32nd URSI GASS, Montreal, 19-26 August 2017

Linkedclocks for a robust solution of GNSS timing receivers

Javier Díaz [(1)], Eduardo Ros [(1)], Rafael Rodríguez [(2)], Benoit Rat [(2)], Alejandro González [(2)]
(1) Seven Solutions/ U. Granada, Spain, http://www.sevensols.com/
(2) Seven Solutions, Spain, http://www.sevensols.com/

1. Abstract

GNSS is vulnerable due to the low power satellite signal reception that can be easily jammed with domestic equipment (accidental and malevolent local events). With this disadvantage in mind and at least 17 of 21 types of infrastructures classified as critical by government authorities require timing information, most of them by GNSS timing receivers. There are a requirement of make the time obtained more robust against jamming. The way to make the reception of GNSS time can now be done linking the time signals from scattered sources (as GNSS receivers located at medium distance from each other). This solution is scalable in the number of GNSS receivers that can be redundantly used and the distance (up to 100Kms) between them. Its regular self-calibration functionality facilitates its deployment providing a full and accurate time integrity solution. Our approach is based on IEEE1588v2 and can take advantage of high accuracy profiles as White-Rabbit to enhance the scalability and robustness of the solution. This allows time-critical nodes to access a distributed timing network linking three or more GNSS receivers without affecting significantly the time accuracy in the time transfer stage.

2. Introduction

Many safety critical infrastructures are in fact time-critical infrastructures. Some of them as the Smart Grid for power distribution have elements distributed over very wide areas. In order to allow efficient data analysis, monitoring and forensic analysis (in the case of a black out event in the framework of the Smart Grid) all these elements produce data that need to be time-stamped with respect to a global time reference. The most widely approach for providing time to different elements of a distributed facility (distributed instrumentation) is to use GNSS time receivers (because they provide a global time reference widely available) and distribute it locally using IEEE1588v2 (Precision Time Protocol). But this approach is highly vulnerable.

a. GNSS time receivers

For the different applications that require accessing to a global time reference (traceable to Coordinated Universal Time, UTC) the typical approach is to use GNSS time receivers. Different institutions in the world (usually the timing labs of some national metrology institutes) actively work on continuously calibrating the atomic clocks of the satellites (constituting the GNSS satellite constellation) towards achieving (and tracking) a tight synchronization between the different atomic clocks at the different satellites. Thus, we can see the clocks at the satellites of a GNSS system as a "globally accessible clock", a time reference traceable to UTC can be received through GNSS time receivers (as the case of Galileo constellation).
The main advantage of this approach is that it is cost-effective (GNSS time receivers are not very expensive equipment and easy to install). But the approach has also several disadvantages. The satellite signals are sent from satellites powered by solar panels and very far away above the atmosphere. This translates in satellite signals being weak when they are received at the surface. This represents the main drawback of this approach because of its vulnerability to jamming events. It is easy to cause interferences on this weak satellite signals at the surface with cheap and easily available domestic equipment.

Figure 1. GNSS jammer from 49$

Other factors such as the complex operational tasks of the satellite constellation (that in some cases have led to disturbances in the satellite based time reference (for instance the 13 microsecond's error caused by the replacement of a satellite of the GPS constellation on the 26th January 2016 [1, 2, 3]). Also global events like a solar flare that might affect more or less dramatically the satellite constellation and constitute a real thread (more at a global scale [4, 5], as called by the Department of Homeland security a "low probability but high-impact event") motivate preventive investment and actions in contingency or complementary approaches.

b. Time distribution through Precision Time Protocol (PTP, IEEE1588v2)

From a GNSS receiver or any other primary time reference, timing can be distributed locally using IEEE1588v2 protocol. But the accuracy depends on careful calibration (to compensate for factors such as links asymmetry), it degrades with distance and number of hops. This approach is not easy to deploy (it is not a turn-key solution) and is not scalable at high accuracy. This is why the protocol is now being revised for a new version, with a specific High Accuracy (HA) profile whose current version is heavily based on the White Rabbit PTP (WRPTP) [6].

3. WHITE RABBIT PTP FACILITATES GNSS RESILIENCE

White Rabbit PTP [6, 7] allows ultra-accurate and deterministic time distribution over long distances [8, 9]. This allows accessing to different sources of reliable time through optical fiber time distribution. In the long term, we can think of a constellation of atomic clocks (similar to the ones at the GNSS satellites) distributed at different sites in the surface and linked through high accuracy WRPTP links.

But even now, we can use the extrem accuracy of WRPTP to deploy redundant GNSS time receivers to implement a solution resilient to local jamming attacks (in fact this kind of attacks are typically local). WRPTP allows subnanosecond accuracy. Since GNSS time receivers provide time with significantly less precision (typically from several nanoseconds to tens of nanoseconds), GNSS time can be distributed through optical fiber with WRPTP without degradation. We can use a set of GNSS receivers distributed at certain distance from each other and linked through WRPTP over optical fiber. With equipments capable of switch over, i.e. capable of switching from one time source to another one depending on their quality characteristics the time-critical elements will rely on a constellation of GNSS receivers (each one placed far away from each other) instead of a single point of failure (being the most probable failure local jamming and spoofing attacks).

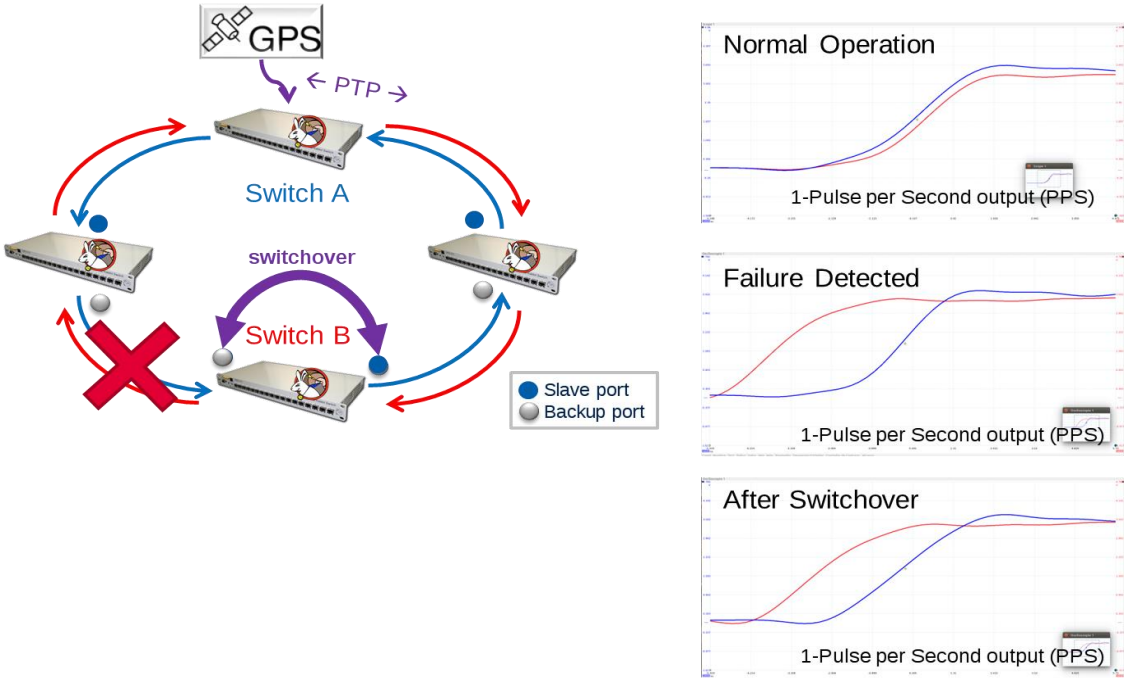

Figure 2. Scheme of robust linked clocks

With this approach, the time-critical elements of the infrastructure receive the time from a "virtual clock" that is based on a constellation of time sources linked through WRPTP (to avoid loss of accuracy at the time distribution process). The constellation of time sources can be some redundant GNSS receivers (at a certain distance from each other) not to be affected by local jamming and spoofing, and can also include hold over clocks.

From a more general point of view, WRPTP allows sharing time sources making any time critical infrastructure more resilient. More specifically, using several GNSS receivers appropriately distributed at secured locations and linked through WRPTP increases resilience to local jamming and spoofing attacks. This is illustrated in Fig. 2.

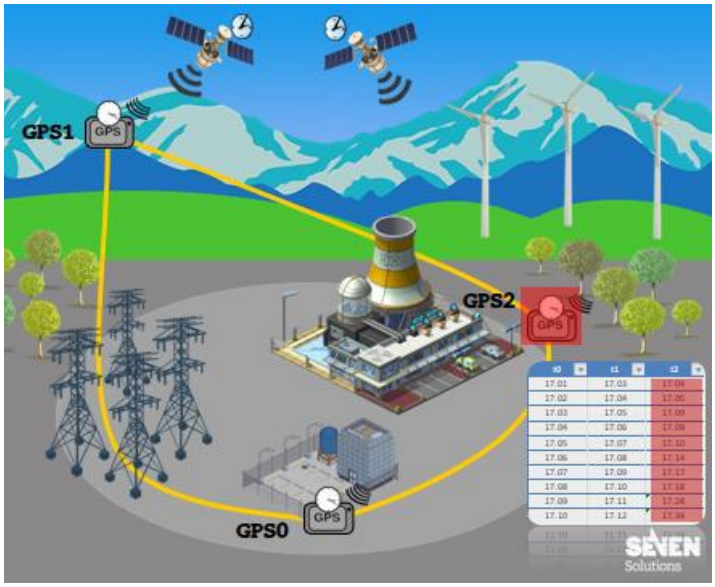

Figure 3. Several GNSS receivers are linked through WRPTP over optical fiber

If one of the GNSS receivers fails to provide reliable timing, the ultimate receiver equipment shall switch over to other reliable time source (in this case other GNSS receivers not affected by the local jamming or spoofing attack).

4. Examples

In the previous section we show the possibilities of the linkedclocks for robust GNSS timing transport. The applications are endless, for example:

- Network and phase synchronization in wireline and wireless networks (Communications/IT Sectors) used by multiple critical infrastructures.
    a. The telecom equipment developers and integrators consider timing and synchronization one of the critical issues to improve current telecom service capabilities. Particularly indoor cells face the problem of lack of GPS time signal.
    b. Accurate Time transmission becomes mandatory to allow these indoor cells to be well synchronized with respect to the global telecom infrastructure.
    c. Next generation of 100G links based on optical fibers imposes demanding timing requirements in order to monitor network traffic to guarantee the QoS (Quality of Service).
    d. Proper identification of the networks bottlenecks translate in a more effective and reliable service. It is also key for new services based on guaranteed latency, legal timestamping, network infrastructure virtualization or secure (encrypted) networks links.
    e. The most optimistic solutions request 2ns timestamps. Our solutions are able to provide accurate latency measurements with sub-ns accuracy.

- Phase synchronization in Electric Power, Nuclear Power, and Hydroelectric power sectors.

- Process scheduling, control, and synchronization in Oil and Natural Gas/Chemical/Critical Manufacturing/DIB sectors.

- Precise time stamping of data, transactions/Finance/Postal and Shipping sectors.
    a. MiFID (II) new directive starts in 2017 including new timing demands.
    b. Legal time distribution. The reliable **WR** timestamp makes possible the legal certification of financial transactions.

- Airports, GNSS control centers, Space, Defense, …

5. Concusion

Advanced WRPTP allows ultra-accurate (subnanosecond) time distribution. This makes possible distributing GNSS time over optical fiber without degradation. Jamming and spoofing attacks are usually local; they cause interferences to a GNSS receiver at a local scale.

A solution based on a set of GNSS receivers placed at secured locations (complemented with holdover clocks) is resilient to local jamming and spoofing attacks. The final time receivers will rely on a virtual clock based on these different time sources. It shall be able to switch from one primary time source to another in case of failure.

Furthermore, since now, with WRPTP, atomic clock accurate timing can be distributed; expensive atomic clocks at different strategic locations can be shared and used as accurate and stable hold over time sources. Still GNSS would be used as primary time sources for many time-critical infrastructures because their timing is traceable to UTC and facilitates matching time over wide areas.

In this way, GNSS time receivers (with UTC traceability) can be now redundantly used with other GNSS receivers (at secured locations) and also complemented with expensive holdover clocks. The cost of these holdover clocks can be shared, since their time can now be distributed also to different facilities.

6. References

1. J. Saarinen. "Satellite failure caused global GPS timing anomaly", itnews. 28th January 2016. http://www.itnews.com.au/news/satellite-failure-caused-global-gps-timing-anomaly-414237
2. "GPS Experiences UTC Timing, IIF Satellite Launcher Problems", Inside GNSS, http://www.insidegnss.com/node/4829 . 28th January 2016.
3. Chronos. "GPS SVN23 Timing Anomaly 26 Jan 2016", http://www.chronos.co.uk/index.php/en/resources/case-studies/351-cs-support/1611-gps-svn23-timing-anomaly-26-jan-2016
4. T. Johnson, "Super-Powerful Solar Storms Could Knock Out Communications, GPS, Power Systems With Only a Few Hours' Warning", The Weather Channel, 31st July 2015. https://weather.com/science/space/news/solar-storm-1859-less-than-day-to-prepare-global-disruption-impact
5. IEEE 1588TMStandard for A Precision Clock Synchronization Protocol for Networked Measurement and Control Systems. https://ieee-sa.imeetcentral.com/1588public/
6. http://sevensols.com/index.php/projects/white-rabbit-technology/
7. J. Díaz and E. Ros, "Scalable and Long Distance, Deterministic Time Transfer", ITSF 2016, Prague, November 2016.
8. http://www.mikes.fi/mikes/Esitteet/TopFive2014/TopFiveSpring_2014_www.pdf
9. A. Wallin, "Comparing H-masers over a 280 km White Rabbit-PTP link", ITSF 2016, Prague, November 2016.