Frequency & Time

Proceedings of the 5th IFSA Frequency & Time Conference

20-22 September 2023

Funchal (Madeira Island), Portugal

Edited by Sergey Y. Yurish

IFSA Publishing

Sergey Y. Yurish, *Editor*
Frequency & Time
IFTC' 2023 Conference Proceedings

E-mail (for orders and customer service enquires): ifsa.books@sensorsportal.com

Visit our Home Page on http://www.sensorsportal.com

ISBN: 978-84-09-53747-1
BN-202120916-XX
BIC: TBMM

Contents

Foreword

On behalf of the IFTC' 2023 Organizing Committees, we introduce with pleasure these proceedings devoted to contributions from the 5th IFSA Frequency & Time Conference held in Funchal (Madeira Island), Portugal. The conference is organized by the International Frequency Sensor Association (IFSA) - one of the major professional, non-profit association serving for industry and academy more since 1999 in technical cooperation with *IFSA Publishing, S. L. (Barcelona, Spain).*

The proceedings contain all papers of both: oral and poster presentations. We hope that these proceedings will give readers an excellent overview of important and diversity topics discussed at the conference.

We thank all authors for submitting their latest work, thus contributing to the excellent technical contents of the Conference. Especially, we would like to thank the individuals and organizations that worked together diligently to make this Conference a success, and to the members of the International Program Committee for the thorough and careful review of the papers. It is important to point out that the great majority of the efforts in organizing the technical program of the Conference came from volunteers.

Prof., Dr. Sergey Y. Yurish
IFTC' 2023 Chairman

(001)

A Novel Direct Digital Phase Comparison and Phase-locked Loop Technology between Complex Phase Change Signals

Wei Zhou, Zhiqi Li, Tiangen He and Zhe Tan
School of Electro-Mechanical Engineering, Xi'dian University, Xi'an 710071, Shaanxi, China
Tel.: 13892861331
E-mail: wzhou@xidian.edu.cn

Summary: The common phase relationship of signals with different frequencies is reflected by the least common multiple period T_{minc} between signals and a series of related time-frequency parameters. For sinusoidal waveforms, it is always possible to select the linear phase change value for digital voltage sampling. The phase difference does not show a significant pattern of change within the T_{minc} of the two compared frequency signals. But at intervals of T_{minc}, there are a large number of continuous phase changes. There is a linear region of voltage/phase difference value at the point where the phase of the sine signal crosses 0. The implementation of direct phase comparison and locking between different frequency signals in this article is based on the feedback control of continuous sampling phase changes between T_{minc} of complex frequency signals, which is the working foundation of the new phase-locked loop. The digital AD conversion and direct phase processing of frequency signals such as 12.8 MHz, 10.23 MHz, 4.43361875 MHz and much more frequencies were locked, and the accuracy of the locked frequency reached the ideal nominal frequency value, while the frequency stability was significantly improved. This method is also used to improve the frequency link of the active hydrogen atomic clock circuit, greatly simplifying the system hardware and improving the system's technical specifications.

Periodic signals are characterized by greatest common factor frequency f_{maxc}, least common multiple period T_{minc}, equivalent phase detection frequency f_{equ} and the quantized phase shift step value Δ P between two frequency signals. The phase difference varies periodically in T_{minc}, and at the corresponding moments on multiple T_{mincs} is continuous. For example, T_{minc} = 2.5 μs between 12.8 MHz VCO and 10 MHz clock sampling signal frequency, and ΔP = 3.125 ns, f_{maxc} = 400 kHz, f_{equ} = 32*25*400 kHz = 320 MHz. With 2.5 μs as sampling cycle time, and only the voltage/phase difference that is closest to the 0-phase difference in the linear segment of the signal is selected, ΔP = 3.125 ns ensures appropriate sampling and control of change areas. Using 16-bit AD, the measurement resolution theoretically guarantees 0.1 ps. The microcontroller communicates with the FPGA, to calculate the collected phase values that have been converted into digital quantities, fit the linear phase change rate, and adjust the frequency of the crystal oscillator through a DA converter based on the voltage control sensitivity of the crystal oscillator. The achievement of controlling its frequency value at the nominal value and the conversion accuracy of the DA converter ensure the frequency stability index of the controlled crystal oscillator.

For more complex frequency relationships, only when ΔP is too fine and the stability of phase locking is affected can ΔP and T_{minc} be adjusted by dividing the clock signal. The most important application of this method is in optimizing the frequency link of active hydrogen atomic clocks.

Keywords: Phase comparison, PLL, Least common multiple periods, Direct digital, Phase shift step, AD conversion.

1. Introduction

Although traditional phase concepts and processing methods have achieved many achievements in understanding phase over the years – higher measurement resolution, faster response time, and the need for a linearized expression. The methods of pulse filling and pulse averaging have insufficient resolution and set many limitations for applications [1, 2]. Especially for a wide range of frequency signals, the processing route may not necessarily be reasonable. Due to the fact that phase discriminators can only be used conceptually for phase comparison between signals with the same frequency nominal value, the locked in oscillator must undergo frequency division, doubling, or even more complex frequency transformations. The more complex the frequency relationship, the more complex this transformation becomes [1, 2]. The frequency link circuit of an active hydrogen atomic clock is a typical example. In order to detect and lock phases at the same nominal frequency, a conversion chain composed of multiple complex frequency conversion circuits has to be used to create phase comparison conditions [3].

The traditional phase-locked loop technology is essentially a narrowband processing technology, but with the progress of science and technology, in many cases, such as navigation, communication, radar, precision instruments, electronic engineering, and metrology technology, the frequency of the locked object is different from the reference frequency signal, and even the frequency relationship is very complex. For example, the clock and frequency standards in the above fields often encounter frequencies such as 12.8 MHz, 10.23 MHz, 16.384 MHz, 32.768 MHz, 4.43361875 MHz, and some specialized instruments such as single sideband phase noise measurement systems also require the collection of phase fluctuations of the measured signal frequency that continuously change over a wide frequency range. So, it is meaningful to explore the digital direct phase measurement and phase locking methods under this

complex frequency relationship. And with its implementation, a large number of technical indicators can also achieve breakthrough changes.

The importance of this paper lies in demonstrating and experimentally verifying that the phase change information of the measured signal can be directly collected and all time-frequency parameters can be measured and controlled under any frequency relationship. Due to the more abundant phase information under complex frequency relationships [4], the main task of a phase-locked loop is to perform reasonable phase sampling rather than frequency transformation. From this, a series of new technologies and products can be derived.

2. Regular Phase Characteristics Between Frequency Signals with Different Nominal Values

Over the years, our extensive previous work on the definition of parameters related to the periodic interrelationships between signals of any frequency has been the basis for analyzing and processing phase changes between them [4, 5]. In recent years, the understanding of the original parameters such as the minimum common multiple period T_{minc} has been further deepened, especially the study of the inherent periodic linear phase change region of the most commonly used sine wave signal, which has formed favorable conditions for measurement and control. Fig. 1 is a description of the phase difference variation in T_{minc} between signals under complex frequency relationships.

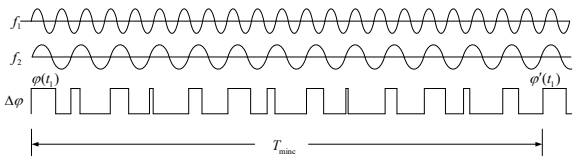


Fig. 1. Phase difference variation in T_{minc} under complex frequency relationships.

In the field of time-frequency measurement and control, periodic signals are the most common standard signals and measured signals. Therefore, it is often necessary to use parameters such as maximum common factor frequency $f_{\max c}$, minimum common multiple period $T_{\min c}$, and equivalent phase detection frequency f_{equ} to describe the mutual characteristics between periodic signals. The $f_{\max c}$, $T_{\min c}$ and f_{equ} between periodic signals f_1 and f_2 are [4, 5]:

$$\begin{aligned} &f_1 = A \cdot f_{\max c}\ , f_2 = B \cdot f_{\max c}, \\ &T_{\min c} = \frac{1}{f_{\max c}}, \\ &f_{equ} = ABf_{\max c}, \end{aligned} \tag{1}$$

A and B are coprime positive integers. The complexity of the phase change between two frequency signals is closely related to the A and B magnitude and specific numerical situation of the values.

$$\Delta P = 1/ABf_{\max c}, \tag{2}$$

The frequency f_{equ} here is referred to as the equivalent phase discrimination frequency [4], and ΔP is referred to as the quantization phase shift resolution between two frequency signals [5], which is also the step value of the quantization phase difference. There are only B situation where the phase difference between f_1 and f_2 exists within one T_{minc}, as follows:

$$\begin{bmatrix} \Delta\varphi_1 \\ \Delta\varphi_2 \\ \vdots \\ \Delta\varphi_i \\ \vdots \\ \Delta\varphi_B \end{bmatrix} = \begin{bmatrix} n_1 \\ n_2 \\ \vdots \\ n_i \\ \vdots \\ n_B \end{bmatrix} T_1 - \begin{bmatrix} 1 \\ 2 \\ \vdots \\ i \\ \vdots \\ B \end{bmatrix} T_2 \tag{3}$$

In the formula, the period of f_1, f_2 is T_1, T_2, $\Delta\varphi_1$, $\Delta\varphi_2, \ldots \Delta\varphi_i, \ldots \Delta\varphi_B$ is the phase difference between f_1 and f_2 at each f_2 periodic phase feature point respectively, and the magnitude is represented by the pulse width in Fig. 1. The phase difference at f_2 any phase feature point is:

$$\Delta\varphi_i = n_i T_1 - iT_2 \tag{4}$$

Within a T_{minc}, $0 \le \Delta\varphi_i \le T_2$ and $\Delta\varphi_1$, $\Delta\varphi_2, \ldots \Delta\varphi_i, \ldots \Delta\varphi_B$ are not equal to each other.

The phase differences of corresponding multiple T_{minc} intervals are continuous respectively, as $\varphi(t_1)$ and $\varphi(t_1')$ shown in Fig. 1.

As the phase comparison time of the two signals extends, formula (2) evolves into a parallel subgroup of multiple T_{minc} that differ from each other. Corresponding different $\Delta\Phi_i$ is continuous in phase at intervals of T_{minc} and varies according to frequency fluctuations. This is also the basis for considering phase processing between signals of different frequencies. Selecting rows with linear phase changes for sampling and calculation can provide a basis for measurement and control. From the perspective of phase analysis, there are multiple "synchronous" states of each phase value at the minimum common multiple period interval for specific two frequency signals regarding the specific phase change states between different frequency signals. This is exactly what is unique to the new different frequency signal phase analysis. That is to say, the values of A and B within the minimum common multiple periods remain unchanged, the minimum common multiple periods

remain unchanged, and the quantization phase step value ΔP remains unchanged after the signal is locked in phase with each other.

3. Introduction to the Composition of New Processing Systems

3.1. Introduction to Digital Direct Phase Comparison with Wide Frequency Range

The foundation of its work is Fig. 1 and Formula (2), as well as the key to sampling and processing based on Tminc. This is also due to the existence o f a linear region of phase changes that can be captured with a reasonable Tminc between a wide range of different frequency signals, and this linear region is often able to be adjusted reasonably. Although it is also possible that the Tminc may appear too long for certain frequency points, resulting in long intervals between specific linear segments and too small quantization phase step values [6]. However, this situation can be achieved by adjusting the frequency of the reference signal or selecting several frequency standards signals with different nominal frequency values [7]. These are all beneficial for measuring over a wide frequency range.

Fig. 2 is a block diagram of a digital phase comparison system between signals based on complex phase change relationships [7]. In practical applications, the frequency division coefficient of the reference clock and whether frequency division is necessary should be determined based on the relationship between the clock frequency and the frequency of the measured signal.

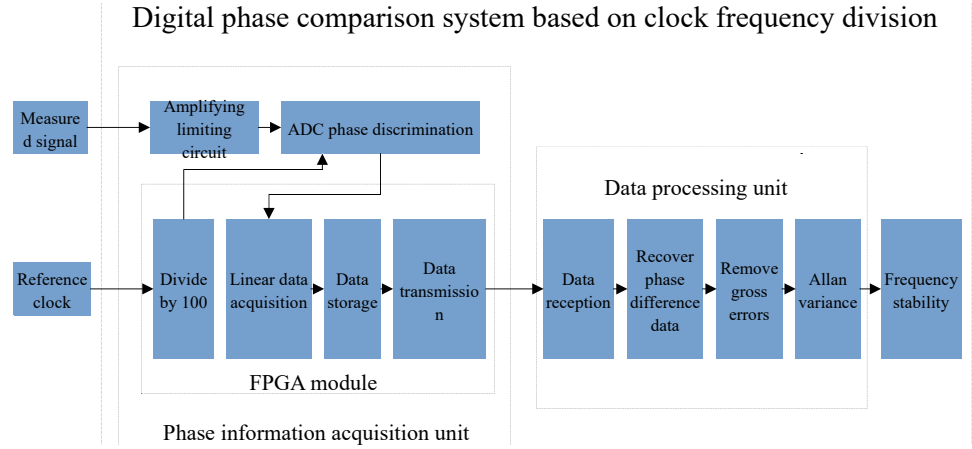


Fig. 2. Design of a digital phase comparison system between signals based on complex phase change relationships.

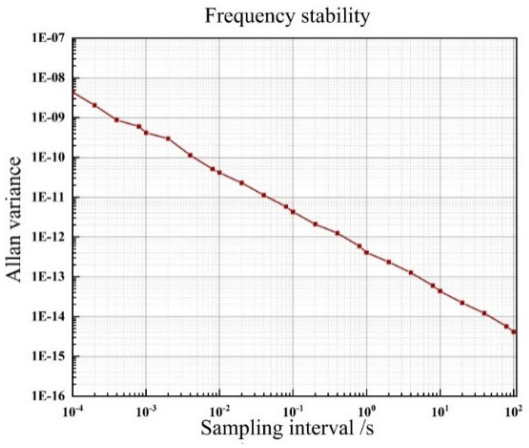


Fig. 3. Frequency stability of self-calibration experiment with the phase comparison system.

In the mutual comparison experiment in Fig. 4, the 10.23 MHz signal generated by the OCXO-PIOLTC2X crystal oscillator was selected as the measured signal, and the actual second level stability of the crystal oscillator was 1E-11. Perform mutual comparison experiments using the digital phase comparison system designed in this article, and calculate the frequency stability of 100 μs , 1 ms, 10 ms, 100 ms, 1 s, and 10 s, as shown in the Fig. 4 The measurement results are true and reliable.

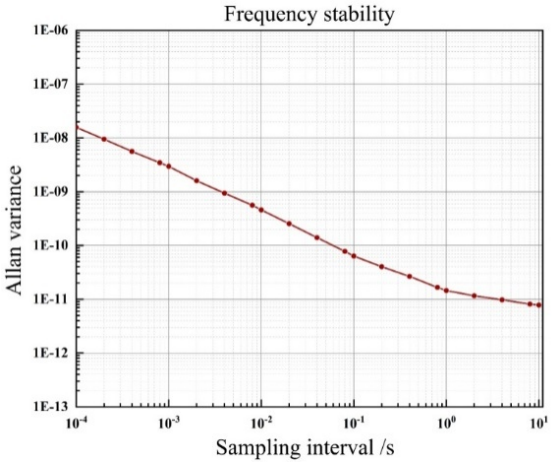


Fig. 4. Frequency Stability Curve of Phase Comparison System for Mutual Comparison Experiment

3.2. Digital Direct Phase Locked Loop Between Arbitrary Frequency Signals

One important aspect of the phase-locked loop between signals of different frequencies is the working steps of the phase-locked loop: (1) calculating and determining T_{minc} between signals; (2) Calculate the quantization phase step value ΔP between two signals and check if it is appropriate; Otherwise, adjust the frequency division of the clock signal (including the frequency division in software processing); (3) Set the voltage/phase difference extracted by the AD converter according to the size of ΔP; (4) Determine and extract the phase difference within a ΔP near the linear region of the 0 phase difference; (5) Calculate the change in phase difference ΔT and the relative or additional relative frequency difference $\Delta f/f = \Delta T/T_{minc}$ at intervals of T_{minc}; It can also be calculated using multiple T_{minc} times as cycles; (6) Calculate the control voltage change value for the controlled crystal oscillator based on the phase difference change and the voltage control sensitivity of the controlled crystal oscillator; (7) The control voltage is used to complete one cycle of voltage controlled crystal oscillator control. If necessary, monitor the T_{minc} of the working cycle. The specific method is to count the number of clock signals between two adjacent voltage acquisition values (in the linear region), and calculate the value of T_{minc} based on the clock cycle.

The digital phase-locked loop designed above can be quickly locked and has high phase-locked accuracy, but its capture range appears narrower for ordinary frequency signals. The maximum phase shift adjustment capability of this digital phase-locked loop is ±ΔP/2. Once the phase jitter of the input signal exceeds this range or the frequency shifts, the phase-locked loop cannot automatically complete capture locking. Therefore, if it is an ordinary frequency signal, an extended design is required for this design. However, for crystal oscillator signals with high stability requirements, it has been proven through experiments that expansion measures are not necessary.

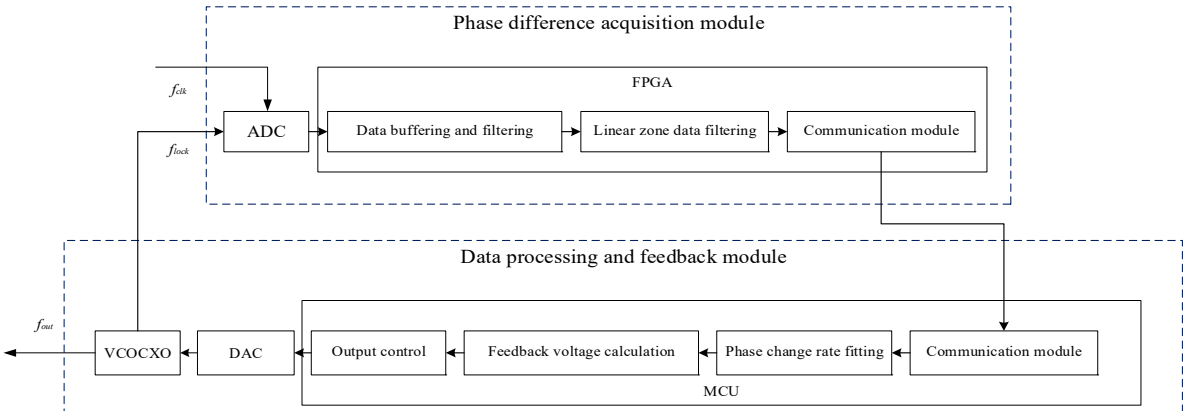


Fig. 5. Design block diagram of a digital phase-locked loop system between different frequencies.

4. Experiments, Analysis and Prospects

For the comparison and digital sampling between stable high-precision reference signals and controlled signals, the low-frequency clock still ensures that one of the clock sequences is collected in the linear region and has uniqueness [8]. That is, one clock cycle corresponds to the cycles of multiple incomplete measured signals, but the basic law of signal phase change within T_{minc} remains unchanged.

Here, a 12.8 MHz high stability voltage-controlled crystal oscillator was selected as the measurement and control object locked by a phase-locked loop. The parameters between 12.8 MHz and 10 MHz clock frequencies are T_{minc} = 2.5 μs, f_{maxc} = 400 kHz, f_{equ} = 32*25*400 kHz = 320 MHz; ΔP = $1/f_{equ}$ = = 3.125 ns. It can be seen that there are only 25 clock sampling signals in a T_{minc}. Therefore, signal processing is relatively simple. According to the principle of uniformly sampling the phase of the measured 12.8 MHz signal within T_{minc}, it is ensured that the 3.125 ns specific phase step occurs in the linear region of phase change within the full cycle phase range of 1/12.8 MHz = 78.1 ns. Direct AD sampling is used to extract and calculate the linear variation data as shown in Fig. 6 at intervals of Tminc, and feedback control is used to achieve phase locking of the highly stable crystal oscillator.

Fig. 6 is a schematic diagram of the voltage/phase change sampling results between signals to be measured and controlled at 12.8 MHz or 10.23 MHz and using a 10 MHz clock signal, in the case of digital sampling. Of course, the number of clocks collected within T_{minc} under the two tested frequencies is significantly more than that in the figure (for example A = 32, B = 25). From the linear relationship between sampling voltage change and phase difference, it can be seen that at the beginning of each T_{minc} selected in the figure, the phase difference of the measured signal is close to the zero-phase value. That is, the linear region of the phase change of a sinusoidal signal. In the case of open loop pure measurement, due to the

wide range of phase changes between signals, it is possible to switch between linear regions. However, in the operation of the phase-locked loop, due to the feedback control of the tested oscillator, the variation range of the sampling voltage/phase difference between signals operating in the linear region is very small. So, there is no need to consider the possibility of switching between sampled values.

For the most commonly used 10.23MHz VCXO in communication as the measured and phase-locked control signal, T_{minc} between 10.23 MHz and 10 MHz frequencies is 100 μs; f_{maxc} = 10 kHz; f_{equ} = 1023*1000*10 kHz = 10230 MHz; ΔP = $1/f_{equ}$ = = 97.75 ps. Here, as a sampling interval control of 100 μs, the time for T_{minc} is appropriate. However, the 97.75 ps value, which serves as the sampling flag for the linear region, is too small, which is not conducive to the operation of the system's software and hardware.

When ΔP is too fine and the stability of phase locking is affected, the system can work reasonably by adjusting ΔP and the number of sampling clocks in T_{minc} by dividing the clock signal. At this time, for the ΔP value at 10.23 MHz, the ΔP and T_{minc} before the clock signal division are 97.75 ps and 100 μs, respectively. This inspection setting range is too narrow (related to ΔP), which is not conducive to the stability of system operation. At the same time, in T_{minc}, direct sampling with too many clock signals (1000 in this case) may not necessarily be conducive to stable operation and complex processing. After dividing the clock signal at 10 MHz, such as 50 division, ΔP and T_{minc} are 4.89 ns and 100 μs respectively. The number of clock signals in T_{minc} is 20 (corresponding to the low-frequency clock sampling to 1023 measured signal cycles), reduced the difficulties in handling. Of course, the frequency division ratio can also be adjusted according to the actual situation, more or less.

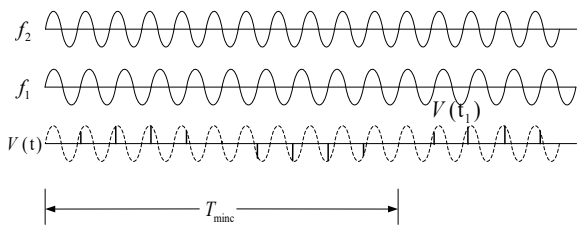


Fig. 6. Sampling effect of voltage/phase change under the condition of monotonic phase difference change within T_{minc}.

For the ΔP value at 16.384 MHz, the ΔP and T_{minc} before clock signal division are 97.7 ps and 62.5 μs respectively. In a T_{minc}, the number of clock signals for direct sampling is 625. After dividing the clock signal at 10 MHz, such as 25, ΔP and T_{minc} are 2.44 ns and 62.5 μs respectively; The number of clock signals is 25 (corresponding to 1024 cycles of the measured signal). This also alleviates the difficulties in handling.

The above is an analysis of the phase-locked loop operation of three locked oscillators with different frequencies. The most classic application of this new technology is in the improvement of the frequency link part of the active hydrogen atomic clock [8]. The frequency conversion link of the traditional hydrogen atomic clock phase-locked loop is very long [1, 9]. The following experiment proves that using T_{minc} between signals as the processing time constant can achieve better results.

Fig. 7 is a block diagram of an improved hydrogen atomic clock for digital phase-locked loops between complex frequency signals. Compared with traditional methods, the hardware of the system has been greatly simplified [8]. Here, the 405750 Hz signal obtained after primary mixing in the active hydrogen atomic clock system is directly coupled with the 10 MHz crystal oscillator in the output part of the atomic clock through a digital direct AD converter to form a phase-locked loop, which can obtain the error signal of the 10 MHz crystal oscillator outputted by this phase-locked loop and form a control voltage for the oscillator itself based on the voltage control sensitivity of the oscillator, forming a control loop. The mutual time-frequency parameters between the 405750 Hz reference signal obtained from hydrogen atomic clock pulse mixing and the local 10 MHz frequency signal are: f_{maxc} = 250 Hz, T_{minc} = 4 ms, A = 1623, B = 40000, f_{equ} = 1623 * 40000 * 250 Hz = 16230 MHz, ΔP = $1/f_{equ}$ = 61.6 ps. Obviously, there are too many clock samples like this. And the area set for sampling according to the linear region of ΔP is also too narrow. If the clock signal (i.e., the locked crystal oscillator signal) is divided by 50 times, then B = 800, the clock frequency is 200 kHz, and the clock cycle is 5 μs. f_{equ} = 1623*800*250Hz = 324.6MHz, ΔP = $1/f_{equ}$ = =3.08 ns. This clock sampling rate and linear sampling area can meet the convenient and correct sampling of linear phase and its variation. It also provides reliable working conditions for later analysis and processing. The 10-frequency division method in the figure can also obtain suitable operating conditions, with a higher sampling rate and a narrower linear region. However, for hydrogen atomic clocks and locked high stability crystal oscillators, there is no problem with operational reliability. The frequency stability and other results obtained by the phase-locked loop circuit of this digital method are currently not significantly different from the previous analog methods. Further experiments will be conducted in collaboration with relevant units on a hydrogen atomic clock.

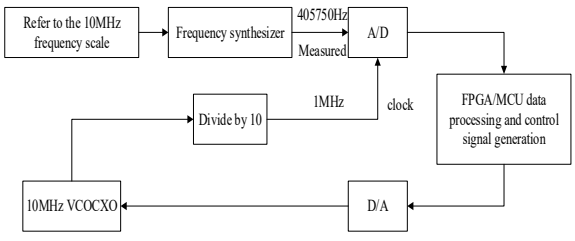


Fig. 7. Digital Direct Link Processing of Hydrogen Clock Frequency Link.

Another experiment on the frequency link of the hydrogen atomic clock is based on the hydrogen maser signal generated by the physical part, which is replaced by 1420.405 MHz generated by OCXO8607 through SMB100A [8]. This frequency is another frequency point of the maser signal in the hydrogen atomic clock [10, 11]. Perform spectrum analysis on the signals of key modules in the entire system. The power of the ADC analog input signal at 20.405 MHz is 12.4 dBm, the 3 dB bandwidth is 0.21 MHz, and the signal bottom noise is -36 dBm. There is no obvious noise frequency. In this experiment, it was consciously chosen that the stability index of the controlled crystal oscillator was significantly lower than the reference signal. After testing and comparing the signal performance parameters before and after the crystal oscillator was locked, it can be seen that the frequency stability of the crystal oscillator output signal improved from $1.84\times10^{-12}/1s$, $2.37\times10^{-12}/2s$, to $4.84\times10^{-13}/1s$, $5.43\times10^{-13}/2s$, $7.02\times10^{-13}/4s$, and the initial frequency deviation between the output signal and the nominal frequency of 10 MHz decreased from 2.721 Hz to, and the frequency drift within 12 hours decreased from 5.121×10^{-4} Hz to 1.375×10^{-6} Hz. This experiment on digital phase processing and phase-locked loops of hydrogen atomic clocks also demonstrates that the new principle proposed in this paper can always achieve phase comparison and phase locking between frequency signals in situations of large frequency differences and complex phase relationships. This provides important support for the progress of a wider range of time-frequency measurement and control technologies.

5. Conclusions

This article provides an in-depth analysis of the phase difference changes between different frequency signals with complex frequency relationships, and combines the waveform characteristics of the most common sinusoidal signals to provide a detailed description of the implementation and high-precision acquisition of direct digital phase locking between frequency sources with different nominal frequency values. There must be a T_{minc} and a specific phase difference change and arrangement order between a fixed reference frequency signal and any specific frequency signal. Precise phase control is used to achieve the locking of complex frequency signals, that is, to maintain the periodic variation relationship between them and the reference signal, which is complex and specific to each other. The guarantee of this relationship is to achieve the control of signal frequency by maintaining consistent voltage/phase sampling requirements in the linear region of the phase change at the most sensitive position of the signal, while ensuring the basic stable phase change of the locked frequency source. Unlike traditional phase states for the same frequency nominal value, the phase information displayed within T_{minc} between frequency signals with complex frequency relationships is more abundant. So, there is always a natural linear phase change zone. The sampling area of AD for the linear phase change zone corresponds to the quantized phase step value ΔP at the 0-phase difference between signals, which is convenient for measurement and feedback control. The innovative application in this area is also manifested in the optimization of the circuit of active hydrogen atomic clocks. This work subverts the traditional approach and understanding of phase processing and will be recognized in a large number of application fields.

References

[1]. W. Zhou, X. Ou, H. Zhou, et al., Time Frequency Measurement and Control Technology, *Xidian University Press*, 2006.

[2]. Z. Li, Phase comparison and processing technology of time-frequency signals, PhD Thesis, *Xidian University*, 2012.

[3]. C. Faxi, Z. Wei, Application of new PLL in active atomic frequency standard circuit, in *Proceedings of the IEEE International Frequency Control Symposium, Joint with the 22nd European Frequency and Time Forum*, 20-24 April 2009, pp. 565-567.

[4]. W. Zhou, The Greatest Common Factor Frequency and Its Application in the Accurate Measurement of Periodic Signals, in *Proceedings of the IEEE Frequency Control Symposium (IFCS'92)*, May 1992, pp. 354-359.

[5]. W. Zhou, Systematic research on high-accuracy frequency measurements and control, PhD Thesis, *Shizuoka University*, Feb. 2000.

[6]. W. Zhou, Equivalent Phase Comparison Frequency and Its Characteristics, in *Proceedings of the IEEE Frequency Control Symposium (IFCS'08)*, 2008, pp. 468-470.

[7]. L. Yang, Research on digital phase comparison system based on clock division, PhD Thesis, *Xidian University*, 2023.

[8]. M. Fan, Research on the servo circuit of hydrogen atomic clock, *PhD Thesis*, Xidian University, 2023.

[9]. F. Chen, W. Zhou, Application of new PLL in active atomic frequency standard circuit, in *Proceedings of the IEEE International Frequency Control Symposium Joint with the 22nd European Frequency and Time Forum*, 20-24 April 2009, pp. 565-567.

[10]. Y. Xie, Y. Cai, W. Zhang, Experimental Analysis of the Effect of Phase Locked Loop on the Performance of Hydrogen Atomic Clock, *Journal of Metrology*, Vol. 33, Issue 3, 2012, pp. 272-277.

[11]. Z. Zhai, Y. Li, T. Liu, The Space Application Prospects of Hydrogen Atomic Clock, *Space Electronics Technology*, Vol. 8, Issue 4, 2011, pp. 55-60.

(002)

Capacitive Sensor System with Frequency Output for Reading Extrinsically Inserted Hidden Information in 3D Objects

F. Marocko, F. Irmler, F. Piepereit and A. Bailleu
HTW Berlin University of Applied Science, Wilhelminenhofstr. 75 A, 12459 Berlin, Germany
Tel.: +49 30 5019-3341, fax: + 49 30 5019-48-3341
E-mail: anett.bailleu@htw-berlin.de

Summary: A capacitive sensor and the realisation of the integration of hidden information in 3D printed objects by means of technical processes is presented, whose main feature is that it can be read out capacitively from the 3D objects and thus contactlessly and completely non-destructively.

This paper describes the development and realisation of the developed capacitive readout unit integrated into a 3D printer, and the investigation into the selection of suitable material combinations for the 3D printing of invisible sub-surface information. Details of the realised targets with the hidden information are presented, as well as the test environment and the filtering and processing of the raw data from the capacitive sensor for successful readout of the previously generated hidden information. Dependencies between minimum structure widths and usable depth in the material for generating re-readable hidden information are presented.

Keywords: Capacitively, Contactlessly, Non-destructivly readout of hidden information, 3D-printing of hidden information.

1. Introduction and Motivation

Intrinsic and extrinsic hidden information plays an important role in product protection applications [1]. In this context, hidden information refers to data or features that are located inside objects or on their surfaces in such a way that they are undetectable to humans and can only be read out by a technical process with knowledge of their position, orientation and physical properties. In addition, the type of encoding of the information must be known in order to make the originally introduced information available to authorised user groups in decoded or recoded form [2].

Additive manufacturing has been playing an increasingly important role in industrial applications for years [3]. In addition to specific aesthetic and functional requirements, the embedding of copy protection elements and security features to prevent plagiarism or to authenticate branded products are among the most common customer requirements. There is also a growing trend to integrate customisable 3D printed structures into products to enable seamless traceability throughout the product lifecycle. This requires the implementation of adapted read-out processes that are both secure and simple and cost-effective to achieve widespread acceptance.

Multi-material 3D printing processes are already technically established. The combination of different materials offers numerous possibilities for embedding hidden information [1].

2. Idea and Implementation

2.1. Capacitive Sensor for Reading the Hidden Information

A Prusa i3 MK3s with an MMU2s extension is used to produce multi-material 3D printed objects containing hidden information. The printer has been modified to allow the information to be read out again. This is done by mounting a self-developed readout unit on the extruder of the 3D printer.

The readout unit (Fig. 1) consists of a sensor which provides two electrodes, each with an area of 4 mm² aligned to the print bed. These electrodes form a capacitor and are part of an oscillator (Fig. 2). Using the 3D printer's traversing unit, the sensor can be moved over the surface of an object at a uniform speed and with a constant height.

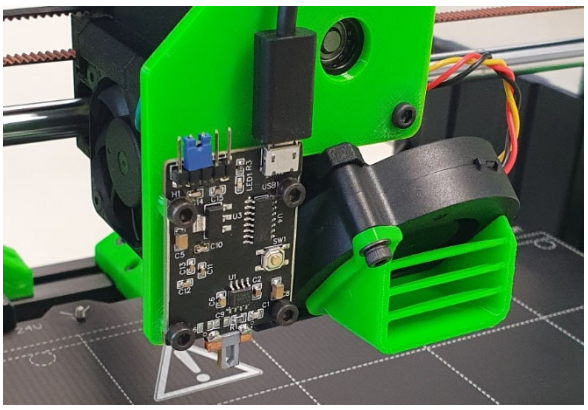


Fig. 1. Readout unit.

The elementary sensor (at the bottom of the board in Fig. 1) was realised with a 3D-printed body and adhesive copper tape as electrode material. In the experiments presented, it functions as a planar stray field sensor with electrode surfaces of 2 mm * 2 mm each and an electrode spacing of approximately 0.1 mm.

If the permittivity of the material in the stray field of the sensor changes in the process, its capacitance changes and thus the output frequency of the RC

oscillator. In the schematic (Fig. 2), C2 represents the capacitance of the sensor, which functions with a very low intrinsic capacitance.

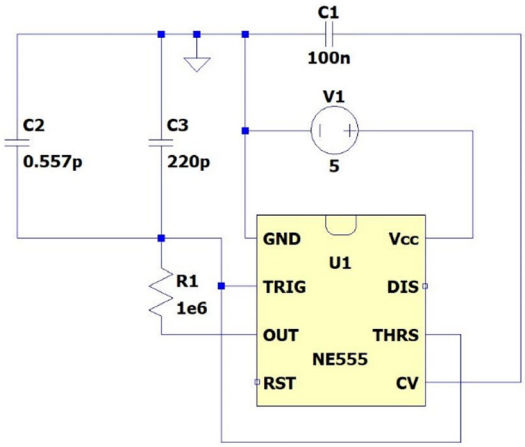


Fig. 2. Schematic of the RC oscillator.

The period duration is measured by a microcontroller and sent to a computer via a serial interface. Since times can be measured precisely with a microcontroller, a high resolution of the measurand is possible, which is crucial for the application described here, since very small capacitance differences in the femtofarad range have to be measured.

2.2. Generation of Multi-material 3D Objects with Hidden Information

In order to capacitively discriminate different materials in an electric field, their relative permittivities, which are primarily material dependent, must differ.

In our experiments, the selection of filaments consisted of commercially available products. Since not all material properties of interest are usually provided for commercially available 3D printing filaments, functionally important values such as relative permittivity (conductivity as a dielectric) must be determined experimentally. For this purpose, flat test specimens were 3D printed and installed as dielectric in a plate capacitor of known dimensions. The capacitance of the plate capacitor was then measured using an LCR bridge and the dielectric constant calculated (Table 1).

Table 1 shows that the use of the composite conductive PLA in combination with the yellow-green PLA can produce particularly large permittivity differences. This seems to be particularly suitable for creating a 3D printed object with hidden information. In the future, a combination of two black-coloured PLA grades could be considered, as this would make the filaments even less different.

To test the functionality of the test setup, rectangular test objects were generated which contain hidden information in the form of an alphanumeric barcode of type Code 128. The object contains the three-dimensional barcode inside, which is imperceptible to the human eye from all sides when viewed from the outside. The contained barcode represents the initials "HTW" of the Berlin University of Applied Sciences.

Table 1. Dielectric properties of selected 3D printing materials.

Filament name	Manufac-turer	Base material*	Relative permittivity*
Composite Conductive PLA	Proto-Pasta	PLA	37.40
CopperFill	colorFabb	PLA	3.38
Compostie Iron PLA	Proto-Pasta	PLA	2.75
PLA Galaxy silver	Prusa Research	PLA	2.34
Crystal green	3dk.berlin	PLA	2.31
IR black	3dk.berlin	PLA	2.28
PETG orange	Filament-world	PETG	2.27
Crystal	3dk.berlin	PLA	1.65
Yellow green	3dk.berlin	PLA	1.57

*** PLA: Polylactid, PETG: Polyethylenenterephthalat-Glycol**
**** Results of own measurements at 1kHz, 23 °C**

2.3. Process Control and Data Acquisition

With regard to take full advantage of the capabilities of the test bench, it is being partially automated. A graphical user interface is programmed in MATLAB to receive, process, evaluate and output data from the readout unit. At the same time, the user interface can be used to enter measurement parameters such as traverse paths and the dimensions of the object to be scanned. This allows reproducible measurements to be carried out in an uncomplicated manner. The graphical output of the reconstructed barcode and the direct output of the read string in plain text make the measurement results easily accessible to the user.

Data processing involves removing outliers (Fig. 4) from the raw measurement data (Fig. 3) and applying finite impulse response (FIR) filtering (Fig. 5).

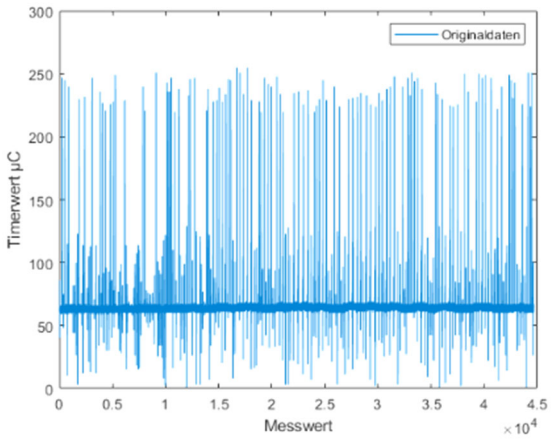


Fig. 3. Example of raw measurement data.

Rmoutliers detect and remove outliers in the data: by default, an outlier is a value greater than three scaled absolute median deviations (MAD). Savitzky-Golay filters apply a finite impulse response (FIR) polynomial order frame length Savitzky-Golay smoothing filter to the data in the vector x [4, 5] (Fig. 5).

Based on the resulting cleaned data, the graphical barcode is reconstructed (Figs. 5, 6). This is evaluated and the result is decoded and displayed directly in a form that can be interpreted by the user (Fig. 7).

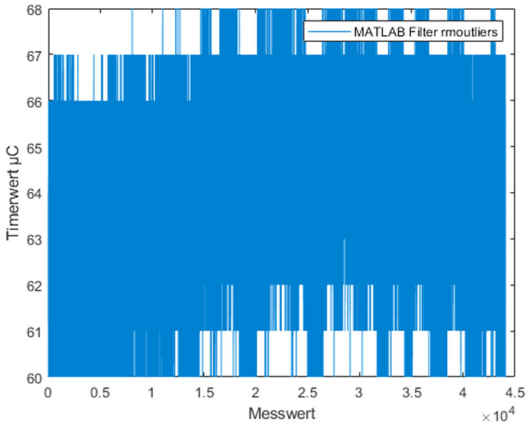


Fig. 4. Filtered data – remove outliers.

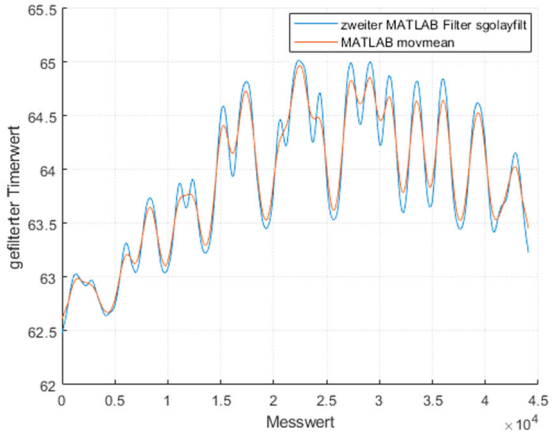


Fig. 5. Filtered data - Savitzky-Golay filter and moving average.

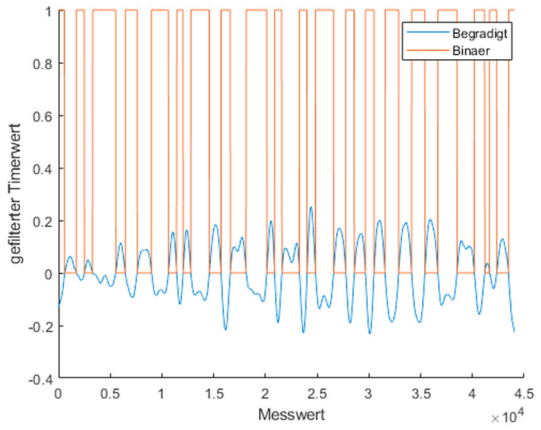


Fig. 6. Reconstructed binary code.

The processing can be done in MATLAB, or alternatively with a standard barcode scanner or smartphone app.

Fig. 7. Reconstructed barcode (Hiding of axes, saving as image, evaluation by Matlab barcode scanner).

3. Consideration of Information Density and Its Boundary Conditions

In order to test the limits of the method presented, a series of measurements is carried out using different test bodies (Table 2). These bodies contain the same bar code with the content "HTW", but the representation on the object varies. The minimum structure width and the printing depth can be distinguished between the barcodes. The minimum structure width indicates the width of the thinnest bar of the barcode. The print depth indicates how much material lies between the barcode and the surface of the sample over which the measurement is made.

Table 2. Test results for the minimum width of the structure and the depth of the print.

		printing depth				
		0.6 mm	0.8 mm	1.0 mm	1.2 mm	1.4 mm
minimum structure width	1.2 mm	✓	✓	✓	✓	×
	1.0 mm	✓	✓	✓	×	×
	0.8 mm	✓	×	×	×	×
	0.6 mm	×	×	×	×	×

The minimum print depth used in the tests was 0.6mm, as it is only above this overlap that the barcode cannot be seen by the human eye with the materials used below the visually observable surface.

The staggering of the print depths in 0.2 mm increments results from the filament layer height used during printing.

The distance between the sensor and the sample is 0.1 mm.

The highlighted line in table 2 shows the limit of readability of the hidden information from the test objects. For the test objects marked with a ✓, the barcodes can be correctly reconstructed and evaluated. This is not possible for the other fields (marked with ×).

4. Conclusion and Outlook

As a result, it is possible to show how a dielectric barcode can be produced by 3D printing and then read and decoded using a capacitive measurement method and a specially designed measurement sensor, so that the hidden information can be read by the user in plain text using a smartphone app. The process has been partially automated, and both the control of the measurement setup, the processing of the measurement data and the evaluation of the hidden barcode are carried out in a reproducible and reliable manner.

The findings and investigation results on the achieved and possible structure sizes, on the print depths of the hidden information that can be realised so far, and on the measuring distance between sensor and test object are presented.

In the solution currently implemented at the HTW Berlin, the measuring head for reading out the hidden information has been integrated directly into the 3D printer.

In the future, it is conceivable that freely movable handheld devices will make it possible to read out the hidden information.

References

[1]. D. Steffen, Herausforderung Produktschutz, in Prävention gegen Produktpiraterie.Intelligente Technische Systeme – Lösungen aus dem Spitzencluster it's OWL (C. Plass, Ed.), *Springer Vieweg*, Berlin, Heidelberg, 2020.

[2]. F. Irmler, F. Marocko, Entwicklung und Auswertung versteckter Informationen in Multimaterial-3D gedruckten Objekten, die mit einem kapazitiven Messverfahren ausgelesen werden, Masterarbeit unpublished, *HTW Berlin*, 2021.

[3]. D. Quitter, Industry of Things. Wie die deutsche Industrie die additive Fertigung nutzt, https://www.industry-of-things.de/wie-die-deutsche industrie-die-additive-fertigung-nutzt-a-1072127/

[4]. A. Savitzky, M. J. E. Golay, Smoothing and Differentiation of Data by Simplified Least Squares Procedures, *Anal. Chem*., Vol. 36, Issue 8, 1964, pp. 1627-1639.

[5] M. Schmid, D. Rath, U. Diebold, Why and How Savitzky-Golay Filters Should Be Replaced, *ACS Measurement Science Au*, Vol. 2, Issue 2, 2022, pp. 185-196.

(004)

Determination of Frequency of Acoustic Waves by Bragg Light Diffraction Method

F. R. Akhmedzhanov
Institute of Ion-plasma & Laser Technologies, TMS Laboratory,
33 Durmon yuli str., Tashkent, 100125, Uzbekistan
Tel.: + 998902121998
E-mail: akhmedzhanov.f@gmail.com

Summary: A new technology for determining the frequency of an acoustic wave has been proposed. The method is based on the use of Bragg diffraction of light by a high-frequency transverse acoustic wave in a gyrotropic crystal. The studies were carried out in the range of 0.8-1.1 GHz using a sample of a single crystal of lanthanum gallosilicate, oriented with high accuracy along the third-order crystallographic axis. An expression is obtained for the magnitude of the specific rotation of the plane of polarization of an acoustic wave depending on the effective constant of the acoustic gyrotropy pseudotensor and the effective elastic constant. During the measurements, it was taken into account that the attenuation coefficient and the specific rotation of the plane of polarization depend on frequency according to a quadratic law. The possibility of determining or controlling the frequency of an acoustic wave by measuring the dependence of the intensity of diffracted light on the distance along the direction of propagation of the acoustic wave is shown.

Keywords: Acoustic wave, Bragg light diffraction, Gyrotropic crystal, Frequency, Intensity.

1. Introduction

The Bragg diffraction of light by acoustic waves is widely used to study the elastic and photoelastic properties of various materials [1-4]. In the present work, this method was applied to determine the frequency of an acoustic wave propagating in a gyrotropic crystal. To understand the proposed technology, the phenomenon of acoustic activity is briefly described below without theoretical details.

It is known that acoustic activity is a mechanical analogue of optical activity. Its simplest manifestation is the rotation of the plane of polarization of a transverse acoustic wave propagating in a gyrotropic crystal in some special directions [5-11]. Although the phenomenon of acoustic activity was discovered relatively long ago, its direct experimental study is much more complicated than its optical counterpart, especially when the propagation direction of the acoustic wave does not coincide with the acoustic axis [9, 10].

In contrast to optical activity, acoustic activity can manifest itself in crystals belonging to one of the 21 noncentrosymmetric point symmetry groups [5, 6]. Acoustic activity is explained by first-order spatial dispersion, when a deformation created at a certain moment of time at some point in the crystal induces stress at another point in the crystal at a later moment of time. The complex elastic constants of a gyrotropic crystal c_{ijkl}, taking into account the spatial dispersion, can be written as [10]:

$$c_{ijkl}(\omega, q) = c_{ijkl}(\omega) + iq\gamma_{ijklm}(q)\kappa_m, \qquad (1)$$

where γ_{ijklm} is the acoustic activity tensor, c_{ijkl} is elastic tensor, ω is the frequency of the acoustic wave, $\boldsymbol{q}$ is the wave vector of the acoustic wave and κ_m is the components of normal vector.

As is known, the propagation of acoustic waves is accompanied by a decrease in its energy. The reasons are various dissipation processes, including phonon-phonon and electron-phonon mechanisms [1, 12, 13]. In piezoelectric crystals, a noticeable contribution to sound attenuation can be made by dielectric losses due to the piezoelectric effect [1, 3].

2. Samples and Experimental Methods

In the present work, acoustic activity and Bragg diffraction of light by hypersonic waves in a lanthanum gallosilicate crystal were used to control a measure the acoustic wave frequency at room temperature. The $La_3Ga_5SiO_{14}$ sample was oriented along the threefold crystallographic axis with an accuracy of 10'. X-cut lithium niobate piezoelectric transducers were used to excite plane-polarized transverse acoustic waves in the frequency range from 0.8 to 1.1 GHz.

An acousto-optic cell for measuring the intensity of diffracted light is shown in Fig. 1. The observation of diffracted light was carried out at the moment the acoustic pulse passed through the acousto-optic interaction zone. Light waves with a wavelength of 632.8 nm were generated by a helium-neon laser. The light intensities were measured by a photomultiplier. The dependence of the diffracted light intensities I_1 and I_2 on the distance L from the piezoelectric transducer

was determined at different points of the sample along the acoustic wave propagation direction.

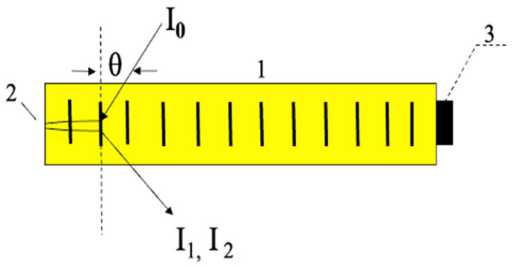


Fig. 1. Scheme of an acousto-optic cell.

The following designations are introduced in Fig. 1: 1 is $La_3Ga_5SiO_{14}$ sample, 2 is the opposite side of the sample, 3 is piezoelectric transducer, θ is the external Bragg angle of incidence of the light beam.

3. Results and Discussion

In the general case, the intensity of diffracted light in a gyrotropic crystal I is a function of several parameters, including the effective photoelastic constant p_{eff}, the attenuation coefficient of the acoustic wave α and the specific rotation of the polarization vector β [12, 13]:

$$I = I_0 \cdot p_{eff} \cdot [\exp(-\alpha L)] \cos^2(\beta L + \varphi_0), \qquad (2)$$

where I_0 is the intensity of the incident laser radiation, φ_0 is the initial phase of the acoustic wave, L is the distance from the piezoelectric transducer to the observation point of light diffraction.

Thus, if a plane-polarized transverse wave propagates from the point x = 0, then such a wave can be represented as a superposition of two waves, right- and left-hand polarized. Moreover, if at the point x = 0 the phases of these waves are taken equal to zero:

$$\phi_л = \phi_п = 0,$$

then at point x = L the resulting vector will rotate by an angle:

$$\phi = \frac{\omega L}{2}\left(\frac{1}{V_п} - \frac{1}{V_л}\right) = \frac{\omega L}{2} \cdot \frac{V_л - V_п}{V_п \cdot V_л}, \qquad (3)$$

where ω is the circular frequency, After some transformations, taking into account that we obtain the value of the specific rotation of the plane of polarization of the acoustic wave [10]:

$$\beta = \frac{\varphi}{L} = \frac{\omega^2}{2V_0^2} \cdot \frac{G_{eff}}{c_{eff}}, \qquad (4)$$

where G_{eff} and c_{eff} are the effective constants of the acoustic gyrotropy pseudotensor and the elasticity tensor, accordingly.

In the experiment, the angle of rotation of the polarization vector and the attenuation coefficient of the acoustic wave were first determined from relation (2), when the frequency of the acoustic wave did not change. Then the same measurements were carried out at other frequencies.

Typical experimental results for $La_3Ga_5SiO_{14}$ crystals at frequencies of 1.0 and 1.06 GHz are shown in Fig. 2.

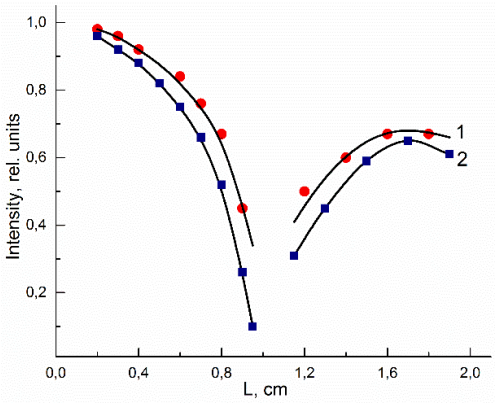


Fig. 2. Dependence of intensity of diffracted light on the distance L from piezotransducer at the frequencies 1.0 GHz (1) and 1.06 GHz (2).

The points in the figure are the results of the experiment; curves – calculation according to equation (2). It can be seen that the direction of rotation of the polarization vector changes at the sample boundary (the length of the sample was 1.05 cm). This effect can be easily explained by the fact that the acoustic wave is reflected from the free boundary of the sample and, accordingly, the direction of rotation changes to the opposite.

After determining the specific rotation of the polarization vector and the attenuation coefficient of the acoustic wave at one frequency of the acoustic wave, its value was changed with a step equal to the double natural frequency of the piezoelectric transducer. In our studies, this step was 0.06 GHz. The measurements took into account that the attenuation coefficient and the specific rotation of the polarization plane depend on the frequency according to a quadratic law [10].

Thus, by observing the change in the intensity of diffracted light at a certain point in the sample, it is possible to estimate the change in the frequency of the acoustic wave. Having previously calibrated the dependence of the intensity of diffracted light on frequency at a certain point of the crystal sample used as a measuring sensor, it can be used to control the frequency of the acoustic wave.

4. Conclusions

Comparison of the measured frequency values with the frequencies of the used radio generator showed that

the proposed method makes it possible to determine the frequency of an acoustic wave with an accuracy of 1 %. The absolute accuracy of frequency determination in the proposed method is relatively low and is limited by the accuracy of light intensity measurement.

However, using special comparison circuits for measuring light intensity it is possible to achieve high relative accuracy in determining the frequency of an acoustic wave. The method can be useful for monitoring the stability or deviation of the frequency of the modulating signal in acoustic-optical and optical signal processing devices, in which gyrotropic crystals are used. It should also be noted that it is necessary to ensure the broadband operation of the piezoelectric transducer in the controlled frequency range and the unconditionally linear operating mode of the photodetector.

References

[1]. D. Dieulesaint, E. Royer, Elastic Waves in Solids, *Masson & Cie*, Paris, 1974.

[2]. A. Erba, R. Dovesi, Photoelasticity of crystals from theoretical simulations, *Phys. Rev*., Vol. B88, 2013, 045121.

[3]. F. R Akhmedzhanov, F. N. Juraev, Attenuation of acoustic waves in Lithium Niobate crystals with impurities, in *Proceedings of the Conference on Acoustics*, Nant, France, 12-16 April 2012, hal-00811325.

[4]. F. R. Akhmedzhanov, T. Sh. Mustafaev, J. T. Nazarov, Attenuation of Acoustic Waves in Langasite Crystals, *Sensors & Transducers*, Vol. 254, Issue 7, 2021, pp. 38-42.

[5]. D. L. Portigal, E. Burstein, Acoustical Activity and Other First-Order Spatial Dispersion Effects in Crystals, *Phys. Rev*., Vol. 170, Issue 3, 1968, pp. 673-679.

[6]. K. V. Bhagwat, R. Subramanian. Acoustical activity in the framework of the rotation–gradient theory of elasticity, *Phys. Rev. B*, Vol. 33, Issue 8, 1986, pp. 5795-5800.

[7]. Y.-y. Li, L. Chen, Theory of acoustical activity, *Phys. Rev. B*, Vol. 36, Issue 18, 1987, pp. 9507-9513.

[8]. T. P. Srinivasan, Description of acoustical activity using irreducible tensors, *J. Phys. C: Solid State Phys*., Vol. 21, Issue 23, 1988, pp. 4207-4219.

[9]. K. V. Bhagwat, R. Subramanian, Acoustical Activity of Crystals: a Comparative Study of Three Descriptions, *Acta Cryst*., Vol. A44, Issue 4, 1988, pp. 551-554.

[10]. M. F. Bryzhina, S. Kh. Esayan, V. V. Lemanov, Acoustical activity in SiO_2 crystals, *Journal of Experimental and Theoretical Physics (SU)*, Vol. 25, Issue 11, 1977, pp. 513-515.

[11]. F. R. Akhmedzhanov, Acoustical activity in $La_3Ga_5SiO_{14}$ and $Nd_3Ga_5SiO_{14}$ crystals, in *Proceedings of the 14th Symposium on Thermophysical Properties*, USA, Colorado, 2000.

[12]. R. Nava, M. P. Vecchi, J. Romero, B. Fernandez, Akhiezer damping and the thermal conductivity of pure and impure dielectrics, *Phys. Rev. B*, Vol. 14, Issue 2, 1975, pp. 800-807.

[13]. V. I. Balakshy, A. S. Voloshin, V. Ya. Molchanov, Influence of acoustic energy walk-off on acousto-optic diffraction characteristics, *Ultrasonics*, Vol. 59, 2015, pp. 102-108.

(005)

Implementing an NTS-Based Security Mechanism for PTPv2.1

M. Langer [1,2], J. Köstel [1] and R. Bermbach [1]
[1] Ostfalia University of Applied Sciences, Salzdahlumer Straße 46/48, 38302 Wolfenbüttel, Germany
[2] Physikalisch-Technische Bundesanstalt, Bundesallee 100, 38116 Braunschweig, Germany
Tel.: + 49 5331 939 42620, fax: + 49 5331 939 42622
E-mail: r.bermbach@ostfalia.de

Summary: Complex or time-sensitive computer networks often require reliable, accurate and, most importantly, secured time synchronization of their nodes. The Precision Time Protocol (PTP) provides the necessary accuracy, but still operates in an unsecured manner. Although first security mechanisms exist in the current version PTPv2.1, they do not work out of the box, but need further specification work. The security protocol NTS4PTP is based on the Network Time Security Protocol (NTS) and seems to be the most promising proposal for securing PTP with the so-called integrated security mechanism. But up to date, there is a lack of implementations and experimental evaluations of NTS4PTP. This paper presents a first proof-of-concept implementation based on the NTS4PTP protocol draft. NTS4PTP as well as the PoC implementation are currently under development. The implementation work provides promising initial test results regarding protocol functionality, security features, and the suitability of cryptographic algorithms based on performance tests.

Keywords: PTP, NTS, NTS4PTP, Security, Time transfer.

1. Introduction

Many computer systems require time information, for example, when security certificates are involved or when interoperability of devices within networks is important. A convenient way to do this is to rely on the widely used Network Time Protocol (NTP) [1], which is easy to use and ensures time synchronization in the low millisecond range. In other domains, such as power distribution, telecommunication, or automation, the requirements for accurate and reliable time synchronization are much higher. These requirements are met by the Precision Time Protocol (PTP) [2], which provides synchronization accuracies in the nanosecond range.

Despite the fact that time information is a critical infrastructure, there has been little effort to protect this sensitive information. Only with the standardization of the Network Time Security (NTS) protocol [3] at the end of 2020, the first effective and practical protection mechanism appeared that exclusively secures NTP in client-server mode. The current PTP standard (IEEE 1588-2019) [2] provides security features as well, but they cannot be used out of the box. As a result, communication in the PTP network remains unsecured. While initial security proposals (see Section 2.2) currently exist to provide feasible protection mechanisms, there is a lack of implementations and experimental testing of the protocols to ensure their proper functionality and behavior. The proof-of-concept (PoC) implementation presented in this paper is based on the NTS for PTP (NTS4PTP) protocol [4], which is under active development as a draft at the IETF. This software is still under development, so extensive testing and evaluation is planned. Fortunately, the implementation is already providing initial test results that confirm the functionality of the NTS4PTP protocol and give feedback to support the standardization work.

In the remainder of this paper, Section II first provides an overview of PTP security aspects and related work. Section III then describes the NTS4PTP protocol flows, distinguishing between multicast-oriented and unicast-oriented connections. Section IV then explains the structure of the PoC implementation, including the architecture, design decisions, and key features. Section V describes the initial measurement setup and discusses the first results of the implementation in terms of protocol functionality, security features, and performance. Finally, the conclusion and next steps are presented in Section VI.

2. Preliminaries and Related Work

The Precision Time Protocol is often used in local and well-administered networks where time synchronization of devices in the microsecond or nanosecond range is needed. It is very complex and distinguishes between various clock types, communication modes, delay measurements and profiles. In multicast mode, masters send their time information to a large number of slaves, while in unicast connections so-called grantors transmit their time information to individual requesters after negotiation. The distribution of the time information is still unsecured, so that there is a high security risk here. The first attempt to establish a protection mechanism was made in 2008. Here, the IEEE Std 1588-2008 (PTPv2) [5] described an experimental approach based on symmetric key cryptography in its Annex K. However, it was never implemented and later analyses [6] [7] revealed various design flaws as well as optimization potential. The results eventually led to a revision of the security mechanisms described in

Annex P, published in 2020 with the PTPv2.1 standard (IEEE Std 1588-2019) [2]. Annex K thus became obsolete and was removed.

2.1. PTPv2.1 Security Options

Annex P describes the security concept in generic form and divides it into four prongs. These are all optional and can be used individually or in combination to protect the PTP network. Prong A defines an integrated security mechanism for PTPv2.1. It specifies an AUTHENTICATION TLV [1] (AuthTLV) which, in addition to various data fields, contains an Integrity Check Value (ICV) to protect the PTP messages. Furthermore, it provides rough guidelines on how to use the AuthTLV, how to store and handle the security associations (contain keys and parameters) and which security processing approaches are available. Prong B includes external transport security mechanisms such as MACsec or IPsec, but depending on the choice, these restrict PTP communication capabilities. Prong C covers architectural mechanisms to increase the resiliency of the network, while monitoring and management to detect attacks or problems in the PTP infrastructure are addressed in prong D.

2.2. Automatic Key Management Solutions

The suitability of prong A for securing PTP has already been confirmed in studies [8, 9]. However, these also show that automatic key management (KM) is necessary to scale the key distribution depending on the PTP network size. Currently, three automatic KM solutions are proposed. The first is the Group Domain of Interpretation (GDOI) protocol-based GDOI-for-PTP [2, P.2.1.2.1], which is designed for group communication in PTP multicast connections and is currently in the IEEE standardization process. Another KM proposal called NTS for Negotiated Unicast PTP (NTS4UPTP) [10] is intended exclusively for PTP unicast connections and bases on the Network Time Security protocol NTS (see Section 3.). However, the development work has already been stopped in 2021, so that the protocol draft has expired. The third available KM proposal is NTS4PTP [4], which is discussed at the IETF as well as in IEEE 1588 and actively under development. It also relies on NTS and supports PTP multicast and unicast connections. Because of its particular advantages we chose the NTS4PTP protocol to realize a PoC implementation of a first NTS-based key management system for PTP.

3. NTS4PTP Protocol Description

The Network Time Security protocol [3] was standardized at the IETF in 2020 and secures NTPv4 since then. NTS consists of two subprotocols and is also suitable for other time protocols such as PTP. The first one is the NTS Key Establishment (NTS-KE) protocol, which is used for the communication between the NTP client and the NTS-KE server (equivalent to a key management server). Here, NTS messages are transmitted over a secured TLSv1.3 [11] channel for parameter negotiation and key establishment. The second subprotocol then protects the NTP messages at the level of the time protocol, which is executed after the successful NTS-KE phase.

NTS4PTP extends the existing NTS standard and adds support for PTPv2.1 to the NTS-KE protocol. Furthermore, it defines the new NTS Time Server Registration (NTS-TSR) subprotocol that specifies the communication between a PTP grantor (time server) and the NTS-KE server. This communication uses NTS messages over a secured TLSv1.3 channel as well. Notably, NTS4PTP defines two different modes a PTP client may utilize. In a multicast or mixed multicast/unicast communication, a PTP client chooses the group-based approach (GrBA) during the NTS-KE protocol phase and the ticket-based approach (TiBA) for pure unicast connections. PTP grantors, on the other hand, require the NTS-TSR protocol, which uses no further distinction or modes.

GrBA divides the PTP network into one or more security groups, which are formed automatically based on the PTP domain and the PTP profile. To join a group, the PTP client (master or slave) sends a request to the NTS-KE server (see Fig. 1). If the client certificate confirms its authenticity and authorization to join this group, then the NTS-KE server provides the corresponding security association (SA), which is shared by all clients within a group. This enables any client to secure PTP messages for this group or to verify incoming messages. Periodically, the group SAs are renewed and an NTS-KE server can exclude individual PTP clients if necessary (group control).

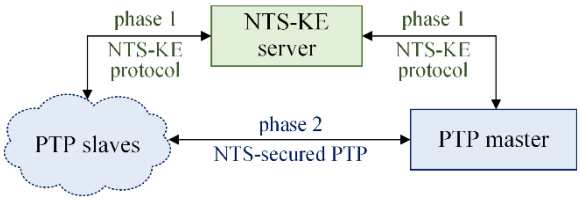


Fig. 1. PTP participants in NTS-secured GrBA mode.

TiBA, on the other hand, is used for end-to-end connections, as it scales much better for this purpose than a group-oriented solution. It is more flexible in parameter negotiation and uses a ticket system to initiate a secure PTP connection. The main difference here is that PTP servers (grantors) register in advance with the NTS-KE server using the NTS-TSR protocol and establish a ticket key during this process (see

[1] A Type-Length-Value (TLV) is a generic data structure that allows easy parsing of data blocks.

Fig. 2). From that point on, any number of PTP clients (requesters) can request an individual SA for this PTP server at the NTS-KE server, again using the NTS-KE protocol. In addition to the SA, a PTP client also receives a ticket that contains the same SA in encrypted form. With the first NTS-secured PTP message that the PTP client sends to the PTP server, it also transmits the ticket, once. The PTP server can decrypt this ticket with the ticket key received during the registration process, extract the SA it contains, and henceforth verify and secure the PTP messages from and to this client. Since PTP servers are stateful, a new ticket transmission is only necessary after a key update, which takes place at defined intervals. Another special feature is the ability of the PTP server to transmit status information to the NTS-KE server via heartbeat messages, thus enabling load balancing if the NTS-KE server manages multiple grantors. [4] and [12] describe NTS4PTP in more detail.

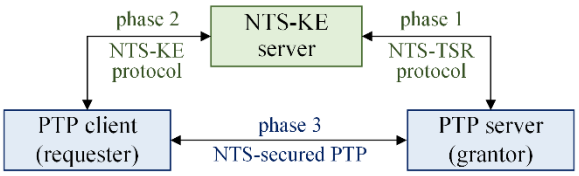


Fig. 2. PTP participants in NTS-secured TiBA mode.

4. Software Concept and Implememtation

The version 05 of the NTS4PTP protocol [4] currently serves as the basis for the PoC implementation [13]. The software is in a work-in-progress stage and will be adapted accordingly as the specification changes. This section describes the objectives of the implementation, its features, and how the architecture has been implemented.

4.1 Objectives

The aim of this work is to provide a reference implementation that can be used to experimentally evaluate the NTS4PTP protocol and to perform interoperability tests in the future. It should demonstrate whether the operations described in the specification can be implemented, the security mechanisms work correctly or changes are necessary due to specification gaps or ambiguities. In addition, the influence of NTS on a secured PTP system is also to be considered. This comprises the necessary information exchange between the PTP and the NTS layer (see Section 4.4), the impact on the PTP protocol flow and the performance of NTS when executing cryptographic operations. The resulting information serves as feedback to the authors of NTS4PTP to support their development efforts.

4.2 Characteristics and Architecture

The implementation of NTS4PTP is written in C++ and can be used on Windows or Linux systems. The current version of the implementation focuses on the execution of tests and is therefore oriented towards this in terms of the software structure. As a result, the software offers a large number of parameters that can be freely configured by the user. In addition, the implementation provides extensive log and diagnostic data in order to be able to detect and trace errors in the protocol flow. Due to the current PoC character of the implementation, runtime optimization is less relevant.

4.3 PTP Layer (PTP Simulator)

The realization of the implementation is not trivial, since in addition to the NTS4PTP specification, parts of the PTPv2.1 standard (IEEE Std 1588-2019) [2] need to be implemented as well. In addition, some parts of the specifications are not yet finalized, such as the regulations when filling the AuthTLV in the PTP messages or the PTP TLV identifier of the Ticket TLV. This naturally leads to the question of which PTP software should be considered as the foundation for the NTS extension. In the open-source sector, there are currently PTPd and Linux PTP. Both are designed for Linux-based operating systems and rely on PTPv2.0, although PTPd is no longer under development. Since upgrading an existing third-party PTP implementation to the current PTPv2.1 standard is very time-consuming and can make testing special scenarios difficult, a PTP simulator (see Fig. 3) has been developed. It can simulate and combine various PTP instances (master, slave, grantor or requester) as well as generate and process PTPv2.1 messages. With the PTP simulator small networks can be created without effort, in which PTP instances on different devices are able to communicate via multicast and unicast. Of course, this simulator is somewhat constrained and is only used to test the NTS4PTP implementation. Thus, only a part of the PTP messages has been implemented, in which merely the fields and TLVs relevant for NTS4PTP are filled in the PTP messages. A transmission and synchronization of time information does not take place here. The PTP simulator further offers the advantage of defining deterministic tests, since all values can be controlled in order to examine packet manipulation or replay attacks.

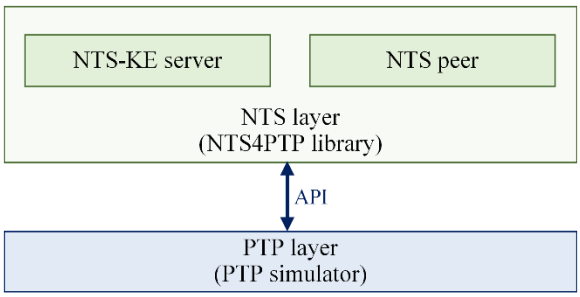


Fig. 3. Software layers of the PoC implementation

4.4. NTS Layer (NTS Library)

The implementation of NTS4PTP was not realized as an integral part of the PTP simulator, instead it was implemented separately from it. It can be embedded as a library and ported into a real PTP implementation at a later stage. The library comprises all functions and protocols described in NTS4PTP (NTS-KE and NTS-TSR) and allows the instances to run as NTS-KE server (key server) or also as any kind of NTS peer (see Fig. 4). Since a PTP device may as well have several PTP-capable Ethernet ports, each representing an independent PTP instance, different states must be handled in the NTS4PTP implementation. The design of the NTS4PTP library allows a single NTS peer (represents a global NTS4PTP instance) to manage any number of PTP instances, regardless of whether they are operating as master, slave, grantor or requester. This means that the NTS peer centrally handles the keys and parameters of all PTP ports on the respective device. Similarly, an NTS-KE server has only one NTS instance, which manages any number of security associations. This works regardless of which NTS4PTP modes (GrBA/TiBA) the PTP network uses.

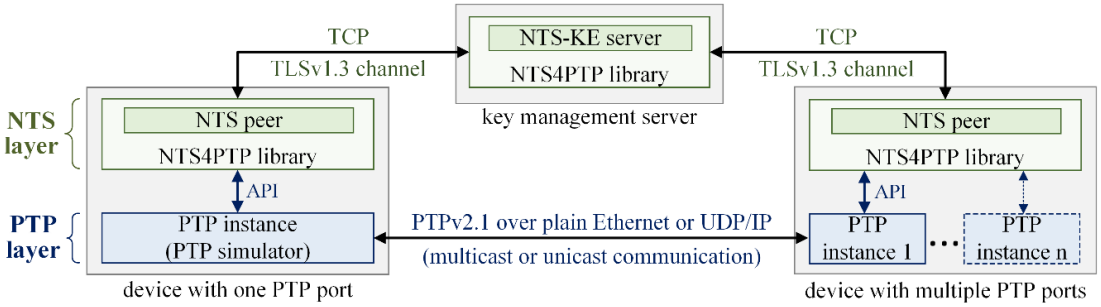


Fig. 4. Communication structure of the PoC implementation.

The SAs are updated automatically. As provided for in the specification, the NTS-KE server generates new SAs at defined intervals. The NTS peers request these automatically without the need for the PTP layer to control this explicitly via the NTS4PTP library interface. To ensure that the SAs are not lost in the event of a device reboot, the NTS-KE server stores them persistently as JSON files when changes are made, so that they can be loaded if necessary. Of course, in future it must be prevented that unauthorized persons or processes can access them. In the case of the PoC implementation, this is not currently a priority. NTS peers, on the other hand, can simply contact the NTS-KE server after a reboot and request a new SA.

The current version of the PoC implementation uses OpenSSL v3.1 [14] to provide the cryptographic algorithms. These include the AEAD algorithms specified in NTS, which are used for ticket encryption and decryption, as well as HMAC and CMAC for securing PTP messages. The NTS layer handles the creation and processing of the AuthTLV in PTP messages, which does not need to be realized in the PTP implementation. For this purpose, the NTS layer (here represented by the NTS library) uses its own PTP parser to read or write the necessary information of a PTP packet. This allows the interface functions between NTS and PTP to be reduced to a minimum.

4.5. Communication Paths

In terms of communication, there are three paths to consider. At the PTP level, we have the normal network communication between the PTP instances as defined in the PTPv2.1 standard. As usual in PTP, plain Ethernet (802.3 mode) or IP/UDP are used here to transmit the PTP messages in multicast or unicast connections. The presence or absence of an AuthTLV differentiates between NTS-secured communication and unsecured transmission.

The second communication path lies between the NTS peer and the NTS-KE server. The network-based communication takes place either directly from the PTP port or from a dedicated management port on the PTP hardware. This path is used for the NTS-based exchange of keys and parameters via a secured TLSv1.3 connection. If the NTS-KE server is an integral part of a PTP-capable hardware (e.g., Grandmaster), this can of course also be implemented via an inter-process communication. From the point of view of the PTP layer, the communication between NTS peer and NTS-KE server is completely invisible.

The last communication path connects the PTP and the NTS layer, which is realized program-internally via an application programming interface (API) and consists of five program functions. *SecurePTP* cryptographically secures the messages generated by the PTP layer by passing the PTP packet with the destination address (e.g., MAC or IP) to the NTS layer. The NTS peer can use it to identify the associated SA and add the AuthTLV to the PTP packet. It does not matter whether the PTP port acts as master, slave, grantor or requester. If there is no SA available yet, the NTS peer automatically connects to the NTS-KE server and obtains the necessary information. If this takes a bit longer for whatever reason, NTS does not block the PTP layer, but signals that the SA is not yet present. In that case the PTP layer discards the current message and tries again a short time later.

The processing and securing runtimes in NTS are not critical and do not affect the PTP synchronization accuracy. When a PTP instance receives a message, it calls the *VerifyPTP* function, passing the PTP packet to the NTS layer. Using the information in the message, the SA can be identified and the packet verified. The NTS layer informs PTP whether the integrity check was successful and no replay occurred. If a PTP instance acts as a grantor, it also needs the functions *InitializeNtsGrantor*, *StopNtsGrantor* and *StatusUpdate*. With InitializeNtsGrantor the grantor registers with the NTS-KE server. Here the PTP layer only has to pass the network addresses to the NTS layer at which it wants to be reachable. If a grantor wants to stop its service, the PTP layer calls StopNtsGrantor, and passes the PortIdentity (unique identifier of the PTP instance in the network) of the corresponding grantor. The NTS peer then sends a Registration Revoke message to the NTS-KE server, which can uniquely identify the grantor based on the certificate and PortIdentity and then delete it from the grantor list. The last function StatusUpdate is optional and allows PTP to communicate the workload to the NTS layer. When a grantor sends heartbeat messages to the NTS-KE server, it can include this status information so that the NTS-KE server can regulate the workload of multiple grantors. However, such a mechanism is not yet available in the PoC implementation.

5. Initial Test Runs and Results

Parallel to the programming work, test runs were performed at regular intervals to verify the specified NTS4PTP protocol sequences.

5.1. Measurement Setup and Configuration

A total of one Windows 10 desktop computer (i5-1035G4 processor with 1,1 GHz), one Windows 11 desktop computer (i5-12600K processor with 3.7 GHz) and three Linux-based Raspberry Pi 3B devices (ARMv7 processor with 1.2 GHz) were used for testing. The Windows 10 computer was always configured as an NTS-KE server, while the Raspberry Pis acted as PTP devices (using the PTP simulator). Depending on the test series, the Raspberry Pis were assigned different roles (master/slave/ grantor/requester) to simulate different scenarios. The Windows 11 computer also added up to 12 additional simulated PTP devices locally. The communication between the devices took place via a normal network switch, since there was no time synchronization or time-critical communication between the devices or the PTP instances during the series of measurements. In most of the tests, the master/grantor sent a message to the network every 600 ms, which was parameterized or manipulated differently depending on the scenario to observe the behavior of the other devices. Periodic key updates were performed every two minutes.

5.2 First Results

The main objective of the measurement series was to prove that the NTS4PTP protocol works and scales. Although not all features (e.g. heartbeat) are fully developed in the implementation, the current results confirm that NTS4PTP works fine. Parameter negotiation and key rotation were performed without any problems. Attacks on the PTP Best Master Clock Algorithm (BMCA), where an attacker takes the role of the time server, were defeated. Manipulation of PTP packet data, tickets, or replay attempts were also reliably detected. During implementation and testing, only minor specification gaps or errors were found, such as the indication of incorrect key lengths. However, these will be addressed and corrected in near future protocol revisions.

With regard to the performance tests, the cryptographic algorithms for generating respectively checking the ICV have been examined in detail. The results in [12] were used as a basis, where HMAC and CMAC were compared. In our own test series, we extended this investigation to include the algorithms GMAC, KMAC, and SipHash. First tests on a desktop PC showed that sipHash provides the best values for the formation of the ICV with a typical data set of 78 octets. The following average (median) values were recorded: sipHash-2-4 (0.99 µs), CMAC-AES-128-CBC (2.64 µs), GMAC-AES-128-GCM (2.78 µs), HMAC-SHA256 (3.01 µs), KMAC-256 (3.09 µs). Of course, keep in mind that these measurements were made on a desktop PC in software. Since KMAC is hardware-optimized, an implementation in hardware might give better results.

Due to the PoC nature of the implementation and the fact that the programming work is not yet complete, the execution times of the securePTP and verifyPTP API functions are in the range of 500 µs on a desktop PC and about 1000 µs on the Raspberry Pis. These values change slightly depending on the negotiated algorithm for securing the PTP messages. When the securePTP function was executed without a valid key, the execution time increased by about 300 µs to 500 µs because NTS performed a new key exchange in the background. The PTP communication could take place without packet loss.

6. Conclusion and Further Work

The development of a PoC implementation for the NTS4PTP protocol proved to be effective and could already provide first feedback. The results show that the protocol flow works fine and that the specification shows only very few gaps. Performance is also satisfactory for a PoC implementation. The next goal is to extend the implementation to a complete reference implementation that can be used for interoperability testing in the future. Therefore, a second and independent NTS4PTP implementation by another author is planned to further improve the quality of the tests. It is also planned to integrate the PoC implementation into a PTP service such as

LinuxPTP or into PTP capable industrial hardware. In the future, the NTS-KE server should also be able to implement the NTS for *NTP* protocol, in order to be able to secure NTPv4 in addition to PTPv2.1.

References

[1]. D. L. Mills, U. Delaware, J. Martin, J. Burbank, W. Kasch, Network Time Protocol Version 4: Protocol and Algorithms Specification, RFC 5905, *Internet Engineering Task Force (IETF)*, June 2010.

[2]. IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems, IEEE Std 1588-2019 (Revision of IEEE Std 1588-2008), *IEEE Standards Association*, June 2020.

[3]. D. Franke, D. Sibold, K. Teichel, M. Dansarie, R. Sundblad. Network Time Security for the Network Time Protocol, RFC 8915, *Internet Engineering Task Force (IETF)*, September 2020.

[4]. M. Langer, R. Bermbach. NTS4PTP - Key Management System for the Precision Time Protocol Based on the Network Time Security Protocol, Internet Draft, draft-langer-ntp-nts-for-ptp-05, *Internet Engineering Task Force (IETF)*, Feb. 2023.

[5]. IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems, IEEE Std 1588-2008 (Revision of IEEE Std 1588-2002), *IEEE Standards Association*, July 2008.

[6]. E. Itkin, A. Wool, A Security Analysis and Revised Security Extension for the Precision Time Protocol, *IEEE Transactions on Dependable and Secure Computing*, Vol. 17, Issue 1, September 2020, pp. 22-34.

[7]. B. Hirschler, A. Treytl, Validation and Verification of IEEE 1588 Annex K, in *Proceedings of the IEEE International Symposium on Precision Clock Synchronization for Measurement, Control and Communication (ISPCS)*, Germany, Munich, September 2011, pp. 44-49.

[8]. E. Shereen, F. Bitard, G. Dán, T. Sel, S. Fries, Next Steps in Security for Time Synchronization: Experiences from implementing IEEE 1588 v2.1, in *Proceedings of the IEEE International Symposium on Precision Clock Synchronization for Measurement, Control, and Communication (ISPCS)*, USA, Oregon, Portland, Sep. 2019, pp. 1-6.

[9]. D. Maftei, R. Bartos, B. Noseworthy, T. Carlin, Implementing Proposed IEEE 1588 Integrated Security Mechanism, in *Proceedings of the IEEE International Symposium on Precision Clock Synchronization for Measurement, Control, and Communication (ISPCS)*, Switzerland, Geneva, September 2018, pp. 1-6.

[10]. H. Gerstung, M. Rohde, D. Arnold, Network Time Security for the Unicast Mode of the Precision Time Protocol, Internet Draft, draft-gerstung-nts4uptp-03, *Internet Engineering Task Force (IETF)*, June 2021.

[11]. E. Rescorla, The Transport Layer Security (TLS) Protocol Version 1.3, RFC 8446, *Internet Engineering Task Force (IETF)*, August 2018.

[12]. M. Langer, R. Bermbach, NTS4PTP – A comprehensive key management solution for PTP networks, *Computer Networks,* 213, 2022, 109075.

[13]. J. Köstel, M. Langer, NTS4PTP Prototype, Github Repository (https://github.com/JKOKAY/-NTS4PTP_Prototype).

[14]. OpenSSL libraries v3.1, OpenSSL.org (https://www.openssl.org/source/).

(006)

Common-view Time Transfer Using GPS, Galileo, GLONASS, BeiDou-2, and BeiDou-3

Gihan G. Hamza
National Institute of Standards (NIS), Time and Frequency and Microwaves Laboratory, Giza, Egypt
Tel.: +201009003126
E-mail: gihan_gomah@yahoo.com

Summary: Comparing distant frequency standards can be done through a Global Navigation Satellite System (GNSS) using the common-view time transfer technique. In this technique each one of the frequency standards is compared to the clocks on-board the visible satellites, then the results are exchanged to calculate the time difference between the two frequency standards. For the time being, there are four different operational GNSS; which are the American system (Global Positioning System (GPS)), the European system (Galileo), the Russian system (GLObalnaya NAvigatsionnaya Sputnikovaya Sistema (GLONASS)), and the Chinese systems (BeiDou-2 and BeiDou-3). These GNSSs are not identical and every system has its own technical specifications. In this paper, we study the performance of the four GNSS when used in comparing distant frequency standards. This study was conducted using real data that belong to four national timing centers. The first and second timing centers are the national metrology institute of the United Kingdom (National Physical Laboratory (NPL)) and the national metrology institute of Germany (Physikalisch-Technische Bundesanstalt (PTB)). The third and fourth timing centers are the national metrology institute of China (National Time Service Center (NTSC)) and the national metrology institute of Check Republic (Institute of Photonics and Electronics, Czech Academy of Sciences (TP)). All these timing centers are using highly precise frequency standards that are used in generating their national time scales (UTC(k)).

Keywords: GNSS, Distant clocks, Time and frequency difference, Common-view time transfer.

1. Introduction

The technical specifications of the precise frequency sources are sensitive to the vibration and the changes in the environmental conditions. If one of the two distant frequency sources is transported to the location of the other source for sake of comparison, then the comparison results are likely to be invalid when this source is returned back. So, time and frequency transfer through an intermediate facility is the preferred choice for comparing distant atomic frequency standards. The intermediate facility for that purpose can be either navigation or the communication satellites. There are three main methods for time and frequency transfer using satellites; the one-way method, the common-view method (the two-station), and the two-way method. The one-way and the common-view methods are using the Global Navigation Satellite Systems (GNSS) and the two-way method is using the communication satellites [1-5].

Each time and frequency transfer method has its own accuracy and stability specifications. The two-way technique is used when a sub-nanosecond stability is required. So, it is used for comparing distant Cesium fountains; which are currently the international primary frequency standards. The one-way technique is used to compare atomic clocks, like the 5071A primary frequency standard, to the standard time of the GNSS (GNSST); which is synchronized to the Coordinated Universal Time (UTC). Previously, the author has proved that the stability of the one-way time transfer differs between the different GNSS. Moreover, the satellites constituting the same GNSS may not have the same behaviour [6].

The common-view technique is equivalent to implementing the algorithm of the one-way time transfer technique at both sites using the same visible satellites at the same time. Actually, the two distant frequency standards are being compared to the GNSST then the results are being exchanged to calculate the time difference. The main advantage of the common-view time transfer is that the common errors are cancelled out or minimized depending on the distance between the two clocks [7]. In this paper, we study the characteristics of the common-view time transfer using GPS, Galileo, GLONASS, BeiDou-2, and BeiDou-3.

2. Error Sources in the Time Transfer Using Navigational Satellites

Atomic frequency standards are generating highly accurate and stable time and frequency signals. So, the noise added by the time transfer method should be minimized to not affecting negatively the characteristics of these precise signals. The common-view time transfer technique is equivalent to conducting the one-way technique two times under certain conditions [7].

During the one-way time transfer, a lot of errors are being added to the measurement results. The sources of these errors are the visible satellite, the communication channel, the receiver, and the surroundings to the receiver. The error sources that add errors of constant values will affect the accuracy of time transfer. The error sources that add errors of non-constant values will affect the accuracy and stability of the time and frequency transfer [8].

The sources of error contributed by the satellite come from the errors in the broadcasted ephemeris, the synchronization error of the clock on-board the satellite, and the delay of the satellite hardware. The sources of error contributed by the receiver come from the errors in its position, the synchronization error of its internal clock, the delay in the antenna and antenna cable, the hardware delay, and the delay in the coaxial cables connecting the external timing signal to the receiver [7]. The errors added by the communication channel are mainly due to the layers of ionosphere and troposphere.

In general, any GNSS measurement is based on measuring the pseudorange between the transmitter and the receiver according to the following equation:

$$P = \sqrt{(X_r - X_s)^2 + (Y_r - Y_s)^2 + (Z_r - Z_s)^2} + \\ + c[\Delta t_r - \Delta t_s] + T_s + I_s + \varepsilon, \quad (1)$$

where X_r, Y_r, Z_r are the receiver coordinates and X_s, Y_s, Z_s are the satellite's coordinates. Δtr is the synchronization error between the receiver's internal clock and the GNSST and Δts is the synchronization error between the transmitter's internal clock and the GNSST. Ts and Is are the tropospheric and ionospheric delays respectively, and ε represent the errors due to the extra delays due to geographic effects (like tide and multipath errors). The first term in eqn.1 represents the geometric path delay between the transmitter and receiver. Since the receiver coordinates are a probable source of errors, then it is highly recommended that timing receivers are fixed with a very well-known coordinate.

The ionospheric delay amounts to 65 ns while the tropospheric delay amounts to 6 ns: 10 ns. The other geographic effects cause a delay of about 2 ns. The combined errors due to the positions of the transmitter and the receiver amount to 10 ns at the most. The combined errors due to the antenna, the antenna cable, and the receiver's hardware are in the range of 100 ns. All these error sources can be estimated and their effect can be minimized. The other error sources are the surroundings of the receiver that make the transmitted signal suffer from multipath reflections before arriving the receiver, which is called multipath error. Multipath errors don't have a constant value, but they are having periodicity similar to the orbital periodicity of the GNSS [9-11].

The main errors added during the one-way time transfer are due to the quality of receiver calibration, multipath reflections, and the ionospheric delays. The receiver calibration is done according to a standard procedure, multipath reflections can be mitigated using chock ring antenna and other processing techniques, and the ionospheric delays can be compensated by using the dual frequency time transfer [7].

Comparing two distant clocks using the common-view time transfer should be done using the same satellites at the same time such that every clock is compared to the clock on-board the commonly visible satellite. This means that all the errors contributed by the satellite will be cancelled out. Moreover, the ionospheric delays will be either completely or partially cancelled out depending on the symmetry of the distance between the two clocks with respect to the observed satellite. So, the remaining ionospheric error in the common-view is much less than in the one-way time transfer and even this small value can be compensated by using the two-color technique [10]. So, the source of error that cannot be completely cancelled out in the common-view time transfer is the multipath reflections. [12].

3. The Common-view Time Transfer Using GPS, Galileo, GLONASS, BeiDou-2, and BeiDou-3

In this study, the author made a comparison between two pairs of distant clocks that are located at national timing centers using GPS, Galileo, GLONASS, BeiDou-2, and BeiDou-3. The first pair is distant by about 751 Km and is located at the Physikalisch-Technische Bundesanstalt (PTB) of Germany and the National Physical Laboratory (NPL) of the United Kingdom. The second pair is distant by about 10532 Km and is located at the National Time Service Center of China (NTSC) and the Institute of Photonics and Electronics, Czech Academy of Sciences (TP) of the Check Republic. PTB, NPL, NTSC, and TP are specially selected for making this study because they are operating multisystem and multichannel dual-frequency GNSS receivers. NPL and PTB are operating PolaRx5TR receiver, while NTSC and TP are operating GTR55 receiver. Although PTB is the pilot laboratory in the time transfer network, but till now PTB don't published data for BeiDou-3. In general, there is a very small number of timing laboratories that are publishing data for BeiDou-3.

The common-view technique is equivalent to making the one-way technique at both laboratories at the same time, using the same satellites, and using the same algorithm. So, the software tool used in the common-view analysis is a modified version of the one-way software tools that were built by the author [6,13]. This tool was used in analysing the time data that are generated during a period of 60 days (from MJD 59853 to MJD 59913).

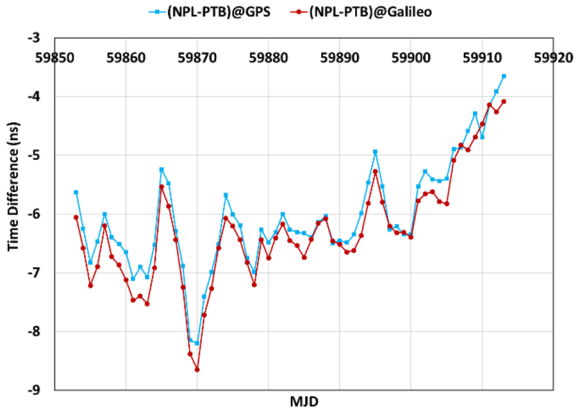
3.1. Comparing UTC(NPL) and UTC(PTB) Through the Common-view Time Transfer Using GPS, Galileo, GLONASS, and DeiDou-2

UTC(NPL) and UTC(PTB) are representing the national time scales of the United Kingdom and Germany respectively. These time scales are generated from atomic frequency standards. The distance between Teddington, where NPL exists, and Braunschweig, where PTB exists, is about 751 km. The German and British laboratories are operating the

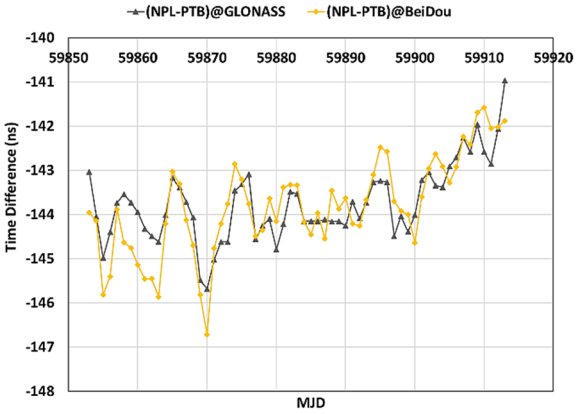
same model of the GNSS timing receiver; which is PolaRx5TR. This receiver is capable of receiving the signals of GPS, Galileo, GLONASS, and BeiDou-2, but it is calibrated only for GPS and Galileo at both laboratories.

Fig. 1 shows the common-view time difference between the British and the German time scales using GPS, Galileo, GLONASS, and BeiDou-2. All the data received from all the commonly visible satellites were considered in the calculations. Comparing the results shown in Fig. 1a and 1b, we find that there is an average time offset of about 135 ns between the results of GLONASS and BeiDou-2 and the results of GPS and Galileo. This large time offset comes from using un-calibrated GLONASS and BeiDou-2 receivers while using calibrated GPS and Galileo receivers. The small difference between the results of GPS and Galileo comes from the difference between GPS and Galileo in the quality of the transmitted ephemeris and the higher immunity of Galileo signals to multipath reflections.

Fig. 2 shows the instability of the common-view time difference between NPL and PTB using all the commonly visible satellites for the four GNSS. It's clear that BeiDou-2 has the worst stability in time transfer.



a. Using GPS and Galileo.



b. Using GLONASS and BeiDou-2.

Fig. 1. The time difference [UTC(NPL) - UTC(PTB)] using the common-view time transfer.

In a previous study made by the author [6], it was proved that the satellites constituting the same GNSS may differ in performance when used in time transfer. So, the author calculated the time difference between NPL and PTB using GPS using all the commonly visible satellite, using the best commonly visible satellite (G27), the worst commonly visible satellite (G08), and a group of the commonly visible satellites (the best four stable satellites). Fig. 3 shows the results of the four cases. Now, it is clear that using all the visible satellites in the common-view time transfer gives the most stable results.

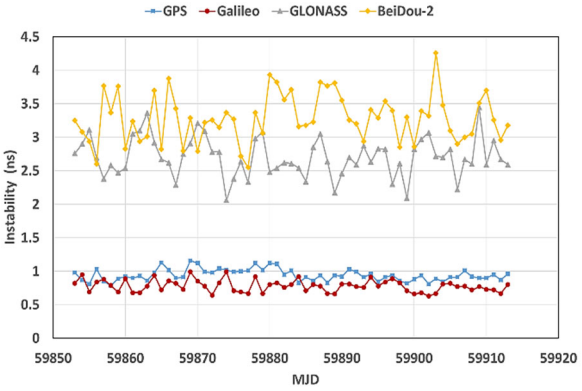


Fig. 2. The instability of the common-view time difference between NPL and PTB using GPS, Galileo, GLONASS, and BeiDou-2 using all the commonly visible satellites.

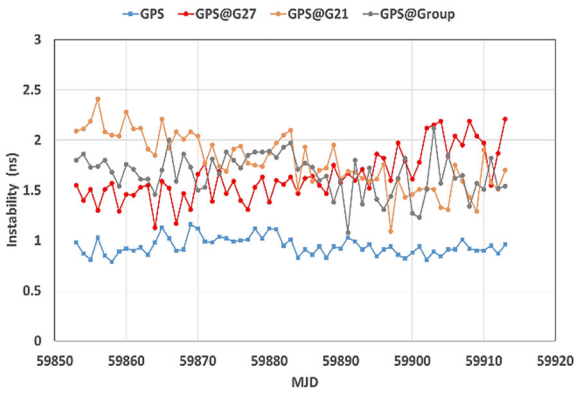


Fig. 3. The instability of the common-view time difference between NPL and PTB using all the visible satellites, the worst and best satellite, and a group of satellites of GPS.

3.2. Comparing UTC(NTSC) and UTC(TP) Through the Common-view Time Transfer Using GPS, Galileo, GLONASS, and DeiDou-3

UTC(NTSC) and UTC(TP) are representing the Chinse and the Czech national time scales respectively. The distance between Lintong, where NTSC exists, and Praha, where TP exists, is about 10532 km. Both the Chinse and the Czech laboratories are operating the same model of the GNSS timing

receiver (GTR55); which is calibrated for GPS at both laboratories. The calibration of the GPS receiver at both laboratories caused a large offset between the result of GPS and the results of the other three GNSS; as shown in Fig. 4. It's clear that the large distance between the two sites negatively affected the number of the commonly visible satellites; which is represented by missing the time difference between the two laboratories at MJD 59897 and MJD 59898.

In general, the accuracy of the time difference doesn't necessarily reflect the accuracy of the GNSS in the common-view time transfer because the parameter that mostly affects the accuracy is the quality of calibrating the GNSS receivers at both sites. On the other hand, the stability of the results can only represent effectively the stability of the GNSS if most of the common error sources are correlated.

Fig. 5 shows the daily instability of the common-view time difference between NTSC and TP using GPS, Galileo, GLONASS, and BeiDou-3 (using all the commonly visible satellites). It is clear that the stability of BeiDou-3 is comparable to the stability of GPS and Galileo.

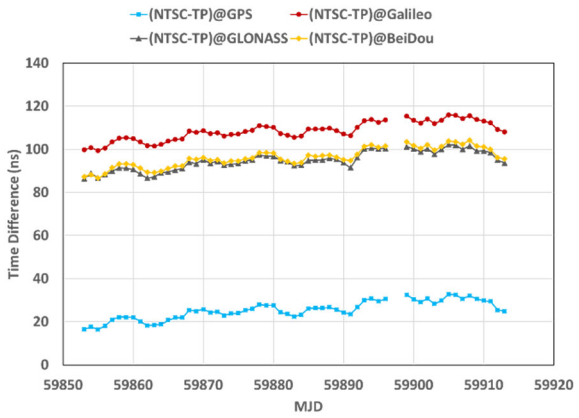


Fig. 4. The time difference [UTC(NTSC) - UTC(TP)] using the common-view time transfer using GPS, Galileo, GLONASS, and BeiDou-3.

When we compare Fig. 2 and Fig. 5, we notice that GPS and Galileo had worse stability when used in comparing very far frequency sources; which are NTSC and TP. This means that the distance between the two sites is a factor affecting the time transfer stability. The stability of the time transfer using GLONASS is almost the same in the two Fig. 2 and Fig. 5. GLONASS is the sole GNSS that is operated according to the Frequency Division Multiple Access technique (FDMA), while the other GNSSs are operating according to the Code Division Multiple Access (CDMA) technique.

4. Conclusion

Time and frequency transfer using the common-view technique can be used in comparing distant frequency standards. This technique is equivalent to making the one-way time transfer at the two distant sites provided that the measurements are done at the same time, using the same satellites, and using the same algorithm. The results are then exchanged for calculating the time difference between the two frequency standards. The error sources affecting the common-view time transfer are much less than the error sources affecting the one-way time transfer provided that the common error sources are being correlated. As the distance between the two frequency standards decreases as this correlation increases. So, the common-view technique is more effective when the two frequency standards are close to each other as much as possible. Moreover, the channel access technique used by the GNSS affects the time transfer stability.

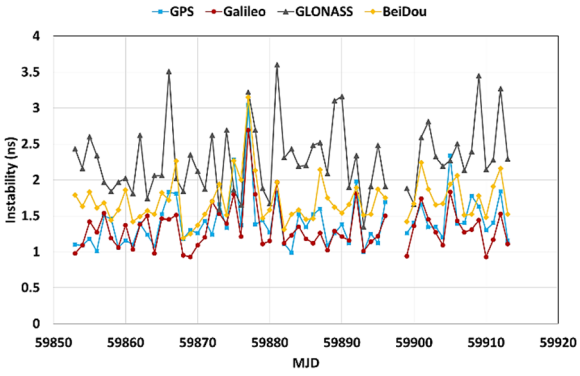


Fig. 5. The daily stability of the common-view time difference between NTSC and TP using GPS, Galileo, GLONASS, and BeiDou-3 using all the commonly visible satellites.

It was proved before by the author that there are differences between the satellites in the same GNSS. So, it was expected that using the best satellites in time comparisons may results in more stable results. The results represented in Fig. 3 contradicted this expectation and, now, it is clear that as the number of the commonly visible satellites increases as the stability of the common-view time transfer improves. Selecting the best satellites may be more effective in the one-way time transfer. Adding more GNSS systems or modernizing the current GNSS has a good impact on both navigation and timing, especially when they are combined.

BeiDou-3 has a much better stability than BeiDou-2. Now, the stability of BeiDou-3 in time transfer became comparable to the stability of GPS and Galileo. So, BeiDou-3 is a plus to the navigation and timing applications.

Acknowledgements

The author would like to thank the colleagues at PTB, NPL, NTSC, and TP for making their data available to the community of time metrology.

References

[1]. V. Reinhardt, J. Lavanceau, A Comparison of the Cesium and Hydrogen Hyperfine Frequencies by Means of Loran-C and Portable Clocks, in *Proceedings of the 28th Frequency Control Symposium*, 1974, pp. 379-383.

[2]. P. Parcelier, Time Synchronization by Television, *IEEE Trans. Instrum. Meas*., Vol. 4, 1970, pp. 233-238.

[3]. W. Klepczynski, GPS for precise time and time interval measurement, in Global Positioning System: Theory and Applications, *American Institute of Aeronautics and Astronautics Inc.*, 1996, pp. 483-500.

[4]. D. Kirchner, Two-way time transfer via communication satellites, *Proceedings of the IEEE*, Vol. 79, Issue 7, July 1991, pp. 983-990.

[5]. S. Yokota, et al, Accuracy of two-way satellite time and frequency transfer via non-geostationary satellites, *Metrologia*, Vol. 42, Issue 5, 2005, pp. 344-350.

[6]. G. G. Hamza, Analysis of Different Global Navigation Satellite Systems in Time Transfer, *IEEE Communications Magazine*, Vol. 60, Issue 2, February 2022, pp. 67-72.

[7]. P. J. G. Teunissen, O. Montenbruck, Chapters 15, 41, in Springer Handbook of Global Navigation Satellite Systems, Vol. 10, *Springer International Publishing*, 2017.

[8]. J. Levine, Time and frequency distribution using satellites, *Reports on Progress in Physics*, Vol. 65, Issue 8, 2002, pp. 1119-1164.

[9]. J. Levine, A review of time and frequency transfer methods, *Metrologia*, Vol. 45, Issue 6, 2008, pp. 162-174.

[10]. J. Levine, Measuring time and comparing clocks, in Handbook of Measurement in Science and Engineering (M. Kutz, Ed.), *Wiley*, 2016, pp. 2109-2162.

[11]. D. Allan, C. Thomas, Technical directives for standardization of GPS time receiver software, *Metrologia*, Vol. 31, Issue 1, 1994, pp. 69-79.

[12]. European GNSS (Galileo) Open Service Signal-in-Space Interface Control Document, *European GNSS Service Centre*, 2021.

[13]. G. G. Hamza, Smart Interpreter for the Common Generic GNSS Time Transfer Standard Data Files, in *Proceedings of the 3rd IFSA Frequency and Time Conference (IFTC'21)*, September 22-24, 2021, Spain, pp. 5-10.