Research engineer in embedded software defined radiofrequency (SDR) digital signal processing (DSP)

J.-M Friedt, November 23, 2020

In the framework of the FAST-LAB [1] joint laboratory between the company Gorgy Timing and the Time & Frequency department FEMTO-ST institute as well as the Besançon Observatory, secure and certified time dissemination is being investigated. Time dissemination aims at synchronizing remote clocks for applications ranging from basic science such as Very Large Base Interferometry (VLBI), radioastronomy or comparison of ultrastable clocks, to such applied engineering issues such as synchronizing national and international rail stations or airports. While the targeted accuracy vary widely between these applications, certification and traceability of the timestamp are hardly ever addressed, a rising concern in the context of extensive technologies available to a broader audience. As an example, Global Navigation Satellite Services (GNSS) provide a classical time dissemination solution by sharing the signals from atomic clocks embedded in the space vehicles: while the weak signal reaching the surface of the Earth is easily jammed with trivially visible consequences on the clock locked on such a signal, spoofing is becoming readily available to a broad technical audience with much more serious concerns. Mobile phone networks as well as banking systems currently rely on such time stamping capabilities, with the risk of introducing false timestamp preventing the secure certification of the transactions.

In this context, Software Defined Radio appears as a flexible means to tackle such challenges. The reconfigurable radiofrequency receiver can adapt to the detected signals, while the flexible hardware architecture allows for updating the processing algorithms once threats are identified. The long term stability of digital algorithms is an additional asset to high stability signal dissemination preventing drift over time due to passive component aging.

Time transfer is intrinsically a broadband operation: as opposed to high stability frequency dissemination which aims at preventing communication media property fluctuations from impacting on the frequency (or its integral, the phase) from being disturbed, timestamping a signal requires spreading the stable carrier to a bandwidth about as large as the inverse as the timing resolution. As an example of such an approach, DCF77 timing capability was improved by spreading ten-fold the amplitude modulated carrier emitted from Mainflingen by adding a phase modulation. The implementation of phase modulation as opposed to amplitude modulation also illustrates the improvements in signal processing capability between the initial implementation of DCF77 after the second World War to 1988 when the phase modulation – requiring carrier recovery – was implemented.

Despite this common scheme of carrier spectrum spreading, a multitude of time transfer media are considered, from long range VLF signals (>1000 km) to short ($\simeq$ m) and long range (>100 km) optical fiber and satellite One-Way (20000 km) or Two-Way Time Transfer ($2 \times 36000 = 72000$ km travel paths). In all cases, spectral bandwidth specifications must be met to keep the useful signal within allocated bands. Various strategies for spectrum spreading exist, from pulse emission to frequency sweep or linearly frequency modulated signals, with arguably pseudo-random sequence the best known strategy as documented in the GNSS communication services. While pseudo-random sequences are readily implemented using discrete digital components, the Software Defined Radio (SDR) again provides a flexibility for switching between approaches that are hardly met with hardware implementations.

Nevertheless, except for the VLF signals, the dream of SDR of a full digital processing following the analog to digital conversion is not (yet) accessible with current technology – and might not even be suitable considering the broad part of the spectrum not being addressed by the modulation scheme – and a transposition of the digitally modulated scheme to the radiofrequency or optical carrier is still needed. The **latest generation of radiofrequency frontends provided by Analog Devices**, AD936x, exhibit attractive features such as broad carrier frequencies and wideband modulation schemes. However, the radiofrequency characteristics of these chips relevant to metrological time and frequency transfers are not documented, and should be addressed in this work.

We wish to tackle the following issues:

1. **software implementation of GNSS receivers**, initially aimed at GPS and Galileo and possibly at Beidou, with some consideration for the cryptographic layer aimed at certifying the transactions.

   GNSS is well known to be subject to jamming and spoofing attacks due to the low radiofrequency power reaching the Earth from the Medium Earth Orbiting (MEO – 20000 km altitude) satellites. Having demonstrated spoofing, spoofing detection, and spoofing and jamming cancellation capabilities using a phased array receiver [1], we now wish to

[1] `http://teams.femto-st.fr/equipe-cosyma/new-joint-lab-gorgy-timing`

(a) implement a low power, low footprint embedded GNSS spoofing detector

(b) consider an extended phased array for beamforming in order to cancel multiple spoofing or jamming signal,

(c) generate a 1-PPS (1-Pulse Per Second) output controlled by the GNSS time offset information,

(d) address long term instabilities of the opensource `gnss-sdr` GNSS SDR receiver.

`gnss-sdr` allows for addressing other constellations than GPS L1, but at the expense of much broader bandwidth and processing power not yet accessible to general purpose processors. Acceleration schemes should be envisioned to address real time analysis of GPS L5 [2] or Galileo E5, possibly by merging the FPGA front end and the general purpose processing unit in a single high-end Zynq System on Chip.

2. **Composite clock aimed at identifying inconsistencies in the timing signals**, hinting at some spoofing of one of the signals. While VLF signals require huge infrastructures and power for wide-range spoofing, its timing capability is far poorer than those achieved using the microwave carriers of GNSS constellations which is however readily attacked with a compact infrastructure: combining both timing information should help identify attacks.

3. On a **wired time transmission level, the openhardware/opensource WhiteRabbit** provides an implementation of PTP being investigated for long range time dissemination. Its security and vulnerability to spoofing is currently unknown, and would deserve investigation. Most significantly, we aim at **using White Rabbit** as a synchronization scheme for distributed radiofrequency data acquisition (distributed RADAR, distributed GNSS receiver) or synthesis. Indeed while a local attack is readily feasible, a long range attack is much more complex to setup and spreading receivers will help identify inconsistencies in the collected radiofrequency signals. In this context, synchronizing Ettus Research X310 USRP on the synchronization signals provided by the White Rabbit networks appears as an attractive solution. We wish to further assess how new clock distribution chips such as Analog Devices AD9548 might meet the requirements of coherent frequency distribution.

Available digital hardware includes most common analog to digital and digital to analog radiofrequency frontends, multitude of FPGA and their SoC extension mostly oriented towards Zynq-based platforms. This program is supported by the OscillatorIMP platform providing the high stability signal sources combining Quartz, Cryogenic Sapphire Oscillators (CSO), Hydrogen Masers (HM) and Cesium Clocks. A commercial Two-Way Time Transfer setup is currently functional, and hardware for deploying a WhiteRabbit network is available.

Pre-requisites: at least two of the following pre-requisites must be met to apply

- familiar with **embedded system** development under **GNU/Linux** (Yocto, buildroot) is mandatory since all work is completed on this operating system, whether on the host or target computers,
- **FPGA** programming (VHDL or Verilog),
- discrete time digital **signal processing** (software defined radio, GNU Radio)

Location: FEMTO-ST institute, Time & Frequency department, Besançon, France

Duration: 1-year renewable

References

[1] W. Feng, J.-M Friedt, G. Goavec-Merou, F. Meyer, *Software Defined Radio Implemented GPS Spoofing and Its Computationally Efficient Detection and Suppression*, IEEE Aerospace and Electronic Systems Magazine (2020)

[2] J.-M Friedt, W. Feng, D. Rabus, G. Goavec-Merou, *Real time GNSS spoofing detection and cancellation on embedded systems using software defined radio*, Proc. EuCAP 2021