Spoof proof GPS timing

A detection and mitigation system for GPS time spoofing

A Schultzen¹

¹Institutt for informatikk Universitetet i Oslo

December 1, 2016

Spoof proof GPS timing

A. Schultzen

Agenda

Introduksjon

GPS timing

Utfordringer og trus Referansetrusselen

Deteksjon og mottiltak

Flere GPS mottakere Referanseklokke

Implementasjon Ønsket funksjonalite Sensor server arkitektur

Klokker Filtre

Test av lokasjonog hastighetsfilter

Test av klokkemodell og filtre

Observasjo

Konklusjor

Etter innlevering

Bibliograf

Agenda

Spoof proof GPS timing A. Schultzen

Introduksjon

Deteksjon og mottiltak

Implementasjon

Test av lokasjon- og hastighetsfilter

Test av klokkemodell og filtre

Konklusjon

Etter innlevering

Bibliografi

References

Agenda

ntroduksjon

GPS timing

Utfordringer og trusler Referansetrusselen

Deteksjon og

lere GPS mottakere

Referanseklokke

Ønsket funksjonalitet Sensor server arkitektur

Klokkemo Filtre

est av lokasjong hastighetsfilter Beskrivelse

okkemodell og tre

)bservasjon

Z....Ll......

tter innleverin

GPS timing

- ▶ Bare tre satellitter *egentlig* nødvendig for å finne sin posisjon.
- ► Fjerde satellitt brukes for å korrigere klokka.
- GPS mottakeren er nå synkronisert med atomklokkene i GPS satellittene.
- ▶ GPS timing er klokker disiplinert av GPS.
- Tidsstempling
 - E-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

> Klokkem Filtre

Test av lokasjonog hastighetsfilter

Test av klokkemodell og filtre

Observasjon

Kanlılı....

Etter innleverin

Bibliograf

Utfordringer og trusler

Spoof proof GPS timing

A. Schultzen

Agenda

GPS timing

Utfordringer og trusler

Utfordringer:

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

Terror mulig motiv for:

- Jamming.
 - Spoofing.
 - Feil i utstyr.

Spoof proof GPS timing

A. Schultzen

Agenda

Introduksjon

GPS timing
Utfordringer og trusler

Utfordringer og Referansetrus

Deteksjon o

Flere GPS mottakere Referanseklokke

Implementasjon
Ønsket funksjonalite
Sensor server
arkitektur

Klokkem Filtre

Test av lokasjonog hastighetsfilter

Test av klokkemodell og filtre

Observasjon

Konklusion

Etter innlevering

Bibliografi

Referansetrusselen

Spoof proof GPS timing

A. Schultzen

Agenda

Utfordringer og trusler

"The Civil GPS Spoofer"

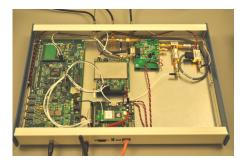


Figure: Civil GPS Spoofer

"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 "falske" satellitter.

Spoof proof GPS timing

A. Schultzen

Agenda

Introduksjon

GPS timing

Utfordringer og trusler Referansetrusselen

Deteksjon og mottiltak

Flere GPS mottakere Referanseklokke

Implementasjon Ønsket funksjonalitet Sensor server arkitektur

Klokkem Filtre

Test av lokasjonog hastighetsfilter Beskrivelse

Test av klokkemodell og filtre

Observasjon

Konklusjo

Etter innleverin

Bibliograf

"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 trusler Referansetrusselen

Deteksjon og mottiltak

Flere GPS mottakere Referanseklokke

Implementasjon
Ønsket funksjonalitet
Sensor server
arkitektur

Filtre

Test av lokasjonog hastighetsfilter

Test av klokkemodell og filtre

Observasjon

Konklusjo

Etter innlevering

Bibliograf

Deteksjon og mottiltak

Spoof proof GPS timing

A. Schultzen

Agenda

Referansetrusselen

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

Introduksjor

GPS timing

Utfordringer Referansetr

Deteksjon og mottiltak

Flere GPS mottakere Referanseklokke

Implementasjon Ønsket funksjonalitet

> arkitektur Klokkemodell

Klokken Filtre

Test av lokasjonog hastighetsfilter

Test av klokkemodell og filtre

Observasjon

Konklusion

Etter innlevering

Bibliograf

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 narren er 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 funksjonalite Sensor server arkitektur

> Klokkem Filtre

Test av lokasjonog hastighetsfilter

Fest av Klokkemodell og

)bservasjon

Konklusion

Etter innlevering

Bibliograf

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.



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



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

Spoof proof GPS timing

A. Schultzen

Agenda

Introduksjon

GPS timing
Utfordringer og trusler
Referansetrusselen

Deteksjon og nottiltak

Flere GPS mottakere Referanseklokke

Implementasjon Ønsket funksjonalitet Sensor server arkitektur

Filtre Fest av Iokas

og hastighetsfilter

Test av klokkemodell og filtre

Observasjor

Konklusjo

Etter innleverin

Bibliogra

Referanseklokke

Vi valgte Symmetricom SA.45s.

- ► Lav vekt og størrelse
- Kortidsstabilitet på rundt (10⁻¹¹)s.
- ▶ Intern frekvensteller og styringsalgoritme
- ► Kommuniserer over RS-232

Spoof proof GPS timing

A. Schultzen

Agenda

Introduksjon

Utfordringer og tr

Deteksjon og

Flere GPS mottakere Referanseklokke

Ønsket funksjonalit Sensor server

Klokker Filtre

Test av lokasjonog hastighetsfilter

Test av klokkemodell og filtre

Observasjon

Konklusjo

Etter innlevering

Bibliograf

Implementasjon

Spoof proof GPS timing A. Schultzen

A. Schultzen

Agenda

ntroduksjon

PS timing tfordringer og

eteksjon og

ttiltak re GPS mottakere

Referanseklokke Implementasjon

Önsket funksjon ensor server rkitektur

> tre t av lol

av Iok Iastigh krivelse

av emodell og

nklusjon

iografi

- -

Ønsket funksjonalitet

- Kunne detektere angrep hurtig
- ► Ha mulighet for å logge data
- Rask og enkel tilgang til innsamlet data
- Enkelt kunne koble til flere GPS mottakere
- Kunne administreres over nettverk
- Konfigurerbar

Spoof proof GPS timing

A. Schultzen

Agenda

Introduksjon

GPS timing

Utfordringer og t Referansetrussel

Deteksjon og mottiltak

Flere GPS mottakere Referanseklokke

Implementasjon Ønsket funksjonalitet Sensor server

Klokken Filtre

Test av lokasjonog hastighetsfilter

Test av klokkemodell og filtre

Observasjon

Konklusion

Etter innlevering

Bibliogra

Sensor server arkitektur

- Mottaker + Raspberry PI = GPS mottaker med nettverkskort = 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 trusle Referansetrusselen

> eteksjon og nottiltak

Flere GPS mottakere Referanseklokke

Ønsket funksjonalit Sensor server arkitektur

Klokkem Filtre

Test av lokasjonog hastighetsfilter

Test av klokkemodell og filtre

Observasjon

Konklusjo

Etter innlevering

5.5..06.4..

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 trusle

Deteksjon og nottiltak

Flere GPS mottakere Referanseklokke

Implementasjon

Ønsket funksjonalitet
Sensor server
arkitektur

Klokkemedell

Test av lokasjonog hastighetsfilter

Test av klokkemodell og filtre

Observasjon

Kanklusian

Etter innlevering

Bibliogra

Implementasjon: Klokkemodell

Spoof proof GPS timing

A. Schultzen

Agenda

ntroduksjon

GPS timing

Utfordringer og trusl Referansetrusselen

nottiltak

re GPS mottaker eranseklokke

nplementasjon

Sensor server arkitektur

Klokkemode Filtre

av lokasjonastighetsfilter

av kemodell og

re pservasion

er innlevering

Bibliografi

Deferences

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 trusle Referansetrusselen

> Deteksjon og nottiltak

Flere GPS mottakere Referanseklokke

Implementasjon Ønsket funksjonalitet Sensor server

> Klokkemodell Filtre

Test av lokasjonog hastighetsfilter

Test av klokkemodell og filtre

Observasjon

Konklusion

Etter innlevering

Bibliograf

Implementasjon: Filtre

Spoof proof GPS timing

A. Schultzen

Agenda

Klokkemodell

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 tru Referansetrusselen

Deteksjon o_l nottiltak

Flere GPS mottakere Referanseklokke

Implementasjon
Ønsket funksjonalitet
Sensor server
arkitektur

Filtre

Test av lokasjonog hastighetsfilter

est av Iokkemodell og Itre

Observasjon

Konklusion

Etter innlevering

Bibliograf

Test av lokasjon- og hastighetsfilter

Spoof proof GPS timing

A. Schultzen

Agenda

Filtre

Oppsett

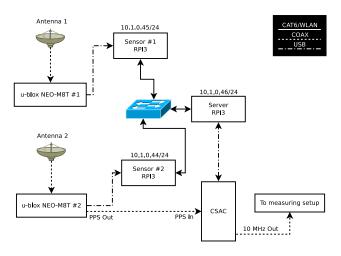


Figure: Oppsett av server og klienter under test

Spoof proof GPS timing

A. Schultzen

Agenda

Introduksion

GPS timing

Utfordringer og trusle Referansetrusselen

Deteksjon o mottiltak

Flere GPS mottakere Referanseklokke

Implementasjon

Ønsket funksjonalitet

Sensor server

Klokkem Filtre

lest av lokasjonog hastighetsfilter Beskrivelse

Test av klokkemodell o filtre

Observasjo

Konklusj

Etter innlevering

Bibliogra

Oppsett

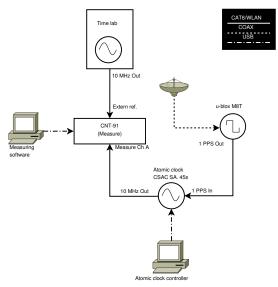


Figure: Oppsett av måleutstyr

Spoof proof GPS timing

A. Schultzen

Agenda

Introduksio

CDC .. .

Utfordringer og trusler

Deteksjon c mottiltak

Flere GPS mottakere Referanseklokke

Implementasjon
Ønsket funksjonalitet
Sensor server
arkitektur

Klokken Filtre

Test av lokasjonog hastighetsfilter Beskrivelse

Test av klokkemodell og filtre

Observasjo

Konklusj

Etter innlevering

Bibliogra

Oppsett: plassering av mottakere

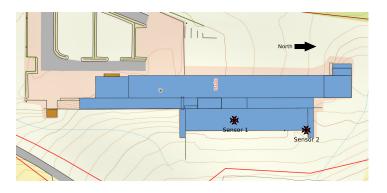


Figure: Plasseringen av GPS mottakere

Spoof proof GPS timing

A. Schultzen

Agend

Introduksjon

Utfordringer og trusler

Deteksjon c mottiltak

Flere GPS mottakere Referanseklokke

Implementasjon
Ønsket funksjonalitet
Sensor server
arkitektur

Filtre

Test av lokasjonog hastighetsfilter Beskrivelse

Test av klokkemodell og iltre

Observasjo

Konklusjo

Etter innlevering

Bibliograf

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

Agenc

Introduksjo

GPS timing Utfordringer og

Referansetrusse

Flere GPS mottaker

Referanseklokke

Ønsket funksjonalit Sensor server

Klokke Filtre

Test av lokasjonog hastighetsfilter Beskrivelse

Test av klokkemodell o

Observasjo

Konklusjo

Etter innleverin

Bibliogra

Observasjon

- ▶ Ingen falske positive
- GPS log korrelasjon
- Server log korrelasjon
- ► Frekvensmåling korrelasjon

Spoof proof GPS timing

A. Schultzen

Agenda

Introduksjo

GPS timi

Utfordringer og tru Referansetrusselen

Deteksjon o mottiltak

Flere GPS mottakere Referanseklokke

Implementasjon

ensor server irkitektur Klokkemodell

Klokke Filtre

Test av lokasjonog hastighetsfilter Beskrivelse

Test av klokkemodell og filtre

Observasjor

Konklusion

Etter innlevering

Bibliograf

Observasjon: Målesystem

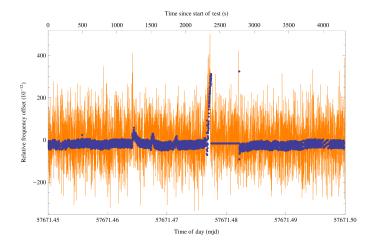


Figure: Måleserie gjort under test av lokasjon og hastighetsfilter

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

Klokken Filtre

Test av lokasjonog hastighetsfilter Beskrivelse

Test av klokkemodell

Observasjon

IZ....LL

Ettor innlovering

Bibliogra

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

Introduksjo

GPS timing

Referansetru

mottiltak

Flere GPS mottakere Referanseklokke

Implementasion

Ønsket funksjonalit Sensor server

Klokkem Filtre

Test av lokasjonog hastighetsfilter

Test av klokkemodell og filtre

Observasjon

Konklusjor

Etter innlevering

Bibliograf

Utførelse

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

Spoof proof GPS timing

A. Schultzen

Agenda

Introduksjon

GPS timi

Utfordringer og trusk Referansetrusselen

Deteksjon o mottiltak

Flere GPS mottakere Referanseklokke

Implementasjon

Sensor server arkitektur

Klokke Filtre

Test av lokasjonog hastighetsfilter

Test av klokkemodell og filtre

Observasjon

Konklusjoi

Etter innlevering

Bibliograf

Observasjon

- ▶ Ingen falske positive
- GPS log korrelasjon
- Server log korrelasjon
- ► Frekvensmåling korrelasjon

Spoof proof GPS timing

A. Schultzen

Agenda

Introduksjo

GPS tim

Referansetrusse

Deteksjon o mottiltak

Flere GPS mottakere Referanseklokke

Implementasjon

Sensor server orkitektur

Klokker Filtre

Test av lokasjonog hastighetsfilter

Test av klokkemodell og filtre

Observasjon

Konklusio

Etter innlevering

Bibliograf

Observasjon

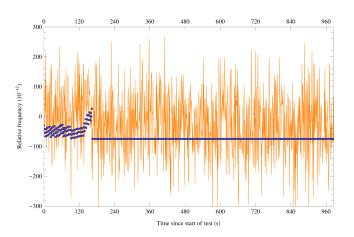


Figure: Måleserie gjort under klokkemodell test

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

Klokker Filtre

Test av lokasjonog hastighetsfilter Beskrivelse

Test av klokkemodell og iltre

Observasjon

Konklus

Etter innlevering

Bibliogra

Konklusjon

Spoof proof GPS timing

A. Schultzen

Agenda

ntroduksjor

Utfordringer og trusl Referansetrusselen

eteksjon og ottiltak

eferanseklokke

Insket funksjona ensor server

itektur okkemodell Itre

av lokasjonastighetsfilter

av emodell og

klokkemodell og filtre Observasjon

ter 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

Spoof proof GPS timing

A. Schultzen

Agenda

Introduksjon

Utfordringer og trusle Referansetrusselen

> Deteksjon og nottiltak

Flere GPS mottakere Referanseklokke

Implementasjon
Ønsket funksjonalitet
Sensor server
arkitektur
Klokkemodell

Test av lokasjonog hastighetsfilter

Test av klokkemodell og filtre

Observasjor

Konklusjon

Etter innlevering

 $\mathsf{Bibliograf}$

Etter innlevering

Spoof proof GPS timing

 $A. \ {\sf Schultzen}$

Agenda

ntroduksjor

GPS timing Utfordringer og

Referansetrusselen

ere GPS mottakere

plementasjon

Ønsket funksjon Gensor server Irkitektur Klakkomadall

kkemodell re

av lokasjonastighetsfilter

av emodell og

okkemodell og tre

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.

Spoof proof GPS timing

A. Schultzen

Agenda

Introduksjon

GPS timing Utfordringer og

Referansetrussele

mottiltak

Flere GPS mottakere Referanseklokke

Implementasjon
Ønsket funksjonalitet
Sensor server
arkitektur

Klokkemo Filtre

Test av lokasjonog hastighetsfilter

Test av klokkemodell og filtre

Observasjon

Konklucio

Etter innlevering

Bibliogra

Bibliografi I



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

Spoof proof GPS timing

A. Schultzen

Agenda

Introduksjon

Utfordringer og trusle

Deteksjon og

Flere GPS mottakere

Implementasjon Ønsket funksjonalite Sensor server arkitektur

Klokkemo Filtre

Test av lokasjonog hastighetsfilter

Test av klokkemodell og filtre

Observasjon

Etter innlevering

.-..-0.-..