Spoof proof GPS timing

A detection and mitigation system for GPS time spoofing

A. Schultzen[1]

[1]Institutt for informatikk
Universitetet i Oslo

1. desember 2016

Agenda

GPS timing

- Tre satellitter *egentlig* nødvendig.
- Fjerde satellitt gir synkronisert klokke.
- GPS timing er klokker disiplinert av GPS.

- Tidsstempling
  - E-handel
  - Høyhastighets aksjehandel
  - Logging etc.
- Fasemålinger i kraftnett.
- Telekommunikasjon.

Utfordringer og trusler

Utfordringer og trusler

Utfordringer:

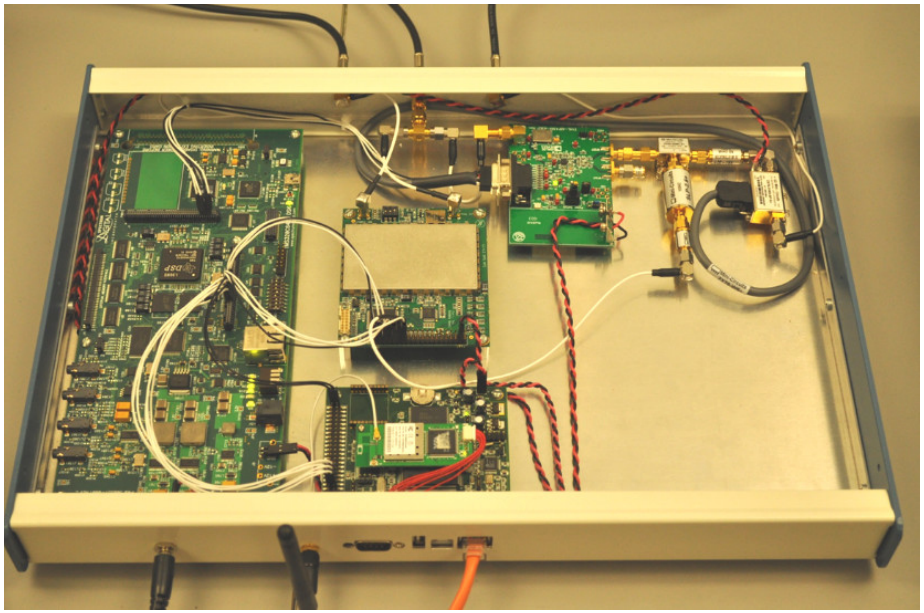
- Avhengig av å ha en antenne med fri sikt.
- Kjent kodestruktur.
- Naive mottakere.

Terror, sabotasje mulig motiv for:

- Jamming.
- Spoofing.
- Feil i utstyr.

Referansetrusselen

The Civil GPS Spoofer”



Figur: Civil GPS Spoofer

The Civil GPS Spoofer”

- Laget et av et team fra *The University of Texas at Austin* i 2012 [1]
- Implementert i SDR”
- Simulere opptil 14 falskesatellitter.

The Civil GPS Spoofer"

Nøkkelfunksjoner:

- Sømløs narring, offeret låser på en kopi av det autentiske signalet. Ingen forandring i løsning.
- Angriper manipulerer signalet.
- Angriperen har gjerne et stort spillerom under angrepet da oscillatoren i mottakeren ofte er av lav kvalitet.

Deteksjon og mottiltak

Deteksjon og mottiltak

- Deteksjon
  - Bruke flere GPS mottakere med kjent posisjon.
  - Bruke stabil klokke som referanse.
- Mottiltak: Bruke klokke som tidskilde.

Flere GPS mottakere og kjent posisjon

- En GPS mottakere med ukjent posisjon: Lett
- En GPS mottakere med kjent posisjon: Gjennomførbart
- To GPS mottakere med kjent posisjon: Svært komplisert
  - Minimum en mottakere løser feil posisjon.
  - Med mindre spooferener like langt fra begge, forskjell i tidsløsning.

Kompleksiteten øker for hver GPS mottaker som legges til.

Referanseklokke

Med en stabil og pålitelig klokke, har en muligheter til å:

- Verifisere GPS løsning.
- Realisere nøyaktig timing selv når GPS disiplinering ikke er mulig.

Figur: Symmetricom 5071A Cesium Primary Frequency Standard (500 000 NOK)

Figur: Symmetricom SA.45s CSAC (5000 NOK)

Referanseklokke

Vi valgte Symmetricom SA.45s.

- Lav vekt og størrelse
- Kortidsstabilitet på rundt 10^{-11} sekunder.
- Intern frekvensteller og styringsalgoritme
- Kommuniserer telemetri over RS-232

Implementasjon

Ønsket funksjonalitet

- Detektere angrep hurtig
- Mulighet for å logge data
- Rask og enkel tilgang til innsamlet data
- Enkelt koble til flere GPS mottakere
- Administreres over nettverk
- Konfigurerbar

Sensor server arkitektur

- Mottaker + Raspberry PI = Sensor
- Eliminerer behovet for lange signalkabler, bruke nettverk:
  - Fiber
  - Mobilnett (3G og 4G)
  - WiFi
- Antall mottakere begrenset av serverens maskinvare.

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

Implementasjon: Klokkemodell

Klokkemodell

Klokkemodellen brukt i oppgaven er designet av Harald Hauglin. Brukes til:

- Referanse for frekvensavvik og klokkedrift
- Generere brukbare styringsparameter i tilfelle GPS løsning ikke lenger er til å stole på.

Modellen er logisk en del av serveren og kjører i en egen prosess.

- Kommuniserer med atomklokka
- Moden etter to dager (konfigurerbart).

Implementasjon: Filtre

Filtre

Filtrene brukes til å detektere avvik. Enten:

- GPS-basert
- Klokkemodell-basert

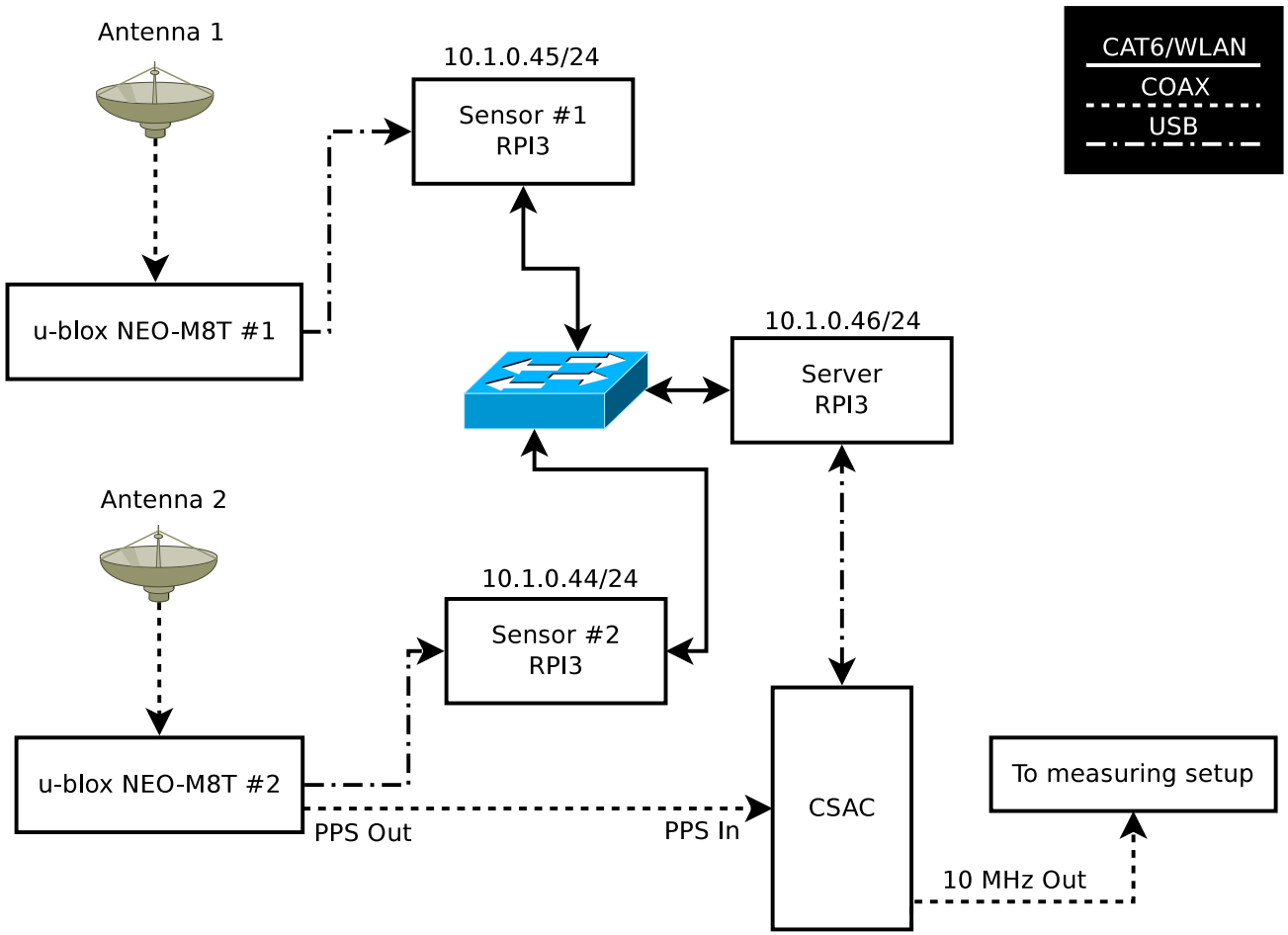
For øyeblikket kun implementert tre filtre:

- Lokasjon og hastighetsfilter
  - Data fra sensorene blir samlet formatert.
  - Sjekker løst posisjon og hastighet mot referanseverdier
- Fasehoppfilter
  - Sammenlikner nåværende fase med pre-konfigurert grense.
- Frekvenskorreksjonsfilter
  - Sammenlikner nåværende styringsverdi med en forventet styringsverdi

Pre-konfigurerte referanseverdier er basert på et gjennomsnitt kalkulert fra en lengre måleserie.

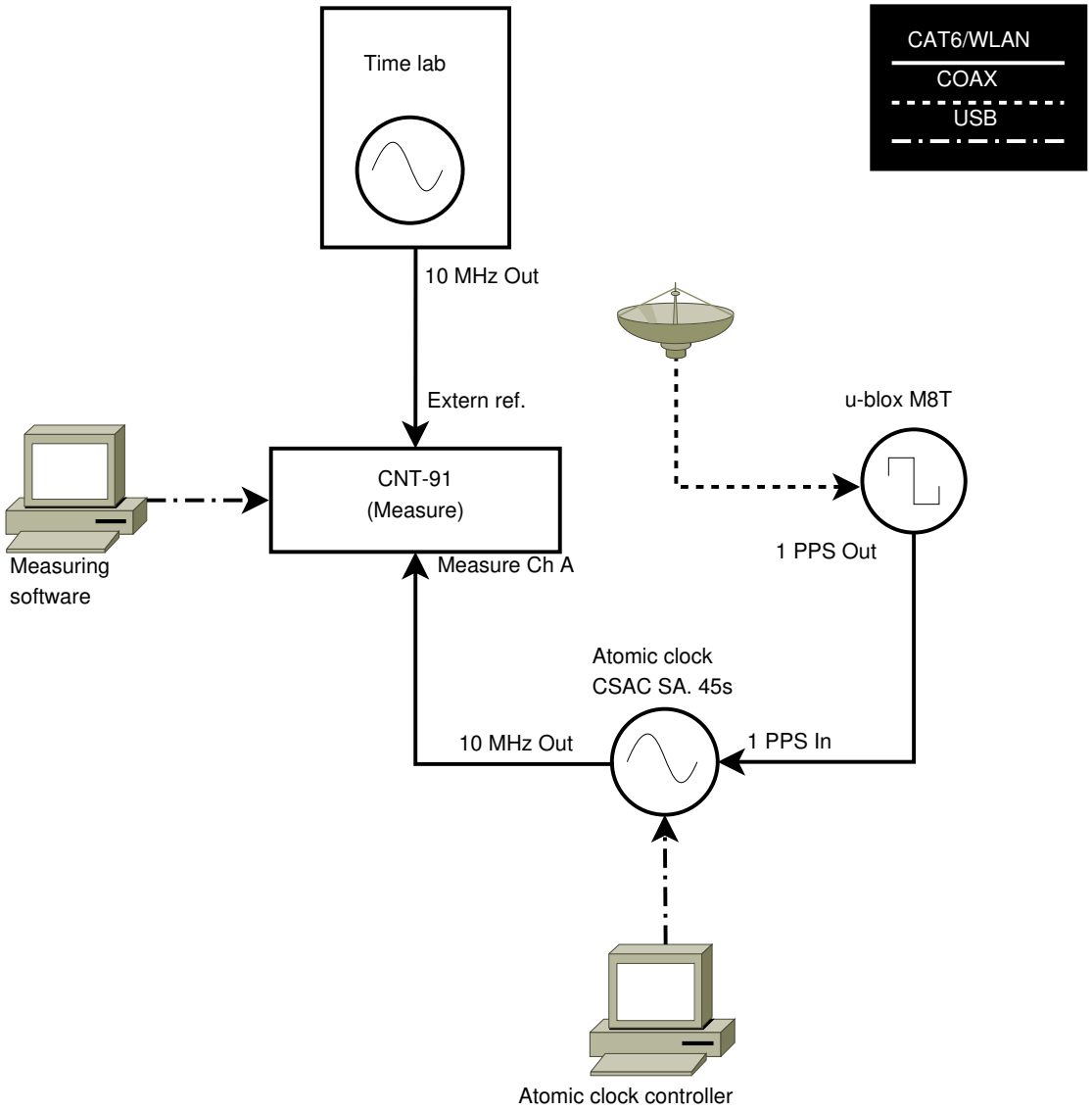
Test av lokasjon- og hastighetsfilter

Oppsett



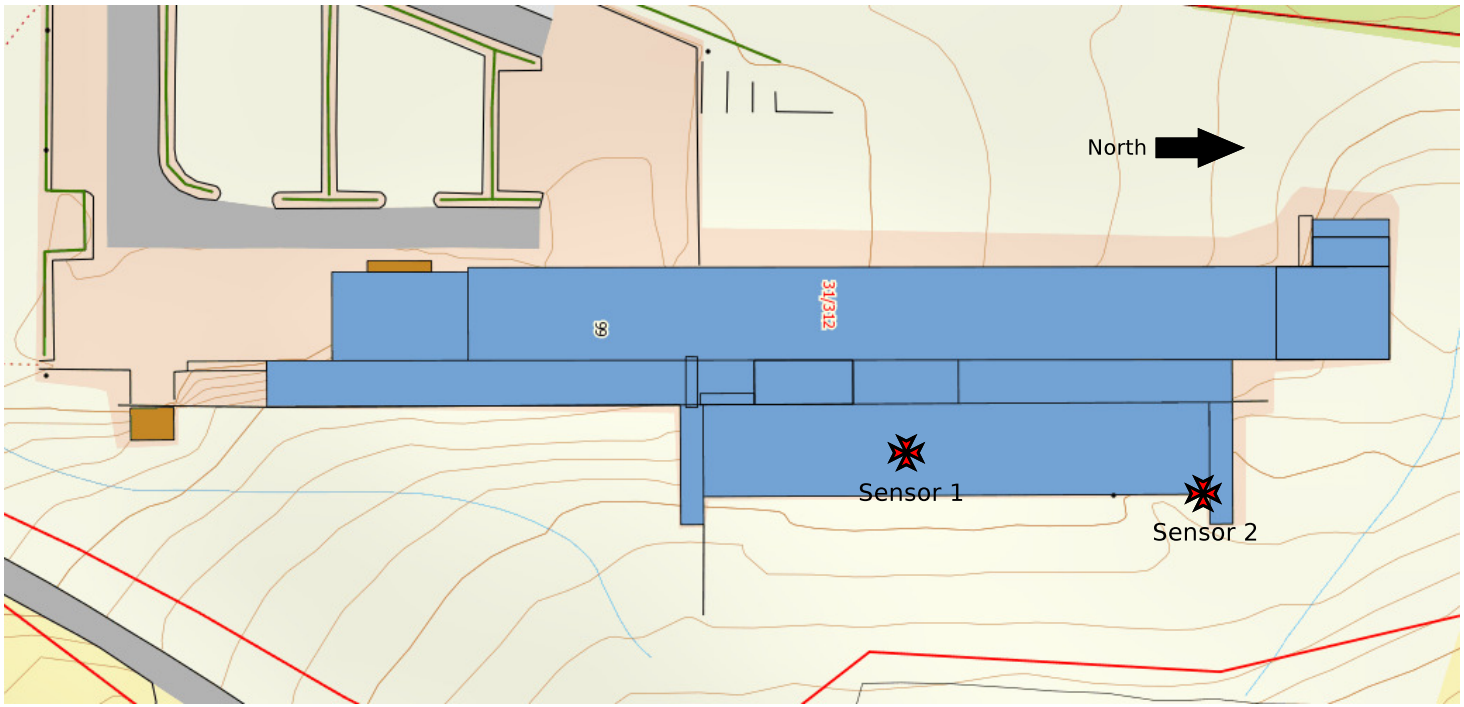
Figur: Oppsett av server og klienter under test

Oppsett



Figur: Oppsett av måleutstyr

Oppsett: plassering av mottakere



Figur: Plasseringen av GPS mottakere

Utførelse

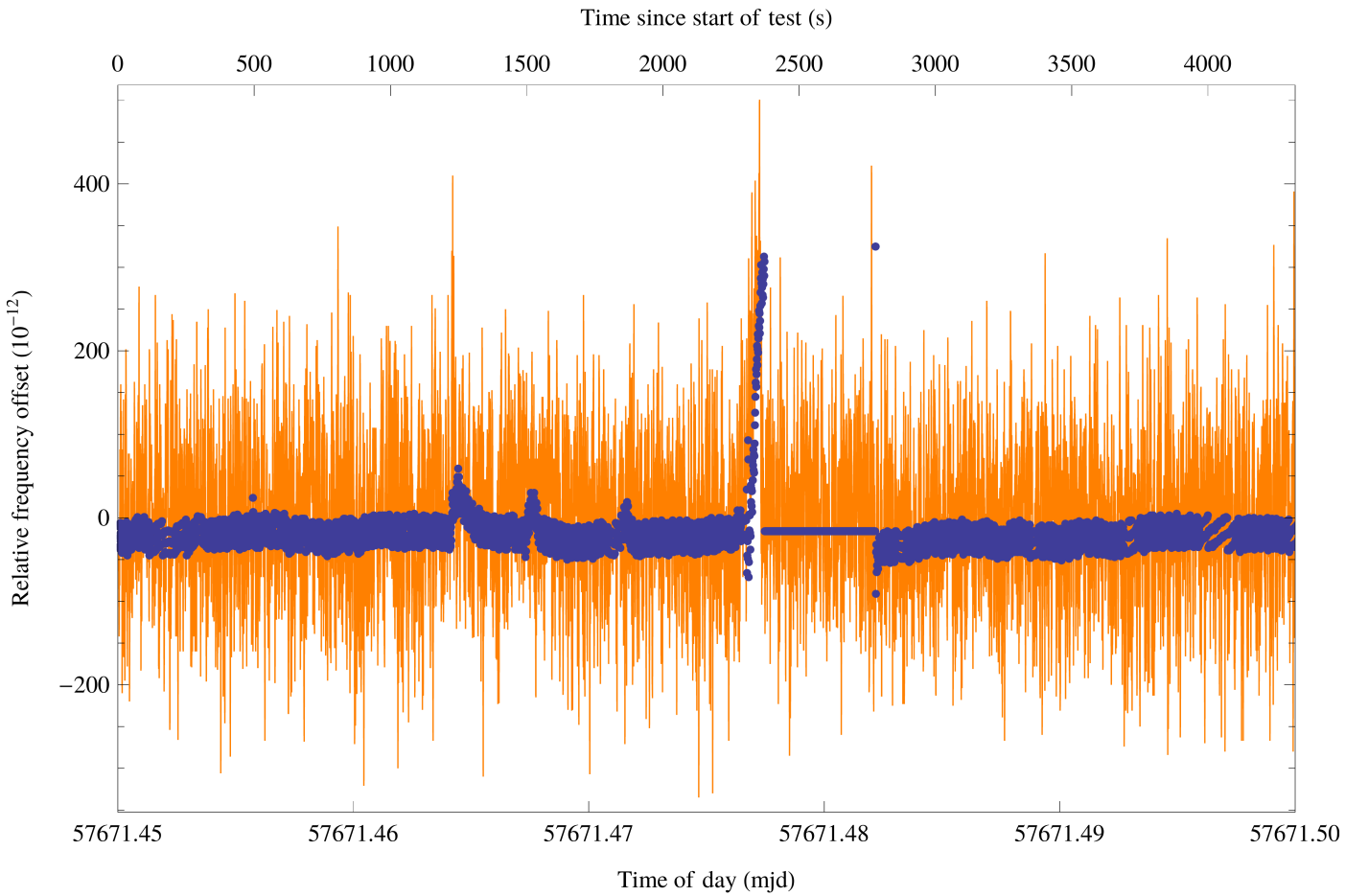
- Flyttet antenne 1 mot antenne 2
- Flyttet antenne 2 mot antenne 1
- Viftet antenne 1 rundt i en halvsirkel
- Viftet antenne 2 rundt i en halvsirkel
- Dekket antennene

Utførelse

Observasjon

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

Observasjon: Målesystem



Figur: Måleserie gjort under test av lokasjon og hastighetsfilter

Test av klokkemodell og filtre

Oppsett

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

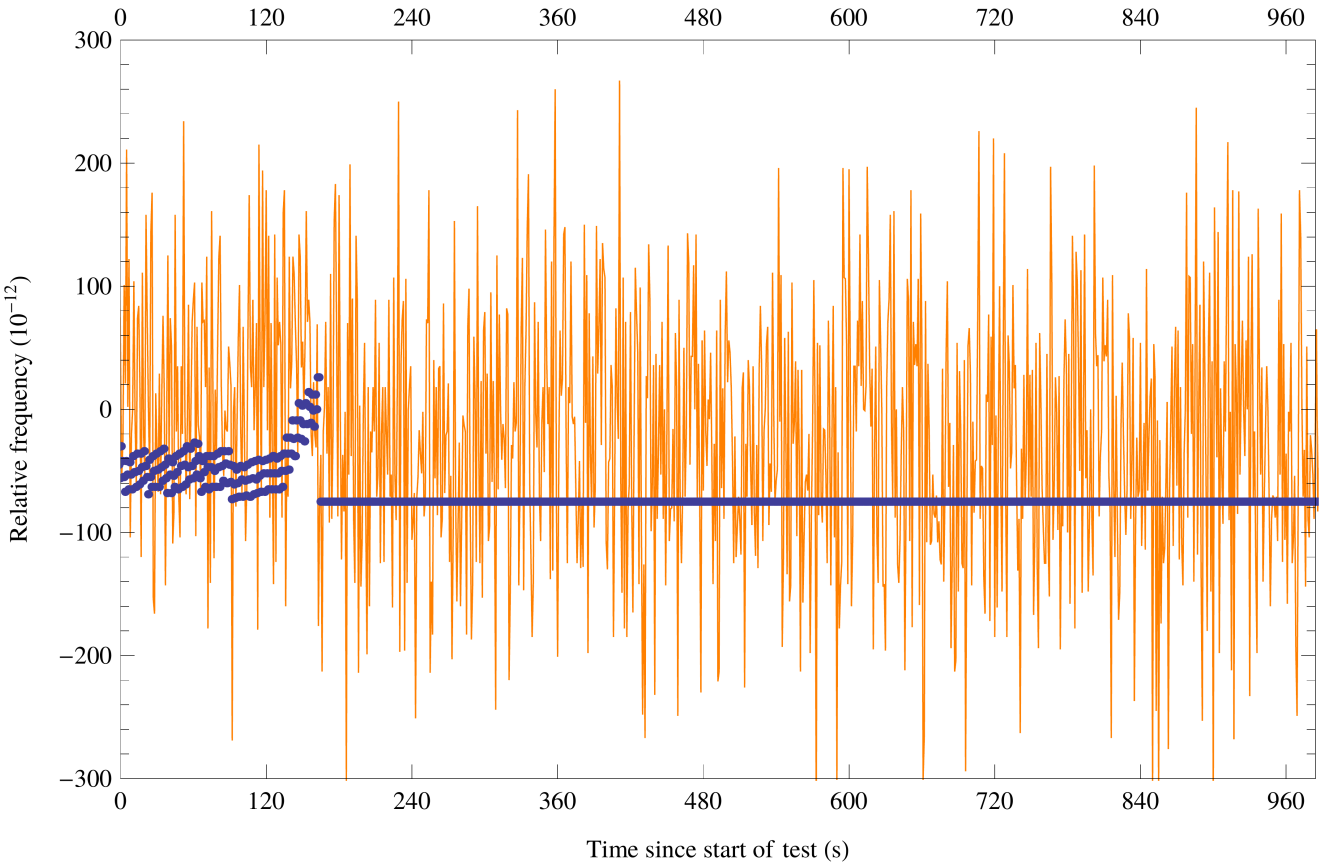
Utførelse

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

Observasjon

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

Observasjon



Figur: Måleserie gjort under klokkemodell test

Konklusjon

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

Etter innlevering

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.

Bibliografi I

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