

Subscription-based and secure GNSS data transmission via TV satellite links

Harald Gebhard¹, Rafał Mielniczuk^{1,2}

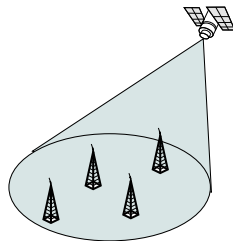
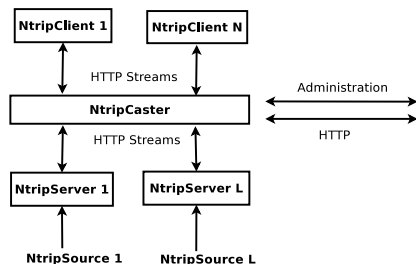
1.Univ. of Applied Sciences, Konstanz

2.AGH Univ. of Science and Technology, Kraków

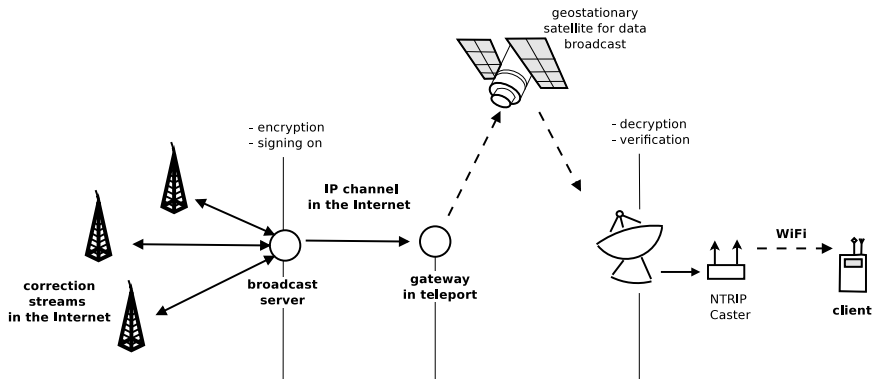
13 March 2012

State of the Art

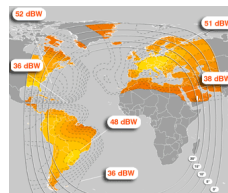
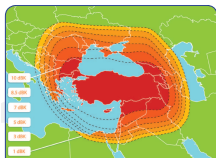
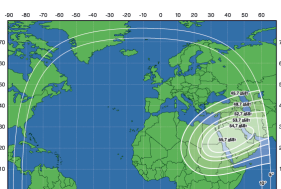
- mobile Internet connectivity
 - NTRIP
 - cheap data transmission
 - requires bidirectional connection (authentication)
 - does not provide data security
 - not available in rural areas
- satellite links:
 - continental signal coverage
 - unidirectional ideal for dissemination to the masses because of cheap reception hardware
 - more expensive than terrestrial links, e.g. 512 kbps - 5000 euro per month



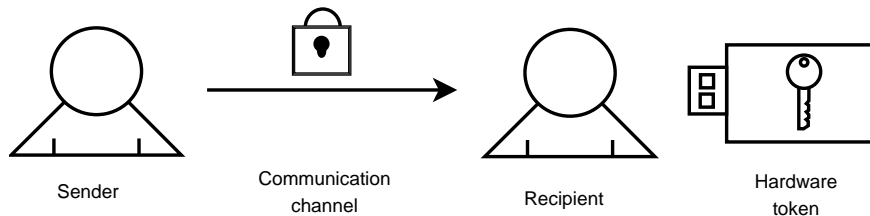
System for GNSS data dissemination via TV satellite links



Some real-world satellite footprints



Main system functions



System advantages:

- any data format support
- no data rate limitations, e.g. 8 bps - ...

Sender requirements:

- data and subscriber management
- data encryption
- replication protection of client's configuration

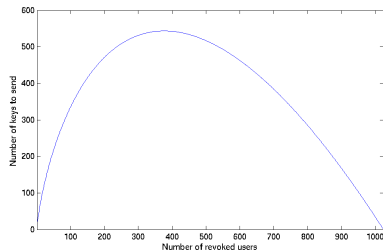
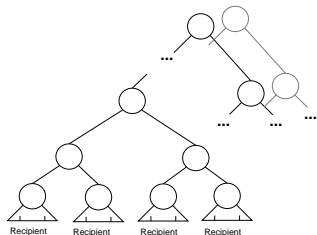
Communication link disadvantages:

- unidirectional
- unreliable
- expensive

Recipient requirements:

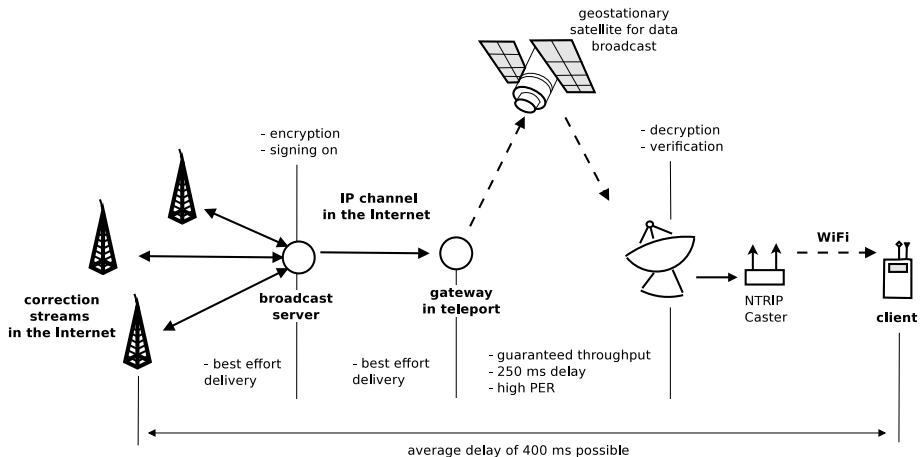
- data authentication and non-repudiation

Encryption and authentication details

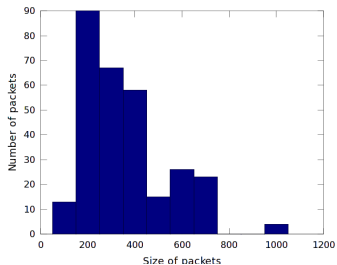
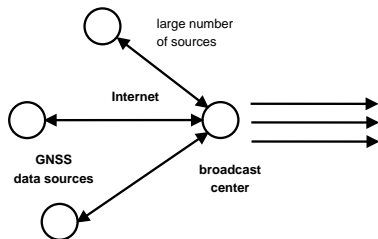


- the Subset Cover framework
 - used in Blu-ray and HD-DVD
 - makes user revocation possible
 - allows for traitor tracing
 - sends encrypted keys and encrypted data
- data encrypted with 128bit AES
- streams arranged in bouquets
- usage of Digital Signature Algorithm and Elliptic Curves Cryptography with a key of length 160 bits

Challenges



Protocol requirements



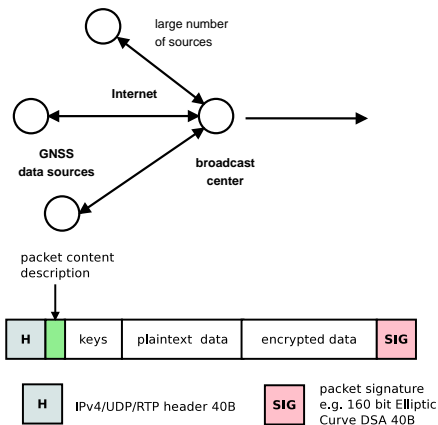
Requirements:

- robustness
- uses IP/UDP stack
- low overhead
- supports large number of sources
- provides synchronization between data and encryption keys

Overhead for single socket-single, single-stream approach:

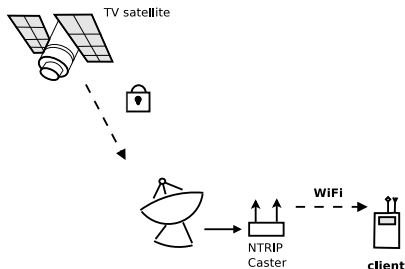
- 16% additional 40B of IP+UDP+RTP headers
- 28% additional 40B of signature

Protocol construction



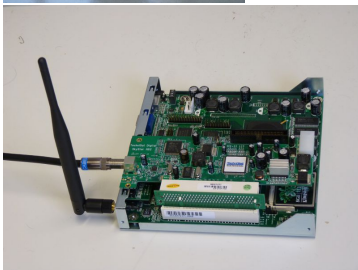
- multiplexes data into cumulative streams
- packets size up to network's MTU
- RTP header used for timing, packets order and sender's identification number encoding
- protocol overhead for the same histogram:
 - 4% (IP+UDP+RTP headers)
 - 6% (with signature)

Mobile TV Satellite Antennas



- automatic satellite acquisition
- require direct line of sight
- required EIRP > 50dBW
- price from 3000 euro
- can already be installed in luxury vehicles

Experimental equipment and setup procedure



exemplary hardware

- orbital 1.0m aluminum dish
- 1m high ground stand, detachable
- Alix 1.D PC Engines, miniITX
- SkyStar HD 2 PCI receiver

setup in few steps

- direct the dish to a satellite
- set up the DVB card
- configure an IP stack
- start the client application

Project status



- system design
- successful implementation
- data delay and integrity tests
- entire system tested in an environment emulating real IP conditions
 - delay
 - throughput limitation
 - packet losses
 - packet reordering
- development of RTCM SC-104 data format compression techniques
- preparations for field tests with a satellite

The End

Thank you for your attention!