ePRTC

White Paper

The Enhanced Primary Reference Time Clock (ePRTC) as a Solution for GNSS Vulnerability

Microsemi
Power Matters.™

Abstract

The significant dependence on global navigation satellite systems (GNSS) as a timing source for synchronizing both wired and wireless telecommunications networks has created potential network reliability issues and security risks. Governments, major telecom and mobile operators, and enterprises are now urgently looking for a way to protect their networks against both regional GNSS issues as well as a potential global GNSS outage. This white paper describes a solution, called the Enhanced Primary Reference Time Clock (ePRTC), which is designed to address the growing issue of GNSS vulnerability. The objective of the ePRTC solution is to generate time by producing its own independent TimeScale that is aligned with GNSS while at the same time maintaining the autonomy of ePRTC-generated phase, time, and frequency signal outputs. The ePRTC system provides secure infrastructure that reduces dependency on GNSS in general, enabling a network operator to take back control of the timing source used for network synchronization.

Introduction

On January 27, 2016, the United Stated Air Force issued the following press release:

Figure 1 U.S. Air Force Official Press Release

AIR FORCE OFFICIAL PRESS RELEASE - GPS GROUND SYSTEM ANOMALY

JAN 27, 2016

On 26 January at 12:49 a.m. MST, the 2nd Space Operations Squadron at the 50th Space Wing, Schriever Air Force Base, Colo., verified users were experiencing GPS timing issues. Further investigation revealed an issue in the Global Positioning System ground software which only affected the time on legacy L-band signals. This change occurred when the oldest vehicle, SVN 23, was removed from the constellation. While the core navigation systems were working normally, the coordinated universal time timing signal was off by 13 microseconds which exceeded the design specifications. The issue was resolved at 6:10 a.m. MST, however global users may have experienced GPS timing issues for several hours. U.S. Strategic Command's Commercial Integration Cell, operating out of the Joint Space Operations Center, effectively served as the portal to determine the scope of commercial user impacts. Additionally, the Joint Space Operations Center at Vandenberg AFB has not received any reports of issues with GPS-aided munitions, and has determined that the timing error is not attributable to any type of outside interference such as jamming or spoofing. Operator procedures were modified to preclude a repeat of this issue until the ground system software is corrected, and the 50th Space Wing will conduct an Operational Review Board to review procedures and impacts on users. Commercial and civil users who experienced impacts can contact the U.S. Coast Guard Navigation Center at (703) 313-5900.

Fortunately, there was not a single critical network outage that was reported from the Microsemi customer base resulting from this event. Although there were many concerns reported from major telecom operators and government institutions across the globe, network operations remained in full service without disruption.

While the incident described was an anomaly, there have been a growing number of intentional and unintentional GNSS interruptions, and dependency on GNSS time sources (GPS, Galileo, GLONASS, others) is becoming a major security vulnerability. The proliferation of GNSS as a timing source for wireless networks has further exacerbated the potential impact, to a point where governments, major telecom/mobile operators, and enterprises are now urgently looking for a way to protect their networks against both regional GNSS issues as well as the potential for a massive global GNSS outage.

Anti-jamming and anti-spoofing solutions can play a part in the protection of GNSS against jamming and spoofing threats that may be encountered in a telecom or mobile network. However, driven by industry standards for primary references, there is a better approach that not only protects the network but also provides a level of performance that has not been previously achieved.

This white paper describes a solution that meets new industry standards and addresses the growing issue of GNSS vulnerability. The solution not only identifies the technologies and products that can provide protection against GNSS anomalies and outages, it also offers an architecture that can enable a network operator to implement a synchronization network that is resilient to GNSS vulnerabilities of any magnitude.

The Synchronization Network

The goal of network synchronization is to get the best possible source of timing to all nodes of the network. The following two fundamental requirements must be in place to ensure network synchronization:

- An accurate source of time
- A “reliable messenger” that distributes timing to all of the nodes

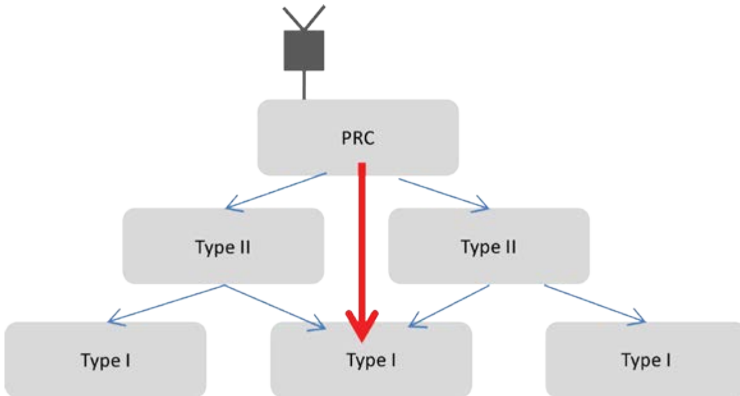
Synchronization in the Core

Looking back at how network synchronization was originally achieved, the architecture employed was based on hierarchical timing distribution.

Hierarchical timing distribution involves the establishment of a primary reference clock (PRC) location that feeds subtending nodes of either Type II clock or Type I clock quality. The PRC location fills the first fundamental requirement of the hierarchical network for an accurate “frequency” source. This location typically uses GNSS as a reference source.

The second requirement of hierarchical timing distribution is fulfilled by qualified connections that serve as reliable messengers for transporting timing from one node to the next. These links are typically engineered and maintained to minimize the effects of network rearrangements on synchronization distribution.

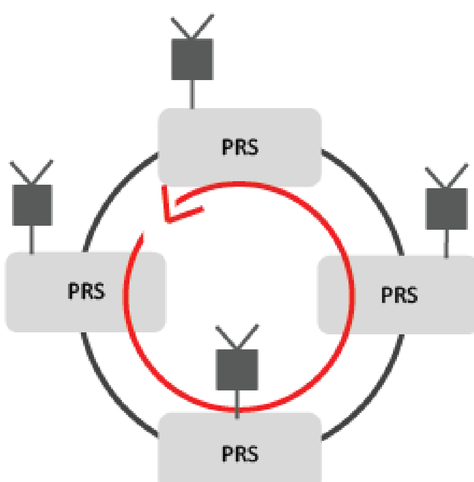
Figure 2 Hierarchical Timing Distribution



Network evolution has driven the core of the network toward transmission architectures that have made hierarchical frequency timing difficult to maintain. This was first seen with the introduction of the Synchronous Digital Hierarchy (SDH) and Synchronous Optical Network (SONET), where a ring-and-chain design and the introduction of intelligent connections resulted in unreliable synchronization paths. Furthermore, synchronization paths became subject to perturbations introduced by serial clocks embedded in the SDH/SONET equipment. Previously simple point-to-point connections were eventually replaced with routes that were frequently reconfigured, resulting in a broken timing hierarchy.

To ease administration of timing distribution in a world with better timing integrity, a new synchronization architecture was adopted. It was based on the approach of deploying a “distributed primary reference source (PRS)” using GNSS technology (originally, the choices were GPS and/or LoranC). Distributed PRS provided a way for network operators to utilize a separate time source that was independent of network transmission and to enable “flattening” of synchronization distribution, thereby removing the dependency on hierarchical timing connections.

Figure 3 Distributed PRS (Frequency)



Over the last decade, distributed PRS has become a pervasive solution for timing in network cores, to the point where hundreds, and in some cases thousands, of GNSS receivers are relied upon for network synchronization.

Synchronization at the Edge

Wireless network build-out is now the primary driver of revenue growth for telcos. For mobile access points to support the latest over-the-air interfaces and to achieve the highest network speed possible, each mobile access point needs to be aligned “in time” with one another. As mobile technology advances from 3G to 4G to 5G, and as densification in mobile access points increases, the need for accurate frequency and time alignment between mobile access points has become even more stringent.

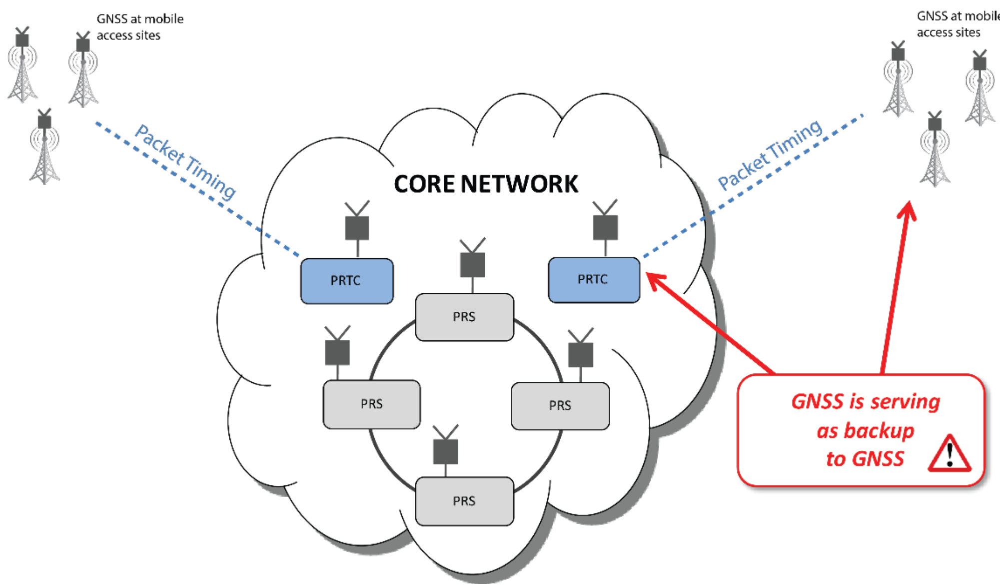
The solution for accurate time distribution for mobile networks, once again, has primarily been GNSS because of its simplicity and low cost of deployment. However, the industry widely recognizes that the near ubiquitous deployment of GNSS at all mobile/cell sites has created a huge dependency on GNSS. While the low cost of GNSS deployment was initially attractive to operators, the massive dependency has suddenly created a significant operational network expense. Specifically, when GNSS failures occur, mobile operators usually need to dispatch maintenance personnel to the location for troubleshooting and repair. Not only is this expensive, but it is also unmanageable, as the number of technicians required to manage so many mobile access points is infeasible for most companies.

Additionally, government authorities recognize that the use of GNSS presents a single point of failure that can bring down a country’s communications infrastructure in a catastrophic way. In fact, this dependency has reached a level of concern where governments around the globe are requiring mobile operators to develop a more secure approach to timing distribution.

In parallel with the rapid deployment of next generation mobile access technologies, the deployment of packet networking throughout a mobile operator’s backhaul and core infrastructure is occurring. As deployment of mobile access points proliferate, packet networking for connection of the mobile access point back to the core of the network is the primary transmission method used. Although packet networking provides a number of benefits, one pitfall is that the use of a packet network connection for the distribution of time is difficult due to the nondeterministic behavior of a packet network.

Fortunately, the industry has set standards for how accurate time can be transported over a packet network. IEEE1588-2008 is the current leading standard of timekeeping. The International Telecommunication Union Telecommunication Standardization Sector (ITU-T) organization developed a series of standards (referred to as the “1588 Packet Timing Protocol”) specifically for transport of time over packet networks, and these standards define profiles for Telecom operation of precision time protocol (PTP) and synchronous Ethernet (SyncE). These standards have driven mobile operators to deploy a new generation of time distribution systems referred to as a primary reference time clock (PRTC). Using PRTC systems (such as Microsemi’s TimeProvider 5000), mobile operators are now using packet time distribution as a way to get timing to a mobile access point as a back-up to locally provided GNSS time delivery.

Figure 4 GNSS in the Core Network and Mobile Access Sites



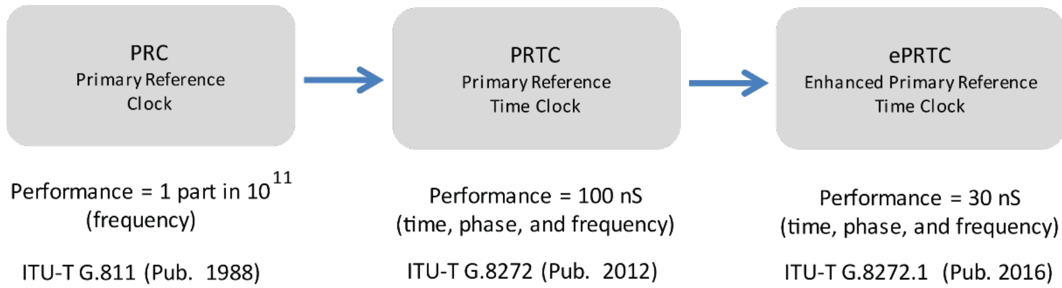
Although the deployment of PRTC systems in the core network to deliver frequency and time over packet networks to mobile access points has proven to be a viable back-up architecture for localized GNSS failures, the ultimate dependency on GNSS in the core network remains. In fact, the GNSS deployed at the mobile access site is actually being backed up by GNSS in the core, and the net result is that the dependency on GNSS remains.

Industry Standards

When looking at the evolution of primary reference standards as developed by the ITU-T, the original specification was for a primary reference clock (PRC) and was called G.811. The G.811 requirement describes a PRC that delivers 1×10^{-11} frequency accuracy and is suitable for frequency synchronization (also known as syntonization) of other clocks within a network. As packet timing requirements emerged, ITU-T developed the primary reference time clock (PRTC) standard to include the requirements for time and phase for transport over a packet network. This standard is known as G.8272 and was originally published in 2012. The G.8272 standard describes a clock that delivers <100 nS phase and time performance suitable for packet networks.

With the need to increase performance for phase and time to meet the requirements of emerging mobile access network technologies and improve security for protection against GNSS outages, the ITU-T has recently consented a new standard called the enhanced primary reference timing clock (ePRTC). This new standard (G.8272.1) calls for performance levels and reliability that will set the foundation for time, phase, and frequency for many years to come.

Figure 5 Evolution of Primary Reference Standards



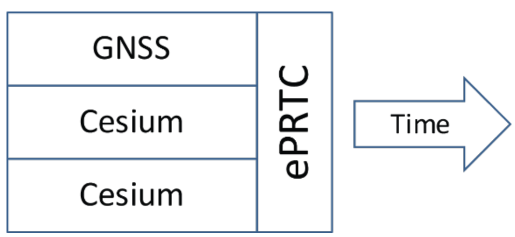
The remainder of this paper looks at the components that comprise an ePRTC system, and how this system performs in both normal operating conditions and during GNSS outages.

ePRTC Solution Overview

The core components of an ePRTC solution include the following:

- GNSS
- Atomic clocks (typically cesium or better)
- ePRTC system

Figure 6 Enhanced Primary Reference Time Clock (ePRTC)



Key attributes of an ePRTC include the following:

- The ePRTC supports a high level of accuracy (Accurate to within 30 ns or better when verified against the applicable primary time standard, such as UTC) and is subject to more stringent output performance requirements when compared to today's PRTC systems.
- An ePRTC is an autonomous source of time that uses one or two co-located atomic clocks to provide the required performance for both time and frequency, even when connection to GNSS is lost.
- An ePRTC delivers a higher level of operational reliability to ensure operators can maintain required time and frequency service performance for long periods regardless of the availability of GNSS.

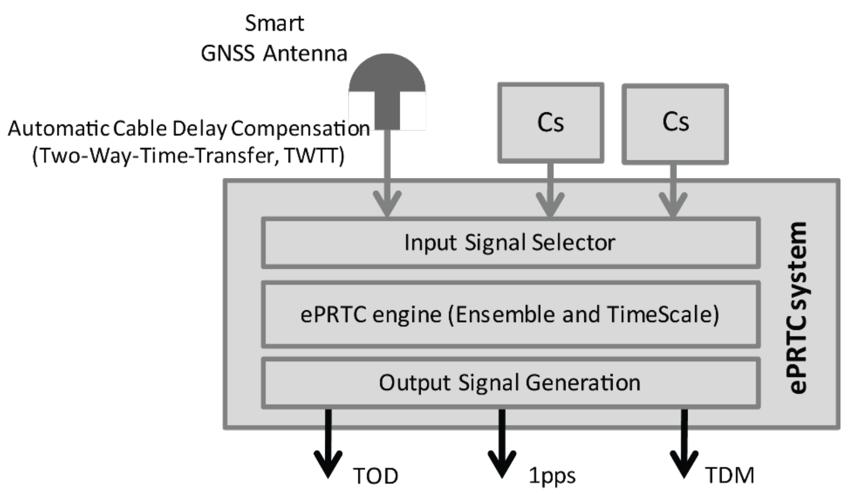
The objective of the ePRTC solution is to generate time by producing its own independent TimeScale that is autonomous. The TimeScale provides time, phase, and frequency that are aligned and calibrated to the GNSS signal over a long observation period, and then the TimeScale is maintained autonomously based on the stability of the atomic clock(s). The frequency stability of the atomic clocks serves as a reference for the ePRTC TimeScale. This is the key distinguishing feature when comparing an ePRTC to a PRTC. In the case of a PRTC, time is coming directly from GNSS. In the ePRTC, the TimeScale is generated locally. Details of this operation will be discussed later in this document.

An ePRTC takes the approach of the famous saying: “The best defense is a good offense.” Instead of defending against GNSS attacks, the ePRTC goes on the offense and generates its own independent time that is not subject to attacks such as spoofing and jamming.

ePRTC System Operation

The ePRTC system itself (typically a rack-mounted unit) comprises three primary elements: the input selector, the ePRTC engine, and output signal generation. Also deployed with the ePRTC system is the GNSS smart antenna along with external/standalone cesium clocks.

Figure 7 ePRTC System Block Diagram



Inputs to the ePRTC system include an interface for the smart GNSS antenna along with 10 MHz interfaces to external atomic clocks (typically cesium). At a minimum, a GNSS input and at least one cesium clock should be connected.

The ePTRC engine provides two primary functions: (1) Ensemble and (2) TimeScale. The Ensemble function is used when there are two cesium clocks connected to the system. Using an ensemble algorithm to measure and compare the stability of the individual cesium clocks, a higher level of accuracy can be produced. Further, by using two cesium clocks, there are operational advantages as one of the cesium clocks can be removed from service during system operation without performance degradation.

The TimeScale function provides time and phase and delivers it autonomously. The ePRTC system references GNSS as the basis for the TimeScale; however, GNSS is used as an untrusted source of time. Instead of assuming that the GNSS time is correct, the ePRTC system evaluates and measures its own autonomous TimeScale relative to GNSS. Using patented measurement algorithms, the ePRTC adjusts its timescale as needed but does not blindly follow GNSS time. The approach with the ePRTC system is that the TimeScale becomes the master source of time, and the cesium clocks and GNSS are used to help maintain the accuracy of the ePRTC TimeScale.

Output signal generation is available from the ePRTC system in a number of formats, including Time-of-Day (TOD), 1PPS, and traditional timing formats such as E1 and DS1 formats. The ePRTC system is not intended to be a large scale distributor of timing outputs, and it is designed for integration with systems like an SSU a Time Grand Master to provide high-capacity PTP and NTP signal outputs.

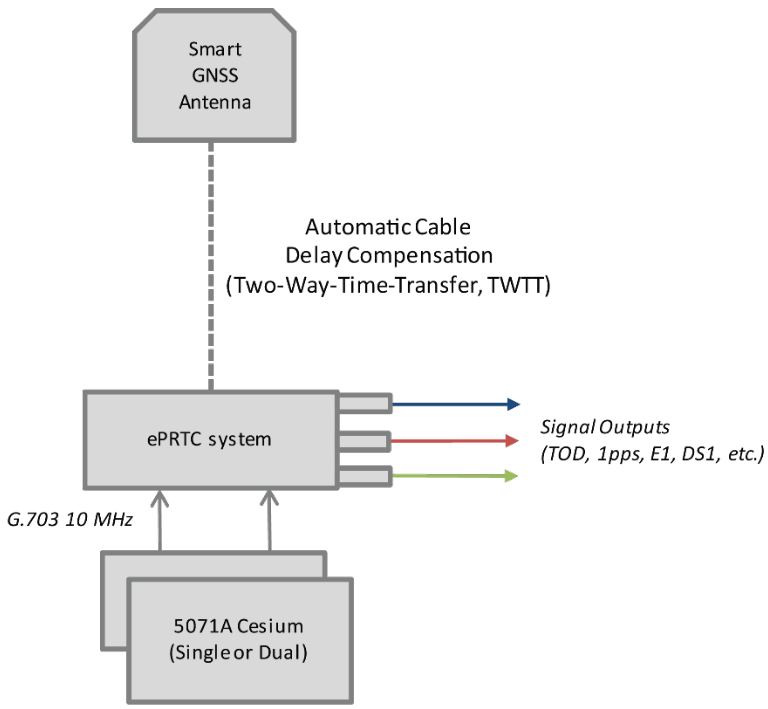
ePRTC Smart Antenna with Automatic Cable Delay Compensation

A key technology of the Microsemi ePRTC system is a unique antenna design that resolves the following key challenges:

- Automatically compensates for phase offsets caused by variable cable lengths between antenna (outdoor) and signal generation and distribution (indoor)
- Reduces installation and set-up costs
- Protects against spoofing and jamming with smart signal receiver algorithms

The following diagram provides an overview of how the antenna and ePRTC system are deployed.

Figure 8 Smart GNSS Antenna and Automatic Cable Delay Compensation Using TWTT



The reception of the GNSS signal and the conversion of the signal for digital consumption all occur in the antenna enclosure, eliminating delays between the GNSS reception and conversion to digital format. Using standard coaxial cable for the physical connection between the smart GNSS antenna and the ePRTC system, a unique Two-Way-Time-Transfer (TWTT) protocol transfers UTC-traceable time. Furthermore, the TWTT transmission of UTC time occurs automatically and is calibrated so that the phase delays caused by varying cable lengths are removed.

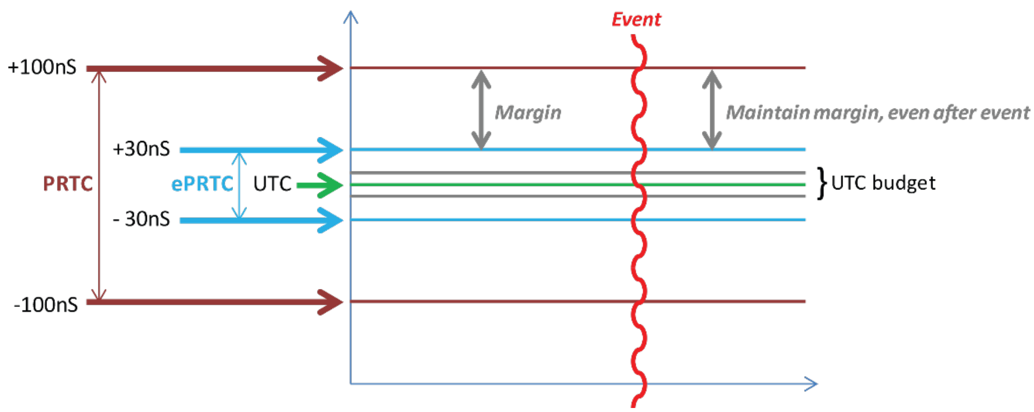
Using the smart GNSS antenna and the TWTT transmission, the ePRTC system is able to receive UTC time with the required accuracy to enable delivery of <30 nS on the ePRTC outputs.

ePRTC Performance

The performance of an ePRTC system is characterized by verifying its accuracy as compared to a primary reference standard such as UTC. Details of the required performance levels, including MTIE and TDEV masks, are contained in the ITU-T G.8272.1 specification; however, the key performance requirement of the ePRTC is to be accurate to within <30 nS when verified against the applicable primary time standard.

The <30 nS requirement is driven by the need to maintain an overall small error budget as time is passed from the core to the edge of the network. The more accurate time can be maintained from the ePRTC, the greater the accuracy that can be achieved throughout the network. The goal is to create as much margin as possible so that time and phase alignment is optimized throughout the network.

Figure 9 Performance and Error Budget



The diagram above provides a simple view of the performance objectives for the ePRTC. It is important to note that the 30 nS accuracy should be maintained during normal operating conditions (when GNSS is available) and, even more importantly, after an event such as when a GNSS outage has occurred.

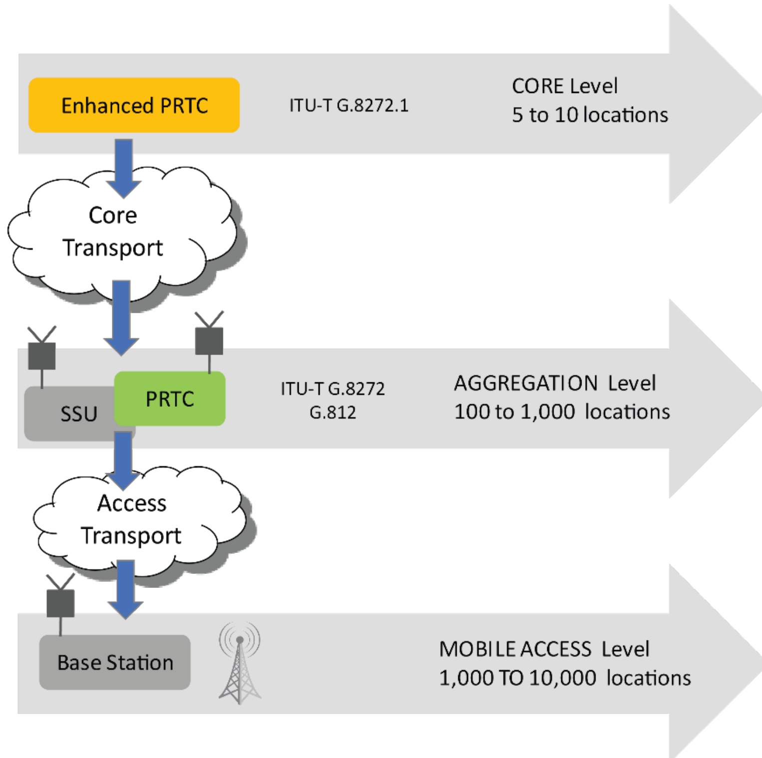
In the case of a GNSS outage, the ePRTC system enters a holdover mode and can achieve this without interruption of the output signals given that, prior to the outage, the outputs were already being driven by the internal TimeScale engine. Once in holdover mode, the TimeScale engine continues to use the cesium clocks as a stable frequency source and maintains phase and time even though GNSS is lost. Per the G.8272.1 standard, once in holdover, the output of the ePRTC system can increase linearly from 30 nS to 100 nS over a fourteen-day period. With this performance, subtending PRTC systems can then meet their accuracy budget of <100 nS when referenced to the ePRTC.

Additionally, maintaining 30 nS performance should take into account all noise types, including time error offsets and phase error. To ensure that all noise types are compensated for, the ePRTC system should be set up, tested, and allowed to operate for at least 30 days before going into service. Annual maintenance measurements are also recommended to ensure ongoing performance and operation.

ePRTC Deployment

To some degree, deployment of ePRTC systems is a return to pseudo-hierarchical network synchronization. The deployment architecture is structured such that ePRTC systems are deployed at a tier above subtending aggregation locations. The aggregation locations typically include synchronization supply unit (SSU) systems that are primarily used for frequency distribution, and primary reference time clocks (PRTC) for packet timing. From the aggregation locations, timing signals are distributed through the access transport for delivery of time to the base stations or other mobile network infrastructure.

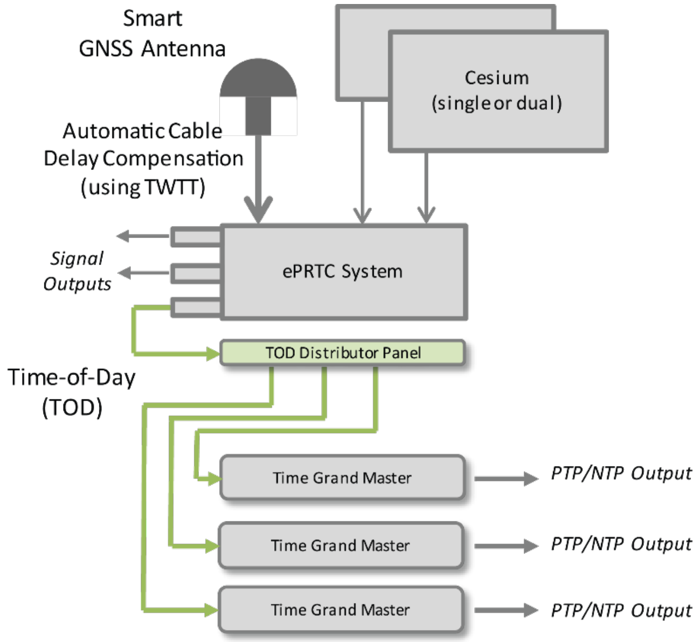
Figure 10 ePRTC Deployment



The number of ePRTC locations varies depending on an operator's network geographical coverage. The key objective is to deliver the highly-accurate time produced by the ePRTC to each aggregation node with minimal time error and with the highest possible level of efficiency, scalability, and fault tolerance.

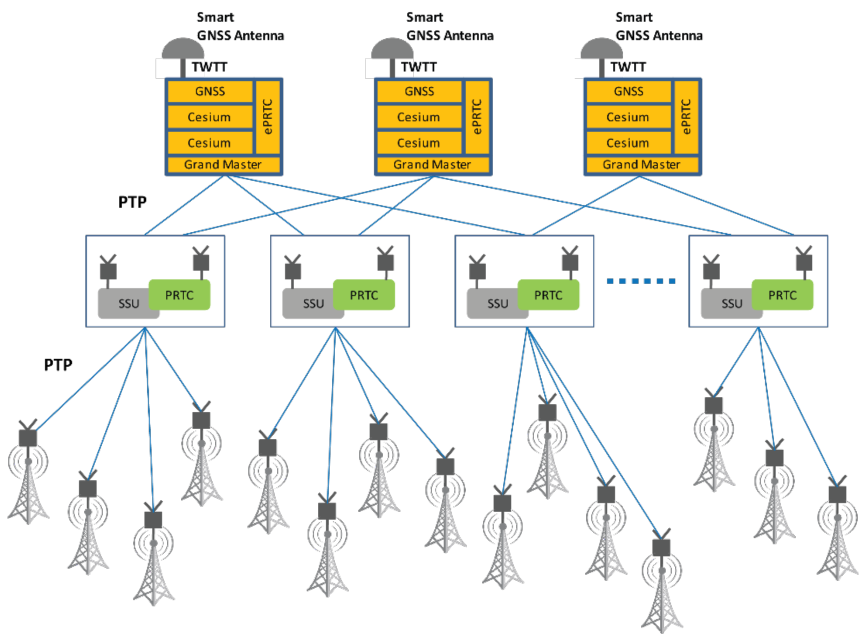
The ePRTC system is not intended to be a large-scale distributor of timing outputs. Typically, the ePRTC integrates with systems like a Time Grand Master to provide a larger number of SyncE, PTP, and NTP timing outputs for synchronizing sub-tending aggregation nodes. Connection between the ePRTC and Time Grand Master is done using the TOD interface. With TOD, multiple Time Grand Master systems can be connected directly to the ePRTC for modular and efficient scaling.

Figure 11 ePRTC and Time Grand Master Integration



Network deployment of ePRTC systems is done using an optimized architecture that limits the number of hops between the ePRTC and the subtending aggregation nodes, and also enables a single aggregation node to receive timing from at least two different ePRTC sources. The deployment of ePRTC systems in the core of the network may use a "Leaf-Spine" network topology similar to that used in data center design. This type of architecture is ideal, as core networks transition from legacy transmission to an all-packet network.

Figure 12 ePRTC Network Deployment



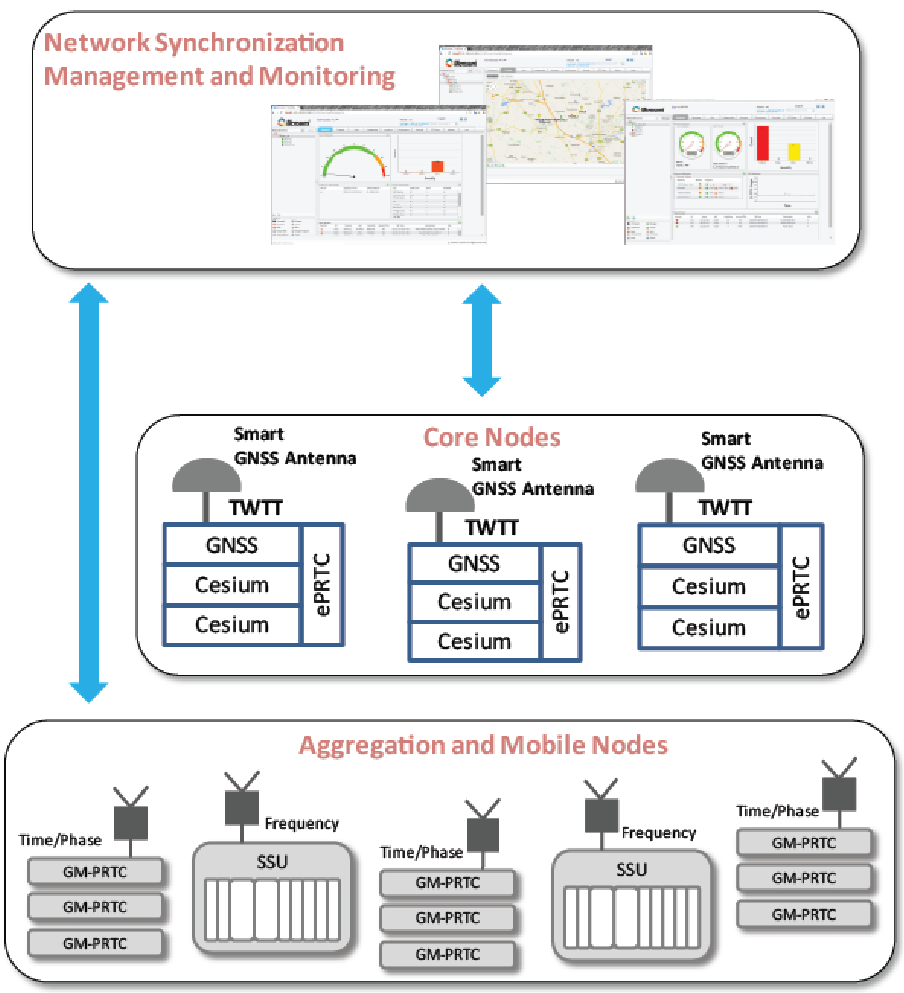
The architecture in the previous illustration limits the core and aggregation synchronization network to just two layers: the Leaf (Aggregation nodes) and Spine (Core nodes). This helps to maintain predictability between the ePRTC and subtending SSU and PRTC systems.

ePRTC Management

The deployment of ePRTC systems is ultimately about improving the overall network synchronization performance for phase, time, and frequency, and improving reliability with the emphasis on protecting the synchronization network from GNSS outages. To succeed with these objectives, it is important to monitor and measure the results on a continuous basis. This means having a unified view of the entire synchronization network from the core to the edge.

As network operators transition their overall network architectures towards a software-defined network (SDN), the strategy for network synchronization deployment needs to be mapped into this model as well. Synchronization performance needs to be viewed with end-to-end network visibility where the most important measurable outcome is how well nodes throughout the network are aligned in phase, time, and frequency.

Figure 13 ePRTC Network Management and Monitoring



Through the use of network synchronization management software (such as Microsemi's TimePictra software), synchronization performance can be viewed with end-to-end network visibility encompassing ePRTC systems at key timing hub locations and sub-tending aggregation and edge nodes. This enables the network operator to measure how well phase, time, and frequency are delivered throughout the network. Having a bird's-eye view of the synchronization network and performing 24/7 management and monitoring is an integral part of the solution, enabling network operators to respond quickly when GNSS outages threaten the network.

Conclusion

Telecom and mobile operators have benefited from the simplicity of deployment that GNSS provides as a network timing reference. As a result, GNSS has been deployed broadly from the core to the edge of the network. However, the threat of GNSS vulnerabilities has become real. Events such as signal anomalies, regional disruptions, and even global outages have prompted governments across the globe to ask their primary network infrastructure providers for a plan to defend against this serious threat.

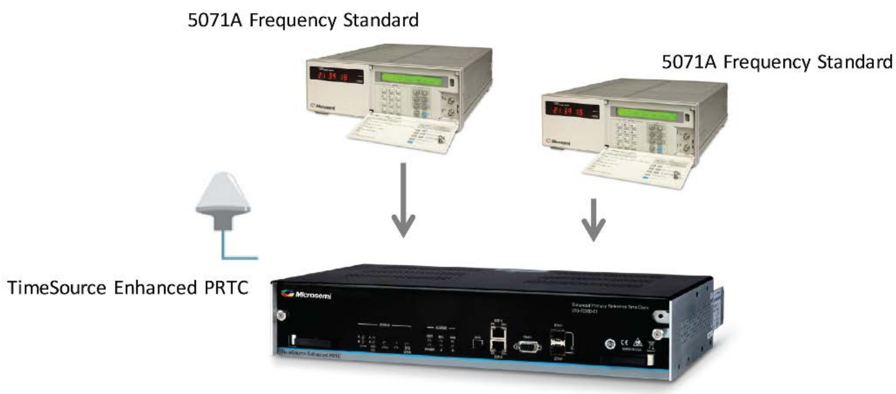
Anti-jamming and anti-spoofing products provide a level of protection; however, these solutions focus on defending against attacks and can be difficult to deploy on a wide geographical basis given that each site would need to be surveyed, and installation costs (such as accessing rooftops) can be expensive. A more permanent, scalable, and efficient solution is to reduce dependency on GNSS and to take back control of the timing source used for network synchronization.

ITU has recently consented a new standard (G.8272.1) which specifies requirements for an Enhanced Primary Reference Time Clock (ePRTC). The ePRTC provides two key benefits:

- It delivers a high level of performance of better than 30 nS accuracy when measured against a primary standard such as UTC. This level of performance allows for an ePRTC to deliver time to sub-tending nodes within required network error budgets.
- It provides a solution that goes beyond mitigating the threat of GNSS by enabling operators to deploy an autonomous time source that is impervious to GNSS anomalies and outages.

Microsemi, as the world leader of network synchronization solutions, is introducing an industry-leading ePRTC solution based on the TimeSource Enhanced PRTC and 5071A cesium frequency standard. The ePRTC solution is available today along with services and support to help network operators with deployment and performance assurance.

Figure 14 ePRTC Solution: TimeSource Enhanced PRTC and 5071A Frequency Standard



Customers interested in the ePRTC solution should contact their local Microsemi-certified partner, or contact Microsemi directly at sales.support@microsemi.com.

Microsemi makes no warranty, representation, or guarantee regarding the information contained herein or the suitability of its products and services for any particular purpose, nor does Microsemi assume any liability whatsoever arising out of the application or use of any product or circuit. The products sold hereunder and any other products sold by Microsemi have been subject to limited testing and should not be used in conjunction with mission-critical equipment or applications. Any performance specifications are believed to be reliable but are not verified, and Buyer must conduct and complete all performance and other testing of the products, alone and together with, or installed in, any end-products. Buyer shall not rely on any data and performance specifications or parameters provided by Microsemi. It is the Buyer's responsibility to independently determine suitability of any products and to test and verify the same. The information provided by Microsemi hereunder is provided "as is, where is" and with all faults, and the entire risk associated with such information is entirely with the Buyer. Microsemi does not grant, explicitly or implicitly, to any party any patent rights, licenses, or any other IP rights, whether with regard to such information itself or anything described by such information. Information provided in this document is proprietary to Microsemi, and Microsemi reserves the right to make any changes to the information in this document or to any products and services at any time without notice.

Microsemi Corporate Headquarters
One Enterprise, Aliso Viejo,
CA 92656 USA
Within the USA: +1 (800) 713-4113
Outside the USA: +1 (949) 380-6100
Fax: +1 (949) 215-4996
Email: **sales.support@microsemi.com**
www.microsemi.com

About Microsemi

Microsemi Corporation (Nasdaq: MSCC) offers a comprehensive portfolio of semiconductor and system solutions for aerospace & defense, communications, data center and industrial markets. Products include high-performance and radiation-hardened analog mixed-signal integrated circuits, FPGAs, SoCs and ASICs; power management products; timing and synchronization devices and precise time solutions, setting the world's standard for time; voice processing devices; RF solutions; discrete components; enterprise storage and communication solutions; security technologies and scalable anti-tamper products; Ethernet solutions; Power-over-Ethernet ICs and midspans; as well as custom design capabilities and services. Microsemi is headquartered in Aliso Viejo, California, and has approximately 4,800 employees globally. Learn more at **www.microsemi.com**.

900-00759-000 A