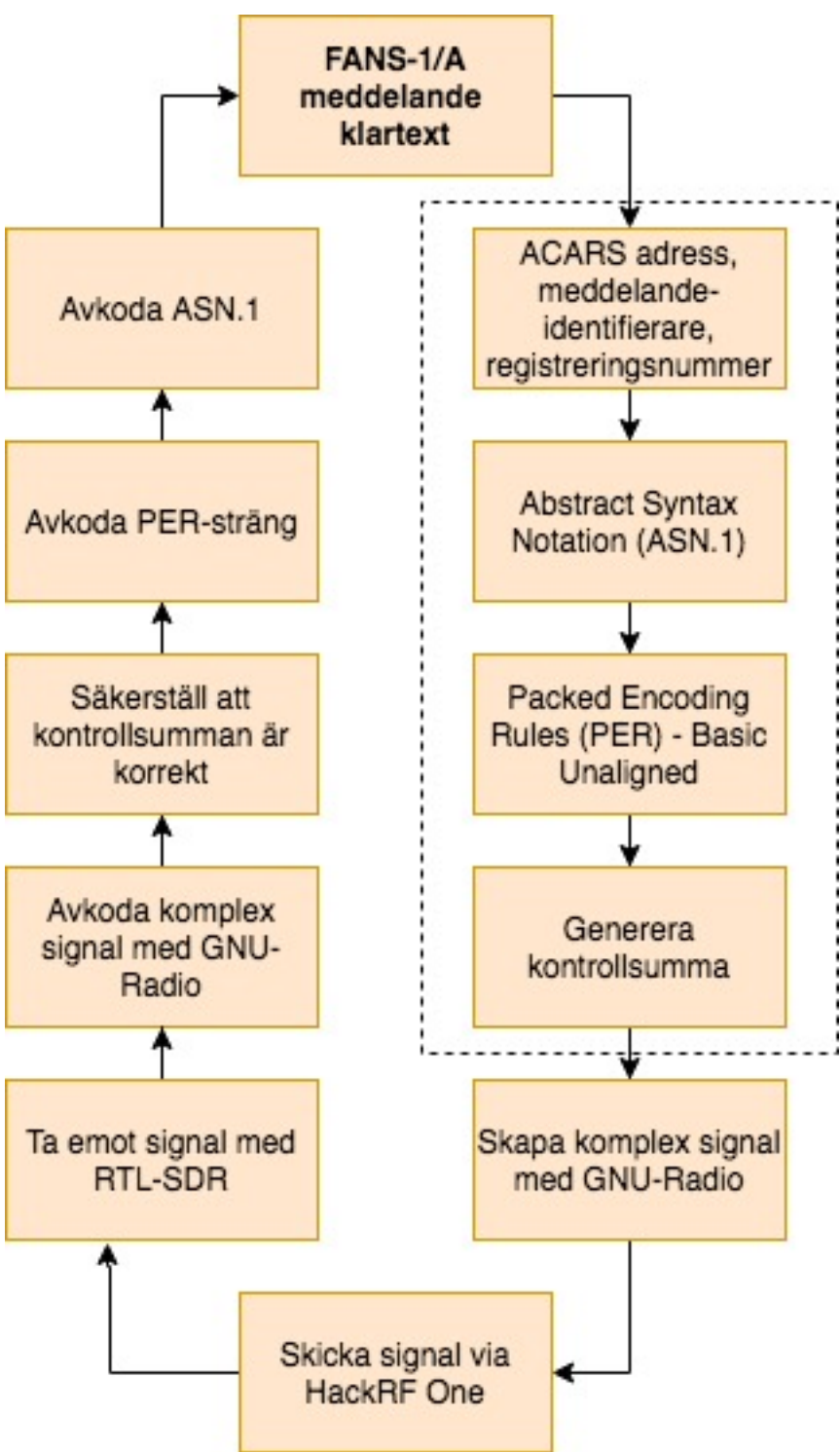
Figur 1: Utrustning

Kodning och avkodning

- ✓ ADS-B och CPDLC skickar kodade meddelanden.
- ✓ Meddelandena avkodas när de tas emot och mottagaren kontrollerar att meddelandet inte är korrupt.
- ✓ Öppen källkod användes för att koda och avkoda ADS-B meddelandet, vilket gör tekniken lätt att injicera för obehöriga.
- ✓ Finns inte tillgängligt för CPDLC-meddelanden.
- ✓ Vi har skapat en metod för att koda ett CPDLC-meddelande med formatet; Future Air Navigation System (FANS-1/A).
- ✓ Vad vi vet är vi de första som avkodat CPDLC-meddelanden.

Resultat

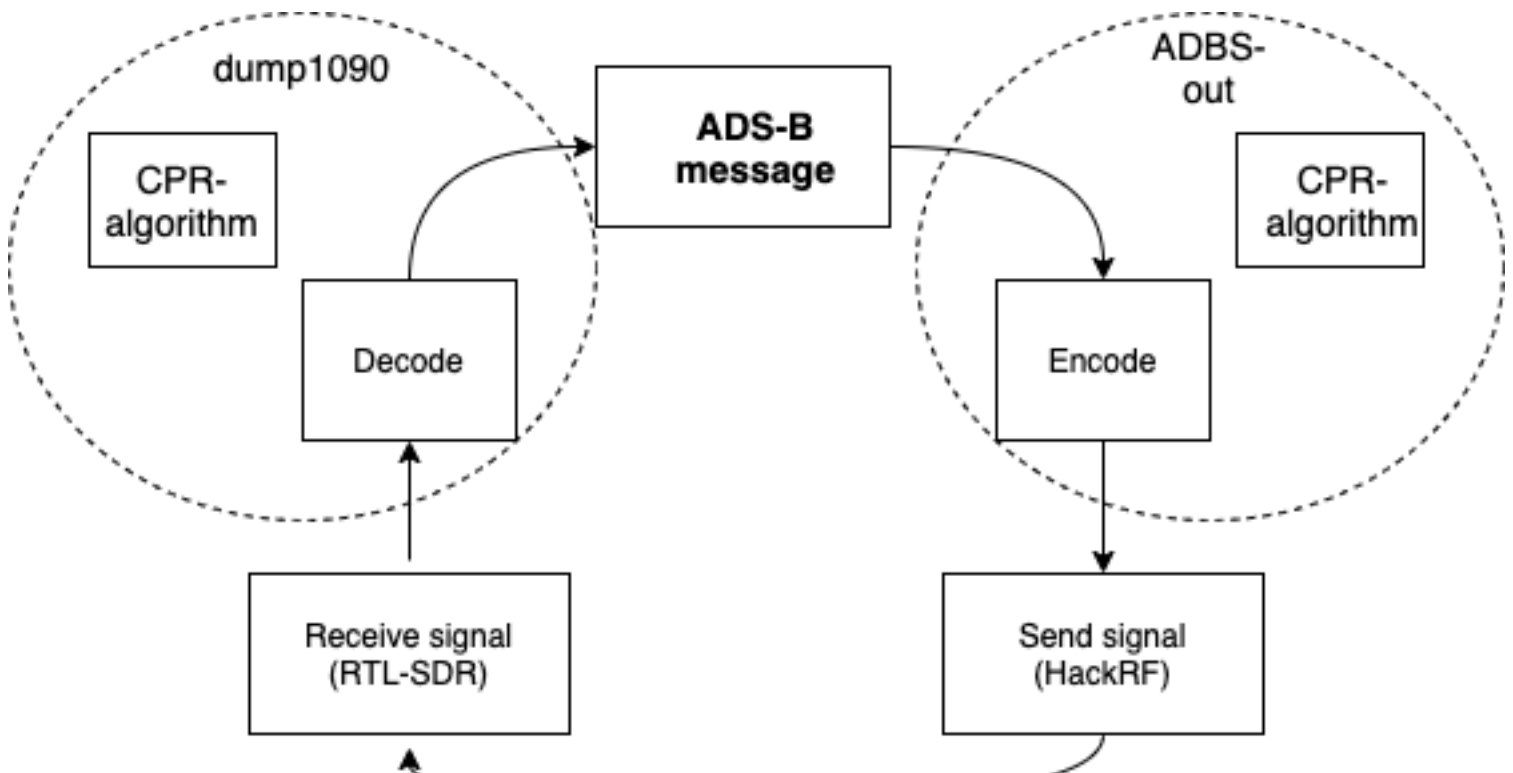
- ✓ Fullständig metod skapades för att koda och avkoda ett ADS-B samt FANS-1/A meddelande.
- ✓ Både ADS-B och FANS-1/A meddelande kunde skickas över licensfria frekvenser med hjälp av hårdvaran HackRF One.
- ✓ De kodade meddelandena togs sedan emot av dongeln RTL-SDR som användes för att illustrera ett mottagande/avlyssnande flygplan.
- ✓ Uppmätt avstånd för ADS-B: 50 m
- ✓ Uppmätt avstånd för FANS-1/A: 1 m



Figur 2: Metod FANS-1/A

Framtida arbete

I framtiden kan L-Band Digital Avionics and Communication System (LDACS) åtgärda säkerhetsproblemen. För att uppnå sekretess, integritet, tillgänglighet och autenticitet rekommenderas algoritmen AES-256 i Galois Counter Mode (GCM) för implementering i LDACS.



CONTACT:

ASDFADFSDF

