Spoof proof GPS timing

A detection and mitigation system for GPS time spoofing

A. Schultzen¹

¹Institutt for informatikk Universitetet i Oslo

1. desember 2016

Spoof proof GPS timing

A. Schultzen

Agenda

Introduksjon

GPS timing

Utfordringer og trusler Referansetrusselen

Deteksjon og

Flere GPS mottakere

Referanseklokke Implementasion

Ønsket funksjonalite Sensor server arkitektur

Filtre

Test av lokasjonog hastighetsfilte

Test av klokkemodell og

Observasjon

O D D C I V G D J C I I

Etter innleve

Agenda

Spoof proof GPS timing

A. Schultzen

Agenda

Introduksjon

GPS timing

Utfordringer og trusler Referansetrusselen

Deteksjon og

Flere GPS mottakere

Referanseklokke

Implementasjon Ønsket funksjonalite Sensor server

Klokkemo

Fiitre Fest av Iokasjo

og hastighetsfilter

Beskrivelse

Test av klokkemodell og filtre

Observasjon

Ettor innlov

Pibliografi

Dibliografi

Introduksjon

Deteksjon og mottiltak

Implementasjon

Test av lokasjon- og hastighetsfilter

Test av klokkemodell og filtre

Konklusjon

Etter innlevering

GPS timing

- ► Tre satellitter *egentlig* nødvendig.
- ► Fjerde satellitt gir synkronisert klokke.
- ▶ GPS timing er klokker disiplinert av GPS.
- Tidsstempling
 - ▶ F-handel
 - Høyhastighets aksjehandel
 - Logging etc.
- Fasemålinger i kraftnett.
- ► Telekommunikasjon.

Spoof proof GPS timing

A. Schultzen

Agenda

Introduksjon

GPS timing

Utfordringer og trusler Referansetrusselen

Deteksjon og mottiltak

Flere GPS mottakere Referanseklokke

Implementasjon Ønsket funksjonalite Sensor server arkitektur

Klokken Filtre

Test av lokasjonog hastighetsfilter

Test av klokkemodell og filtre

Observasjon

Mandalanian

Etter innleve

. . .



Utfordringer og trusler

Spoof proof GPS timing

A. Schultzen

Agenda

Introduksjo

GPS timing

Utfordringer og trusle Referansetrusselen

mottiltak

Flere GPS mottaken Referanseklokke

Implementasion

Ønsket funksjonalit Sensor server arkitektur

Klokkemodel Filtre

Fest av lokasjonog hastighetsfilter

Test av klokkemodell og filtre

Observasjon

Konklusjon

Etter innlevering

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.

Spoof proof GPS timing

A. Schultzen

Agenda

Introduksjon

Utfordringer og trusler

Deteksjon og

mottiltak Flere GPS mottak

Flere GPS mottakere Referanseklokke

Implementasjon Ønsket funksjonalite Sensor server arkitektur

Klokkem Filtre

Test av lokasjonog hastighetsfilter

Test av klokkemodell og filtre

Observasjon

00000.000000.

Etter innleve



Referansetrusselen

Spoof proof GPS timing

A. Schultzen

Agenda

Introduksjoi

GPS timin

Utfordringer og trusler Referansetrusselen

Deteksion og

mottiltak

Referanseklokke

Implementasjon Ønsket funksjonalit

> rkitektur Klokkemode ---

Test av lokasjonog hastighetsfilter

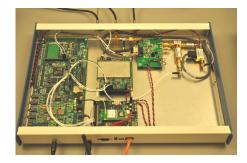
Test av klokkemodell og filtre

Observasjon

.

Etter innlevering

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.

Spoof proof GPS timing

A. Schultzen

Agenda

Introduksjon

GPS timing
Utfordringer og trusle
Referansetrusselen

Deteksjon o mottiltak

Flere GPS mottakere Referanseklokke

Implementasjon Ønsket funksjonalitet Sensor server arkitektur

Klokkem Filtre

Test av lokasjonog hastighetsfilter Beskrivelse

Test av klokkemodell og filtre

Observasjor

Konklus

Etter innleveri

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.

Spoof proof GPS timing

A. Schultzen

Agenda

Introduksjon

Utfordringer og trusle Referansetrusselen

Deteksjon og mottiltak

Flere GPS mottakere Referanseklokke

Implementasjon
Ønsket funksjonalite
Sensor server
arkitektur

Test av lokasjonog hastighetsfilter

Test av Ilokkemodell og

bservasion

Observasjon

Etter innleverir



Deteksjon og mottiltak

Spoof proof GPS timing

A. Schultzen

Agenda

Introduksjoi

GPS timing

Utfordringer og trus Referansetrusselen

Deteksjon og mottiltak

Flere GPS mottakere Referanseklokke

Implementasjon

Ønsket funksjonali Sensor server arkitektur

Klokken Filtre

Test av lokasjonog hastighetsfilter

Test av klokkemodell og filtre

Observasjon

Kaaldusiaa

Etter innlevering

Deteksjon og mottiltak

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

Spoof proof GPS timing

A. Schultzen

Agenda

Introduksjon

GPS timing

Utfordringer of Referansetrus

Deteksjon og mottiltak

Flere GPS mottakere Referanseklokke

Implementasjon Ønsket funksjonalite

Sensor server arkitektur

Klokker Filtre

Test av lokasjonog hastighetsfilter

Test av klokkemodell og filtre

Observasjon

O D D C I V G D J C I I

Etter innleve

.....



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.

Spoof proof GPS timing

A. Schultzen

Agenda

Introduksjon

Utfordringer og trusler Referansetrusselen

Deteksjon og mottiltak

Flere GPS mottakere Referanseklokke

Implementasjon Ønsket funksjonalitet Sensor server arkitektur

Filtre

Test av lokasjonog hastighetsfilter

Test av klokkemodell og

)bservasjon

Observasjon

tter innlever



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) Spoof proof GPS timing

A. Schultzen

Agenda

Introduksjor

GPS timing
Utfordringer og trusler
Referansetrusselen

Deteksjon o nottiltak

Flere GPS mottakere Referanseklokke

Implementasjon Ønsket funksjonalitet Sensor server arkitektur

Klokkem Filtre

Test av lokasjonog hastighetsfilter

Test av klokkemodell og

Observasion

Observasjon

Etter innlever



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

Spoof proof GPS timing

A. Schultzen

Agenda

Introduksjor

Utfordringer og trusle

Deteksjon og

Flere GPS mottakere Referanseklokke

Implementasjon

Sensor server arkitektur Klokkemodell

Klokker Filtre

Test av lokasjonog hastighetsfilter

Test av klokkemodell og filtre

Observasjon

Etter innleve

Etter innleverin

Sibliograf



Implementasjon

Spoof proof GPS timing

A. Schultzen

Agenda

Introduksjoi

GPS timing

Referansetrusselen

mottiltak

Flere GPS mottakere Referanseklokke

Implementasjon

Sensor server arkitektur

Klokkemod Filtre

Test av lokasjonog hastighetsfilter

Test av klokkemodell og filtre

bservasjon

Konklusion

Etter innlevering

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

Spoof proof GPS timing

A. Schultzen

Agenda

Introduksjor

GPS timing

Utfordringer og Referansetrusse

Deteksjon og mottiltak

Flere GPS mottakere Referanseklokke

Implementasjon
Ønsket funksjonalitet

rkitektur Klokkemodel

Test av lokasjonog hastighetsfilter

Fest av klokkemodell og iltre

)bservasion

Observasjon

Etter innleveri



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.

Spoof proof GPS timing

A. Schultzen

Agenda

Introduksjon

Utfordringer og trusler

Deteksjon og mottiltak

Flere GPS mottakere Referanseklokke

Implementasjon

Ønsket funksjonalite
Sensor server
arkitektur

Klokkem Filtre

Test av lokasjonog hastighetsfilter

Test av klokkemodell og filtre

Observasjon

Obscivasjon

Etter innlev

:61:----



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

Spoof proof GPS timing

A. Schultzen

Agenda

Introduksjon

Utfordringer og trusler

Deteksjon og nottiltak

Flere GPS mottakere Referanseklokke

Implementasjon Ønsket funksjonalitet Sensor server arkitektur

> est av lokasjonz hastighetsfilte

Test av klokkemodell og

Observasion

Observasjon

Konklus

Etter innleverin



Implementasjon: Klokkemodell

Spoof proof GPS timing

A. Schultzen

Agenda

Introduksjoi

GPS timing

Referansetrusselen

Deteksjon og

Flere GPS mottaken Referanseklokke

Implementasion

Ønsket funksional

Sensor server arkitektur Klokkemodell

<lokkemo Filtre

Test av lokasjonog hastighetsfilter

Test av klokkemodell og filtre

Observasjon

Konklusjor

Etter innlevering

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).

Spoof proof GPS timing

A. Schultzen

Agenda

Introduksjon

Utfordringer og trusler Referansetrusselen

Deteksjon o_l mottiltak

Flere GPS mottakere Referanseklokke

Implementasjon
Ønsket funksjonalitet
Sensor server

Klokkemodell Filtre

Test av lokasjonog hastighetsfilter

Test av klokkemodell og

Observasjon

· · · · ·

Ettor innlov

Etter innleveri



Implementasjon: Filtre

Spoof proof GPS timing

A. Schultzen

Agenda

Introduksjoi

GPS timing

Utfordringer og trusle Referansetrusselen

mottiltak

Flere GPS mottakere Referanseklokke

Implementasion

Ønsket funksjonal Sensor server arkitektur

Klokkemodell

Test av lokasjonog hastighetsfilter

Test av klokkemodell og filtre

Observasjon

Konklusjon

Etter innlevering

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.

Spoof proof GPS timing

A. Schultzen

Agenda

Introduksjon

GPS timing Utfordringer og tr

Utfordringer og tru Referansetrusselen

Jeteksjon o nottiltak

Flere GPS mottakere Referanseklokke

Implementasjon Ønsket funksjonalitet Sensor server arkitektur

Filtre est av loka

Test av lokasjonog hastighetsfilter

est av lokkemodell o Itre

Observasjon

Z...LL....

......

tter innleveri

Bibliogra



Test av lokasjon- og hastighetsfilter

Spoof proof GPS timing

A. Schultzen

Agenda

Introduksjoi

GPS timing

Utfordringer og trusle Referansetrusselen

Deteksjon og

Flere GPS mottakere Referanseklokke

Implementasjon

Ønsket funksjonali Sensor server arkitektur

> Klokken Filtre

Test av lokasjonog hastighetsfilter

Test av klokkemodell og filtre

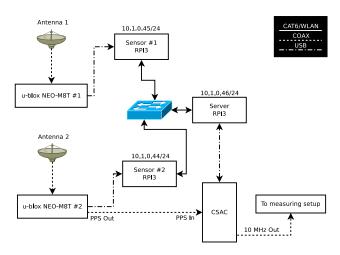
Observasjon

Konklusion

Etter innlevering



Oppsett



Figur: Oppsett av server og klienter under test

Spoof proof GPS timing

A. Schultzen

Agenda

Introduksjon

GPS timing

Utfordringer og trusler Referansetrusselen

Deteksjon o mottiltak

Flere GPS mottakere Referanseklokke

Implementasjon Ønsket funksjonalitet Sensor server

Klokkem Filtre

Test av lokasjonog hastighetsfilter Beskrivelse

Test av klokkemodell c filtre

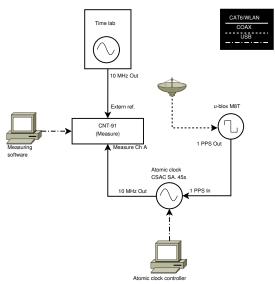
Observasjon

Konklusj

Etter innlevering



Oppsett



Figur: Oppsett av måleutstyr

Spoof proof GPS timing

A. Schultzen

Agenda

Introduksjo

GPS timing

Utfordringer og trusler Referansetrusselen

Deteksjon o mottiltak

Flere GPS mottakere Referanseklokke

Implementasjon
Ønsket funksjonalite
Sensor server

Klokken Filtre

Test av lokasjonog hastighetsfilter Beskrivelse

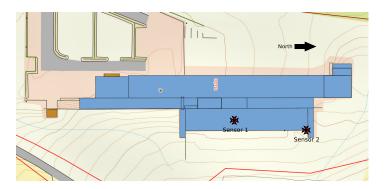
Test av klokkemodell og filtre

Observasjon

Etter innlever



Oppsett: plassering av mottakere



Figur: Plasseringen av GPS mottakere

Spoof proof GPS timing

A. Schultzen

Agenda

Introduksjon

Utfordringer og trusler

Deteksjon og

Flere GPS mottakere Referanseklokke

Referanseklokke

Ønsket funksjonalitet Sensor server arkitektur

Klokkem Filtre

Test av lokasjonog hastighetsfilter Beskrivelse

Test av klokkemodell og

Observasion

. . . .

Etter innleverin



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

Spoof proof GPS timing

A. Schultzen

Agenda

Beskrivelse



Utførelse



Spoof proof GPS timing

A. Schultzen

Agenda

Introduksjoi

GPS timing

Utfordringer og tru Referansetrusselen

> Deteksjon c mottiltak

Flere GPS mottakere Referanseklokke

Ønsket funksjonalit

Klokke Filtre

Test av lokasjonog hastighetsfilter Beskrivelse

Test av klokkemodell og filtre

Observasjon

Konklusio

Etter innleveri

Observasjon

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

Spoof proof GPS timing

A. Schultzen

Agenda

Introduksjo

GPS timing

Utfordringer og tru Referansetrusseler

Deteksjon o mottiltak

Flere GPS mottakere Referanseklokke

Implementasjon

Ønsket funksjona Sensor server arkitektur

Klokker Filtre

Test av lokasjonog hastighetsfilter Beskrivelse

Test av klokkemodell og filtre

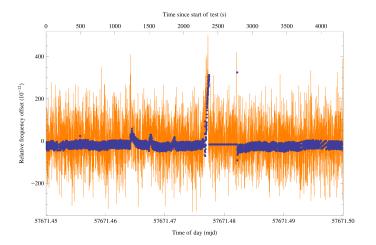
Observasjon

00000110000011

Etter innleve



Observasjon: Målesystem



Figur: Måleserie gjort under test av lokasjon og hastighetsfilter

Spoof proof GPS timing

A. Schultzen

Agenda

Introduksjon

GPS timing
Utfordringer og trusl

mottiltak

Flere GPS mottakere Referanseklokke

Implementasjon

Ønsket funksjonalitet
Sensor server
arkitektur

Klokken Filtre

Test av lokasjonog hastighetsfilter Beskrivelse

Test av klokkemodell filtre

Observasjon

Konklusjoi

Etter innlevering



Test av klokkemodell og filtre

Spoof proof GPS timing

A. Schultzen

Agenda

Beskrivelse



Oppsett

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

Spoof proof GPS timing

A. Schultzen

Agenda

Introduksjor

GPS timing

Utfordringer og Referansetrusse

Deteksjon og mottiltak

Flere GPS mottakere

Referanseklokke

mplementasjon Ønsket funksjonalite

ensor server rkitektur Klokkemodell

Klokken Filtre

Test av lokasjonog hastighetsfilter

Test av klokkemodell og filtre

Observasjon

.

Etter innlev



Utførelse

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

Spoof proof GPS timing

A. Schultzen

Agenda

Introduksjoi

GPS timing

Utfordringer og trusle Referansetrusselen

Deteksjon o mottiltak

Flere GPS mottakere Referanseklokke

Implementasjon

Ønsket funksjonalite

rkitektur Klokkemode

Klokke Filtre

Test av lokasjonog hastighetsfilter

Test av klokkemodell og filtre

Observasjor

----,---

Etter innleve



Observasjon

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

Spoof proof GPS timing

A. Schultzen

Agenda

Introduksjo

GPS timir

Utfordringer og trusl Referansetrusselen

Deteksjon o mottiltak

Flere GPS mottakere Referanseklokke

Implementasjon

Ønsket funksjonal Sensor server Irkitektur

Klokker Filtre

Test av lokasjonog hastighetsfilter

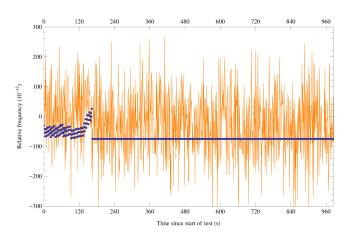
Test av klokkemodell og filtre

Observasjon

Etter innleve



Observasjon



Figur: Måleserie gjort under klokkemodell test

Spoof proof GPS timing

A. Schultzen

Agenda

ntroduksjon

GPS timing

Utfordringer og trusler Referansetrusselen

Deteksjon og mottiltak

Flere GPS mottakere Referanseklokke

Implementasjon
Ønsket funksjonalitet
Sensor server

Klokken Filtre

Test av lokasjonog hastighetsfilter Beskrivelse

Test av klokkemodell og Eltre

Observasjon

Konklus

Etter innleveri



Konklusjon

Spoof proof GPS timing

A. Schultzen

Agenda

Introduksjoi

GPS timing

Utfordringer og trusk Referansetrusselen

Deteksjon og

Flere GPS mottakere Referanseklokke

Implementasjon

Sensor server arkitektur Klokkemodell

Klokkemodel Filtre

Test av lokasjonog hastighetsfilter

Test av klokkemodell og filtre

Observasjon

Kanklusian

Etter innlevering

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
 - Høv stabilitet
 - Enkel å bygge ut med flere sensorer

Spoof proof GPS timing

A. Schultzen

Agenda

Introduksjon GPS timing

Utfordringer og trusler Referansetrusselen

> eteksjon og iottiltak

Flere GPS mottakere Referanseklokke

Implementasjon
Ønsket funksjonalitet
Sensor server
arkitektur

Klokkem Filtre

Test av lokasjonog hastighetsfilter

Test av klokkemodell og Filtro

Observasion

Konklusjon

Etter innleve



Etter innlevering

Spoof proof GPS timing

A. Schultzen

Agenda

Introduksjoi

GPS timing

Utfordringer og trusle Referansetrusselen

Deteksjon og mottiltak

Flere GPS mottakere Referanseklokke

Implementacion

Ønsket funksjonali

rkitektur Klokkemodel ---

Test av lokasjonog hastighetsfilter

Test av klokkemodell og filtre

Observasjon

Konklusjon

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.

Spoof proof GPS timing

A. Schultzen

Agenda

Introduksjon

GPS timing Utfordringer og trusle

> Deteksjon og nottiltak

Flere GPS mottakere Referanseklokke

Implementasjon
Ønsket funksjonalitet
Sensor server
arkitektur

Klokkemo Filtre

Test av lokasjonog hastighetsfilter

Test av klokkemodell og filtre

Observasjon

Observasjon

Etter innlevering



Bibliografi I



Aaron A. Fansler. "Evaluation of the Vulnerability of Phasor Measurement Units to GPS Spoofing Attacks". I: (2012).

Spoof proof GPS timing

A. Schultzen

Agenda

