Spoof proof GPS timing

A detection and mitigation system for GPS time spoofing

A. Schultzen[1]

[1]Institutt for informatikk
Universitetet i Oslo

8. desember 2016

Introduksjon
GPS timing
Anvendelse
Utfordringer og trusler
Referansetrusselen
Deteksjon og mottiltak
Flere GPS mottakere
Referanseklokke
Implementasjon
Ønsket funksjonalitet
Sensor server arkitektur
Klokkemodell
Filtre
Test av lokasjon- og hastighetsfilter
Beskrivelse
Test av klokkemodell og filtre
Observasjon
Observasjon: Utilsiktet
Konklusjon
Etter innlevering
Bibliografi

Laget et rammeverk for å teste forskjellige spoofing deteksjonsalgoritmer. Ikke gjort før.

Introduksjon
GPS timing
Anvendelse
Utfordringer og trusler
Referansetrusselen
Deteksjon og mottiltak
Flere GPS mottakere
Referanseklokke
Implementasjon
Ønsket funksjonalitet
Sensor server arkitektur
Klokkemodell
Filtre
Test av lokasjon- og hastighetsfilter
Beskrivelse
Test av klokkemodell og filtre
Observasjon
Observasjon: Utilsiktet
Konklusjon
Etter innlevering
Bibliografi

GPS timing

Figur: Trilaterasjon

Introduksjon
GPS timing
Anvendelse
Utfordringer og trusler
Referansetrusselen
Deteksjon og mottiltak
Flere GPS mottakere
Referanseklokke
Implementasjon
Ønsket funksjonalitet
Sensor server arkitektur
Klokkemodell
Filtre
Test av lokasjon- og hastighetsfilter
Beskrivelse
Test av klokkemodell og filtre
Observasjon
Observasjon: Utilsiktet
Konklusjon
Etter innlevering
Bibliografi

GPS timing

Figur: Mobilmast [1]

Figur: PMU [2]

Figur: Wall Street [3]

Introduksjon
GPS timing
Anvendelse
Utfordringer og trusler
Referansetrusselen
Deteksjon og mottiltak
Flere GPS mottakere
Referanseklokke
Implementasjon
Ønsket funksjonalitet
Sensor server arkitektur
Klokkemodell
Filtre
Test av lokasjon- og hastighetsfilter
Beskrivelse
Test av klokkemodell og filtre
Observasjon
Observasjon: Utilsiktet
Konklusjon
Etter innlevering
Bibliografi

Utfordringer og trusler

LORENZO FRANCESCHI-BICCHIERAI SECURITY 07.19.12 5:32 PM

GPS HIJACKING CATCHES FEDS, DRONE MAKERS OFF GUARD

Iran–U.S. RQ-170 incident

From Wikipedia, the free encyclopedia

an Lockheed Martin RQ-170 Sentinel unmanned aerial
UAV was brought down by its cyberwarfare unit which c

SPOOFING GPS AND GETTING YOUR OWN UAV

July 1, 2012 by Brian Benchoff 89 Comments

US spy drone hijacked with GPS spoof hack, report says

ctronic warfare comes of age – in Iran

SEPTEMBER 3, 2015

SPOOFING GPS LOCATIONS WITH LOW COST TX SDRS

At this years Defcon 2015 conference researcher Lin Huang from Qihoo 360 presented her work on spo

Getting lost near the Kremlin? Russia could be 'GPS spoofing'

by Clare Sebastian @clarecnn

December 2, 2016: 4:34 AM ET

Introduksjon
GPS timing
Anvendelse
Utfordringer og trusler
Referansetrusselen
Deteksjon og mottiltak
Flere GPS mottakere
Referanseklokke
Implementasjon
Ønsket funksjonalitet
Sensor server arkitektur
Klokkemodell
Filtre
Test av lokasjon- og hastighetsfilter
Beskrivelse
Test av klokkemodell og filtre
Observasjon
Observasjon: Utilsiktet
Konklusjon
Etter innlevering
Bibliografi

Utfordringer og trusler

Introduksjon
GPS timing
Anvendelse
Utfordringer og trusler
Referansetrusselen
Deteksjon og mottiltak
Flere GPS mottakere
Referanseklokke
Implementasjon
Ønsket funksjonalitet
Sensor server arkitektur
Klokkemodell
Filtre
Test av lokasjon- og hastighetsfilter
Beskrivelse
Test av klokkemodell og filtre
Observasjon
Observasjon: Utilsiktet
Konklusjon
Etter innlevering
Bibliografi

The Civil GPS Spoofer"

Figur: Civil GPS Spoofer [4]

Introduksjon
GPS timing
Anvendelse
Utfordringer og trusler
Referansetrusselen
Deteksjon og mottiltak
Flere GPS mottakere
Referanseklokke
Implementasjon
Ønsket funksjonalitet
Sensor server arkitektur
Klokkemodell
Filtre
Test av lokasjon- og hastighetsfilter
Beskrivelse
Test av klokkemodell og filtre
Observasjon
Observasjon: Utilsiktet
Konklusjon
Etter innlevering
Bibliografi

Deteksjon og mottiltak

- Bruke flere GPS mottakere med kjent posisjon og hastighet.
- Gode klokker – Små korreksjoner.

Introduksjon
GPS timing
Anvendelse
Utfordringer og trusler
Referansetrusselen
Deteksjon og mottiltak
Flere GPS mottakere
Referanseklokke
Implementasjon
Ønsket funksjonalitet
Sensor server arkitektur
Klokkemodell
Filtre
Test av lokasjon- og hastighetsfilter
Beskrivelse
Test av klokkemodell og filtre
Observasjon
Observasjon: Utilsiktet
Konklusjon
Etter innlevering
Bibliografi

Flere GPS mottakere og kjent posisjon

Figur: Spoofing deteksjon med to antenner

Introduksjon
GPS timing
Anvendelse
Utfordringer og trusler
Referansetrusselen
Deteksjon og mottiltak
Flere GPS mottakere
Referanseklokke
Implementasjon
Ønsket funksjonalitet
Sensor server arkitektur
Klokkemodell
Filtre
Test av lokasjon- og hastighetsfilter
Beskrivelse
Test av klokkemodell og filtre
Observasjon
Observasjon: Utilsiktet
Konklusjon
Etter innlevering
Bibliografi

Flere GPS mottakere og kjent posisjon

Figur: Spoofing deteksjon med to antenner

Introduksjon
GPS timing
Anvendelse
Utfordringer og trusler
Referansetrusselen
Deteksjon og mottiltak
Flere GPS mottakere
Referanseklokke
Implementasjon
Ønsket funksjonalitet
Sensor server arkitektur
Klokkemodell
Filtre
Test av lokasjon- og hastighetsfilter
Beskrivelse
Test av klokkemodell og filtre
Observasjon
Observasjon: Utilsiktet
Konklusjon
Etter innlevering
Bibliografi

Referanseklokke

- Trenger får korreksjoner
- Lite påvirket av temperatur
- Intern frekvensteller og styringsalgoritme

Figur: Symmetricom SA.45s CSAC

Introduksjon
GPS timing
Anvendelse
Utfordringer og trusler
Referansetrusselen
Deteksjon og mottiltak
Flere GPS mottakere
Referanseklokke
Implementasjon
Ønsket funksjonalitet
Sensor server arkitektur
Klokkemodell
Filtre
Test av lokasjon- og hastighetsfilter
Beskrivelse
Test av klokkemodell og filtre
Observasjon
Observasjon: Utilsiktet
Konklusjon
Etter innlevering
Bibliografi

Referanseklokke

Telemetri (RS-232)

```
0,0x0000,1110CS01616,0x0010,3289,0.96,1.497,13.46,0.995,25.96,5,---,0,2,519,467,1.03
```

Figur: CSAC blokkdiagram

Introduksjon
GPS timing
Anvendelse
Utfordringer og trusler
Referansetrusselen
Deteksjon og mottiltak
Flere GPS mottakere
Referanseklokke
Implementasjon
Ønsket funksjonalitet
Sensor server arkitektur
Klokkemodell
Filtre
Test av lokasjon- og hastighetsfilter
Beskrivelse
Test av klokkemodell og filtre
Observasjon
Observasjon: Utilsiktet
Konklusjon
Etter innlevering
Bibliografi

Ønsket funksjonalitet

- Detektere angrep:
  - GPS
  - Klokke
- Logging
- Enkel utbygging
- Administreres over nettverk
- Konfigurerbar

Introduksjon
GPS timing
Anvendelse
Utfordringer og trusler
Referansetrusselen
Deteksjon og mottiltak
Flere GPS mottakere
Referanseklokke
Implementasjon
Ønsket funksjonalitet
Sensor server arkitektur
Klokkemodell
Filtre
Test av lokasjon- og hastighetsfilter
Beskrivelse
Test av klokkemodell og filtre
Observasjon
Observasjon: Utilsiktet
Konklusjon
Etter innlevering
Bibliografi

Sensor server arkitektur ide

+

=

(Sensor)

Introduksjon
GPS timing
Anvendelse
Utfordringer og trusler
Referansetrusselen
Deteksjon og mottiltak
Flere GPS mottakere
Referanseklokke
Implementasjon
Ønsket funksjonalitet
Sensor server arkitektur
Klokkemodell
Filtre
Test av lokasjon- og hastighetsfilter
Beskrivelse
Test av klokkemodell og filtre
Observasjon
Observasjon: Utilsiktet
Konklusjon
Etter innlevering
Bibliografi

Kommunikasjon: roller

Introduksjon
GPS timing
Anvendelse
Utfordringer og trusler
Referansetrusselen
Deteksjon og mottiltak
Flere GPS mottakere
Referanseklokke
Implementasjon
Ønsket funksjonalitet
Sensor server arkitektur
Klokkemodell
Filtre
Test av lokasjon- og hastighetsfilter
Beskrivelse
Test av klokkemodell og filtre
Observasjon
Observasjon: Utilsiktet
Konklusjon
Etter innlevering
Bibliografi

Kommunikasjon: GPS data

Introduksjon
GPS timing
Anvendelse
Utfordringer og trusler
Referansetrusselen
Deteksjon og mottiltak
Flere GPS mottakere
Referanseklokke
Implementasjon
Ønsket funksjonalitet
Sensor server arkitektur
Klokkemodell
Filtre
Test av lokasjon- og hastighetsfilter
Beskrivelse
Test av klokkemodell og filtre
Observasjon
Observasjon: Utilsiktet
Konklusjon
Etter innlevering
Bibliografi

Sensor server arkitektur

- 3000+ linjer med C99 kode
- Håndterer av/pålogging av klienter
- Håndtere mottak og formatering av GPS data
- En prosess per pålogging
- Delt minne mellom prosesser (anonym MMAP)
  - Semaforer og barrierer for beskyttelse
- Mulighet for brukere å koble på og gi kommandoer, f.eks:
  - Rapporterer lokasjon og tid
  - Rapportere server status
  - Rapportere filterstatus
  - Lagre og gjenopprette tilstand i sensorer
  - Laste inn nye lokasjonsdata
  - Avslutte egen og andres tilkobling
  - Sende kommandoer til atomklokka

Introduksjon
GPS timing
Anvendelse
Utfordringer og trusler
Referansetrusselen
Deteksjon og mottiltak
Flere GPS mottakere
Referanseklokke
Implementasjon
Ønsket funksjonalitet
Sensor server arkitektur
Klokkemodell
Filtre
Test av lokasjon- og hastighetsfilter
Beskrivelse
Test av klokkemodell og filtre
Observasjon
Observasjon: Utilsiktet
Konklusjon
Etter innlevering
Bibliografi

Klokkemodell

- Utviklet av Harald Hauglin
- Bruker klokkedata (telemetri)

Figur: CSAC styringskorreksjon, fra klokke og predikert.

Introduksjon
GPS timing
Anvendelse
Utfordringer og trusler
Referansetrusselen
Deteksjon og mottiltak
Flere GPS mottakere
Referanseklokke
Implementasjon
Ønsket funksjonalitet
Sensor server arkitektur
Klokkemodell
Filtre
Test av lokasjon- og hastighetsfilter
Beskrivelse
Test av klokkemodell og filtre
Observasjon
Observasjon: Utilsiktet
Konklusjon
Etter innlevering
Bibliografi

Filtre

- Lokasjon og hastighet
- Fasehopp
- Frekvenskorreksjon

Introduksjon
GPS timing
Anvendelse
Utfordringer og trusler
Referansetrusselen
Deteksjon og mottiltak
Flere GPS mottakere
Referanseklokke
Implementasjon
Ønsket funksjonalitet
Sensor server arkitektur
Klokkemodell
Filtre
Test av lokasjon- og hastighetsfilter
Beskrivelse
Test av klokkemodell og filtre
Observasjon
Observasjon: Utilsiktet
Konklusjon
Etter innlevering
Bibliografi

Oppsett

Figur: Oppsett av server og klienter under test

Introduksjon
GPS timing
Anvendelse
Utfordringer og trusler
Referansetrusselen
Deteksjon og mottiltak
Flere GPS mottakere
Referanseklokke
Implementasjon
Ønsket funksjonalitet
Sensor server arkitektur
Klokkemodell
Filtre
Test av lokasjon- og hastighetsfilter
Beskrivelse
Test av klokkemodell og filtre
Observasjon
Observasjon: Utilsiktet
Konklusjon
Etter innlevering
Bibliografi

Oppsett

Figur: Oppsett av måleutstyr

Introduksjon
GPS timing
Anvendelse
Utfordringer og trusler
Referansetrusselen
Deteksjon og mottiltak
Flere GPS mottakere
Referanseklokke
Implementasjon
Ønsket funksjonalitet
Sensor server arkitektur
Klokkemodell
Filtre
Test av lokasjon- og hastighetsfilter
Beskrivelse
Test av klokkemodell og filtre
Observasjon
Observasjon: Utilsiktet
Konklusjon
Etter innlevering
Bibliografi

Oppsett

Figur: Oppsett av måleutstyr

Introduksjon
GPS timing
Anvendelse
Utfordringer og trusler
Referansetrusselen
Deteksjon og mottiltak
Flere GPS mottakere
Referanseklokke
Implementasjon
Ønsket funksjonalitet
Sensor server arkitektur
Klokkemodell
Filtre
Test av lokasjon- og hastighetsfilter
Beskrivelse
Test av klokkemodell og filtre
Observasjon
Observasjon: Utilsiktet
Konklusjon
Etter innlevering
Bibliografi

Oppsett: plassering av mottakere

Figur: Plasseringen av GPS mottakere

Introduksjon
GPS timing
Anvendelse
Utfordringer og trusler
Referansetrusselen
Deteksjon og mottiltak
Flere GPS mottakere
Referanseklokke
Implementasjon
Ønsket funksjonalitet
Sensor server arkitektur
Klokkemodell
Filtre
Test av lokasjon- og hastighetsfilter
Beskrivelse
Test av klokkemodell og filtre
Observasjon
Observasjon: Utilsiktet
Konklusjon
Etter innlevering
Bibliografi

Utførelse

- Flyttet antenne 1 mot antenne 2
- Flyttet antenne 2 mot antenne 1
- Viftet antenne 1 rundt i en halvsirkel
- Viftet antenne 2 rundt i en halvsirkel
- Dekket antennene

Introduksjon
GPS timing
Anvendelse
Utfordringer og trusler
Referansetrusselen
Deteksjon og mottiltak
Flere GPS mottakere
Referanseklokke
Implementasjon
Ønsket funksjonalitet
Sensor server arkitektur
Klokkemodell
Filtre
Test av lokasjon- og hastighetsfilter
Beskrivelse
Test av klokkemodell og filtre
Observasjon
Observasjon: Utilsiktet
Konklusjon
Etter innlevering
Bibliografi

Utførelse

Introduksjon
GPS timing
Anvendelse
Utfordringer og trusler
Referansetrusselen
Deteksjon og mottiltak
Flere GPS mottakere
Referanseklokke
Implementasjon
Ønsket funksjonalitet
Sensor server arkitektur
Klokkemodell
Filtre
Test av lokasjon- og hastighetsfilter
Beskrivelse
Test av klokkemodell og filtre
Observasjon
Observasjon: Utilsiktet
Konklusjon
Etter innlevering
Bibliografi

Observasjon

- Ingen falske positive
- GPS log korrelerer
- Server log korrelerer
- Frekvensmåling korrelerer

Introduksjon
GPS timing
Anvendelse
Utfordringer og trusler
Referansetrusselen
Deteksjon og mottiltak
Flere GPS mottakere
Referanseklokke
Implementasjon
Ønsket funksjonalitet
Sensor server arkitektur
Klokkemodell
Filtre
Test av lokasjon- og hastighetsfilter
Beskrivelse
Test av klokkemodell og filtre
Observasjon
Observasjon: Utilsiktet
Konklusjon
Etter innlevering
Bibliografi

Observasjon: Målesystem

Figur: Måleserie gjort under test av lokasjon og hastighetsfilter

Introduksjon
GPS timing
Anvendelse
Utfordringer og trusler
Referansetrusselen
Deteksjon og mottiltak
Flere GPS mottakere
Referanseklokke
Implementasjon
Ønsket funksjonalitet
Sensor server arkitektur
Klokkemodell
Filtre
Test av lokasjon- og hastighetsfilter
Beskrivelse
Test av klokkemodell og filtre
Observasjon
Observasjon: Utilsiktet
Konklusjon
Etter innlevering
Bibliografi

Oppsett

- Testet klokkemodellen og styring.
- Tok bare med en sensor da fokus var på klokkemodell.
- Justerte grenseverdier

Introduksjon
GPS timing
Anvendelse
Utfordringer og trusler
Referansetrusselen
Deteksjon og mottiltak
Flere GPS mottakere
Referanseklokke
Implementasjon
Ønsket funksjonalitet
Sensor server arkitektur
Klokkemodell
Filtre
Test av lokasjon- og hastighetsfilter
Beskrivelse
Test av klokkemodell og filtre
Observasjon
Observasjon: Utilsiktet
Konklusjon
Etter innlevering
Bibliografi

Utførelse

- Flyttet antenne
- Viftet antenne rundt i en halvsirkel
- Aktiverte disiplinering av klokka manuelt

Introduksjon
GPS timing
Anvendelse
Utfordringer og trusler
Referansetrusselen
Deteksjon og mottiltak
Flere GPS mottakere
Referanseklokke
Implementasjon
Ønsket funksjonalitet
Sensor server arkitektur
Klokkemodell
Filtre
Test av lokasjon- og hastighetsfilter
Beskrivelse
Test av klokkemodell og filtre
Observasjon
Observasjon: Utilsiktet
Konklusjon
Etter innlevering
Bibliografi

Observasjon

- Ingen falske positive
- GPS log korrelerer
- Server log korrelerer
- Frekvensmåling korrelerer

Introduksjon
GPS timing
Anvendelse
Utfordringer og trusler
Referansetrusselen
Deteksjon og mottiltak
Flere GPS mottakere
Referanseklokke
Implementasjon
Ønsket funksjonalitet
Sensor server arkitektur
Klokkemodell
Filtre
Test av lokasjon- og hastighetsfilter
Beskrivelse
Test av klokkemodell og filtre
Observasjon
Observasjon: Utilsiktet
Konklusjon
Etter innlevering
Bibliografi

Observasjon

Figur: Måleserie gjort under klokkemodell test

Introduksjon
GPS timing
Anvendelse
Utfordringer og trusler
Referansetrusselen
Deteksjon og mottiltak
Flere GPS mottakere
Referanseklokke
Implementasjon
Ønsket funksjonalitet
Sensor server arkitektur
Klokkemodell
Filtre
Test av lokasjon- og hastighetsfilter
Beskrivelse
Test av klokkemodell og filtre
Observasjon
Observasjon: Utilsiktet
Konklusjon
Etter innlevering
Bibliografi

Observasjon: Utilsiktet

Figur: Måleserie gjort under utilsiktet forstyrrelse

Introduksjon
GPS timing
Anvendelse
Utfordringer og trusler
Referansetrusselen
Deteksjon og mottiltak
Flere GPS mottakere
Referanseklokke
Implementasjon
Ønsket funksjonalitet
Sensor server arkitektur
Klokkemodell
Filtre
Test av lokasjon- og hastighetsfilter
Beskrivelse
Test av klokkemodell og filtre
Observasjon
Observasjon: Utilsiktet
Konklusjon
Etter innlevering
Bibliografi

Konklusjon

Vi har demonstrert:

- At en fullt fungerende *spoof proof atomic clock controller*" ville ha vært i stand til å stå imot et angrep utført med en sofistikert GPS spoofer slik som *The Civil GPS spoofer*".
- Nåværende implementasjonen evne til å detektere en forstyrrelse av GPS signaler og en begrenset evne til å begrense skaden av nevnte forstyrrelse.
- Effektivitet til Sensor server arkitekturen.
  - Lav responstid
  - Høy stabilitet
  - Enkel å bygge ut med flere sensorer

Introduksjon
GPS timing
Anvendelse
Utfordringer og trusler
Referansetrusselen
Deteksjon og mottiltak
Flere GPS mottakere
Referanseklokke
Implementasjon
Ønsket funksjonalitet
Sensor server arkitektur
Klokkemodell
Filtre
Test av lokasjon- og hastighetsfilter
Beskrivelse
Test av klokkemodell og filtre
Observasjon
Observasjon: Utilsiktet
Konklusjon
Etter innlevering
Bibliografi

Ikke løste problemer

- Kommunikasjon med atomklokke
  - Antatt å ha vært et problem med konfigurasjonen av serialport.
  - Systematisk feilsøkt etter innlevering. Forsøkt:
    - Forskjellige kabler
    - Forskjellige datamaskiner
    - Verifisert med serial port sniffer", riktig kommando sendes.
  - Kan være et fastvare problem
- GPS filter ikke ferdig integrert.

Introduksjon
GPS timing
Anvendelse
Utfordringer og trusler
Referansetrusselen
Deteksjon og mottiltak
Flere GPS mottakere
Referanseklokke
Implementasjon
Ønsket funksjonalitet
Sensor server arkitektur
Klokkemodell
Filtre
Test av lokasjon- og hastighetsfilter
Beskrivelse
Test av klokkemodell og filtre
Observasjon
Observasjon: Utilsiktet
Konklusjon
Etter innlevering
Bibliografi

Bibliografi I

Justin Smith. https://commons.wikimedia.org/wiki/File:Cell-Tower.jpg. CC BY-SA 2.5 https://creativecommons.org/licenses/by-sa/2.5/deed.en. URL: https://upload.wikimedia.org/wikipedia/commons/8/85/Cell-Tower.jpg.

Kontinuum Engineering og Design Center. URL: http://ec-continuum.ru/eng/projects/pmu.shtml.

Mike Peel. https://commons.wikimedia.org/wiki/File:New_York_Stock_Exchange,_Wall_Street.jpg. Licenced under CC-BY-SA-4.0 https://creativecommons.org/licenses/by-sa/4.0/deed.en. URL: https://upload.wikimedia.org/wikipedia/commons/5/58/New_York_Stock_Exchange%2C_Wall_Street.jpg.

Introduksjon
GPS timing
Anvendelse
Utfordringer og trusler
Referansetrusselen
Deteksjon og mottiltak
Flere GPS mottakere
Referanseklokke
Implementasjon
Ønsket funksjonalitet
Sensor server arkitektur
Klokkemodell
Filtre
Test av lokasjon- og hastighetsfilter
Beskrivelse
Test av klokkemodell og filtre
Observasjon
Observasjon: Utilsiktet
Konklusjon
Etter innlevering
Bibliografi

Bibliografi II

Daniel P. Shepard, Todd E. Humphreys og Aaron A. Fansler. "Evaluation of the Vulnerability of Phasor Measurement Units to GPS Spoofing Attacks". I: (2012).

Introduksjon
GPS timing
Anvendelse
Utfordringer og trusler
Referansetrusselen
Deteksjon og mottiltak
Flere GPS mottakere
Referanseklokke
Implementasjon
Ønsket funksjonalitet
Sensor server arkitektur
Klokkemodell
Filtre
Test av lokasjon- og hastighetsfilter
Beskrivelse
Test av klokkemodell og filtre
Observasjon
Observasjon: Utilsiktet
Konklusjon
Etter innlevering
Bibliografi