Syncworks

Designing Around the Threat to Network Timing in Modern Networks

Introduction

As technology and services advance, the necessity of reliable network timing is more critical than ever. While legacy analog networks traditionally required frequency synchronization from a central source, properly functioning modern networks require increasingly precise references to single-clock sources. This is a modern demand for telecommunications, media, IT and utility networks. As is the case with all critical requirements, there exists the threat of disruption - both intentional and accidental. In the case of network timing, which is commonly derived from a GNSS (Global Navigation Satellite System) source like GPS, the intentional threat to disruption most often comes in the form of jamming or spoofing. The ease with which jamming and spoofing can be applied to GNSS systems has created the need to ensure that a common clock source can survive multiple types of disruption, be they local or widespread, short in duration or prolonged.

This paper will describe the current need for network timing and the reality of the threats against it. It will also explore the proper methodologies and systems that should be employed in network design and operation to protect the timing source and guarantee consistent, quality services.

What Makes Network Timing Critical

Data transactions between network equipment and applications that are distributed around the world are growing in number quickly year after year. Meanwhile, expectations for performance by users and service providers continue to get more demanding. Highspeed, low latency, high throughput networks are being deployed to enable the normal demand plus new services. IT networks are being designed with faster interfaces, faster processors, and faster storage to shave every possible microsecond off transactions.

Smart Grid technologies are revolutionizing how power is generated and distributed, saving energy, and improving the performance of utilities. 5G wireless technologies have been deployed to satisfy the rapid growth in the number of wireless devices, as well as the demand for high bit rate, low latency services. Edge networks are bringing formerly centralized functions closer to their consumers, further augmenting performance. All of this depends on geographically diverse network architectures to operate.

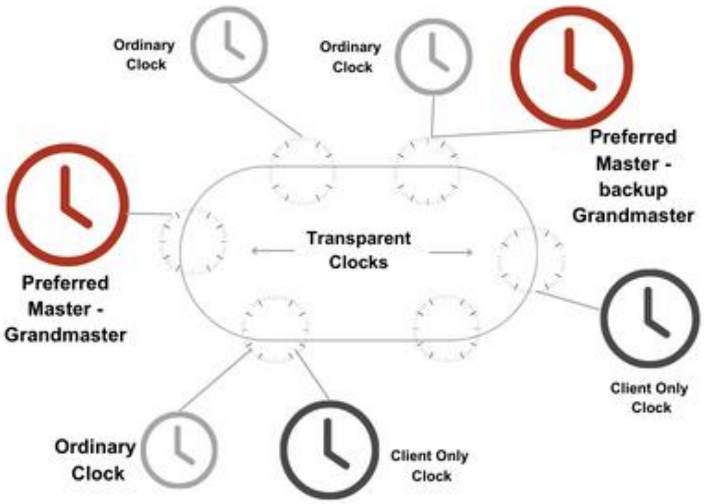
Synchronization of network time - down to the microsecond –is critical for network performance, stability and most importantly, security. This is not optional. Any drift from a commonly referenced time causes operations to unravel.

Precision Timing Protocol (PTP)

PTP is used to counteract this issue, with a standard reference source invariably derived from an RF signal transmitted by the different GNSS satellite networks in Earth's orbit. This is often achieved simply with an antenna at each location or for each different application. It is seemingly always available, which has caused a dependency that is now being exploited. GPS signals originate in space, far away from any terrestrial consumer of the signal. They are very low power, and well documented so the specifications are known. The signal can be spoofed and replaced with a similar signal of a higher power, or, more easily, jammed with different signal of a higher power. While spoofing is an intentional attempt to disrupt service reliant on GNSS signaling, jamming can be intentional or accidental. In modern war zones, jamming or spoofing GNSS signals is a standard tactic, as it is an effective way to insert chaos into standard operations, as well as disrupt tracking capabilities of weapons systems.

Even in peaceful regions, GPS jammers are widely available for purchase. Commercial drivers use them to disrupt monitoring of their delivery vehicle location or speed. Individuals use them to protect themselves from stalkers using tracking devices. Journalists and detectives may use them to avoid being tracked when meeting with confidential sources. Sometimes, car thieves will use them to avoid being caught. For just a few hundred US dollars, it is possible to purchase a handheld jammer that will disrupt an entire city block - including the critical networks that run through it. While network time may be an afterthought for many networks, protection from the harm that GPS disruption can cause is relatively inexpensive and should be a standard component of network architecture.

To fully appreciate the importance of designing timing resiliency for networks, it is important to understand the applications of PTP in several common modern networks. Wireline networks, 5G wireless networks, power utility networks, and high-performance edge data networks are critical to our lives and our national security and need to be protected.



Wireline Networks

Wireline networks are the most typical method of providing broadband services for both residential and enterprise customers. Both cable and telecom companies are rapidly expanding their fiber footprint. Even though cell phones are ubiquitous, the public switched telephone network is still alive and well. It is dependent on traditional voice services as well as leased line and legacy specialized services. It has always been necessary to provide a reliable synchronization source for network elements in wireline networks. Now it is common for those elements to be virtualized and run on Commercial off the Shelf (COTS) server hardware that also requires PTP. While those networks absolutely require a reliable timing source themselves, they often also provide network timing as a service to enterprise customers over fiber or copper.

These networks have traditionally leveraged centralized sources for synchronization and clocking at each facility, but, since the 1990's, those signals are typically derived from GPS. It has been standard practice to back up the GPS with rubidium or cesium clocks that provide a significant holdover of the clock reference in the event of device failure or GPS disruption. Timing disruption in the wireline network could cause widespread and expensive service outages and degradation.

Long-haul fiber network

5G

There are several reasons why 5G makes timing more important than ever in cellular networks. This newer generation of wireless employs technologies that are significantly different and more advanced than LTE, which brings new distributed and open architectures. This creates ambiguities that must be considered. The fact that the technology is designed for its enhancements in supporting high bit rate, ultra-low latency (ULLC) services implies a need for the highly precise alignment of network time across components. The technology itself brings new dependencies as well.

At its core, 5G uses Time Division Duplexing (TDD) as a means of utilizing the same frequency channel for upstream and downstream transmission. This is a departure from 4G, and it requires very precise network timing to ensure that the two paths are well coordinated and do not interfere with each other. A lack of a reliable PTP source will cause dropped calls and substandard call quality, which are key metrics for service providers to determine customer satisfaction and turnover.

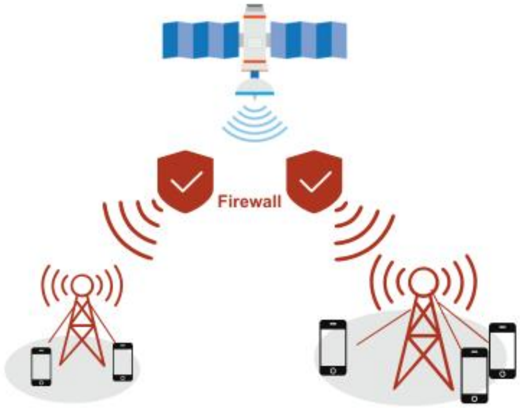
One of the significant advancements enabling the performance of 5G is beamforming. This is a technology that allows 5G radios to focus their power towards specific devices to gain increases in both signal strength and range for targeted devices. Super high bit rate mmWave services are significantly limited in range, so beamforming is a valuable tool for allowing these services to work at scale and range. It has an additional effect of reducing interference from multiple devices vying for the same network resources, as is usually the case in urban areas. Finally, beamforming saves power by explicitly focusing resources where they are needed - not where they won't be used.

Massive MIMO is another key feature of 5G, as it allows many more devices to use the same cell site radios and the same frequencies to communicate. The most valuable asset for wireless network operators is their spectrum, and higher utilization of this asset directly correlates to higher profits. Massive MIMO requires network time to match with extremely high precision at both ends of the signal.

While all of these 5G features require precise timing on their own, mobility includes some of the more complicated functions of the radio access network. When a user's device moves from one cell to another in a 5G network, the device requires seamless handover. Considering TDD, Beamforming, and Massive MIMO, the complexity of this handover process has increased significantly from previous generations of wireless standards. It requires timing to be precisely synchronized between the old and the new cell sites, as well as with components of the 5G core which could be at a significant distance from the radios.

Cell sites are typically equipped with GPS antennas and timing cards to account for local equipment requirements. But, if consideration for network time is made mainly through GPS sources at the cell sites, there is no provision for the disruption of the GPS signal at any one cell site affecting the broader network. Comfort can be taken in the idea that if functions like TDD, Beamforming, and Massive MIMO are disrupted by GPS jamming or spoofing at a single cell site, traffic will be handled by adjacent cell sites. The problem could be constrained and have limited impact. However, if that disruption affects mobile handoffs by taking that cell site out of sync with the timing reference used by the 5G core or adjacent cell sites, a much bigger outage will be experienced. There is an additional challenge in that utilizing GNSS antennas and timing systems at every single outdoor site requires dedicated maintenance. With so many sources, outages are simply more likely than with wireline networks. It is important to take rudimentary steps to provide a reliable timing backup for the whole network.

MIMO Deployment



GPS Satellite Firewall

Edge Networks

Another major trend in networking is the growth and promise of Edge Networks. The definition of an edge network is a bit loose. From an enterprise perspective, the "edge" is the at the WAN interface on the fringe of their property. So, a large enterprise might establish a middle ground between on-site IT operations and centralized IT operations at the "edge" of their physical facility boundaries. This infrastructure is often an extension of the public cloud network or the communications service provider network. It is a way to make possible very high-speed services that will benefit from ultra-low latency made possible by affinity to the end user. A communications service provider may have a different definition of "edge" and use the term to describe IT infrastructure at the edge of their wireline or wireless networks. This edge is typically designed for the same performance reasons but made to be utilized by multiple enterprises or by individual consumers.

In IT networks, quality timing is often an afterthought. However, because edge networks are defined by the performance they provide, a quality reference is necessary. High speed finance, block chain, security services, smart city functions, robotics control and other typical applications at the edge require PTP to offer consistent performance. For some of these, human safety depends on it. It is critical that edge networks can depend on a timing reference that is common to the networks they are connected to. So, a centralized timing reference makes the most sense.

Utilities

Our critical energy infrastructure is being upgraded to meet evolving standards for efficiency, output, stability, security, and environmental impact. As it stands today, power generation and distribution systems are a mix of old and new. This mix makes network timing and synchronization more critical components of utilities' infrastructure.

In power generation, PTP is used to synchronize the clocks of generators, turbines, and other equipment. It is essential to maintaining a stable and reliable power grid. For example, PTP is used to synchronize the clocks of two generators operating in parallel. This ensures that the generators are consistently producing the same frequency and voltage. A lack of synchronization creates inconsistencies that can cause power brownouts and blackouts. PTP is also used to support frequency regulation of generators. This matches output to consumption, which is necessary to ensure an optimally efficient utility.

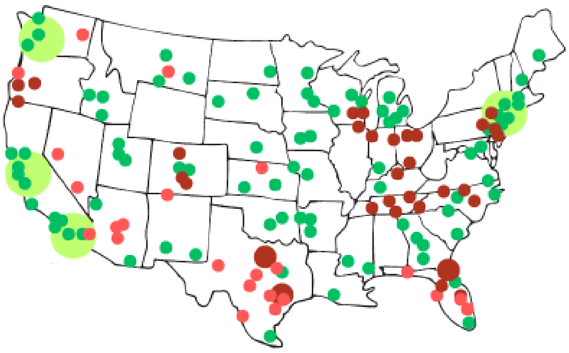
In power distribution, PTP is used to synchronize the clocks of substations, transformers, and other equipment. Consistency is necessary for not only efficiency, but also safety. For example, two substations connected by a transmission line could be receiving their timing source from separate GPS references. When things are working properly, they will be in phase with each other. But the loss of one reference at one substation with no backup source for PTP can cause widespread outages. This is a significant security concern, as any power outage results in disruption of critical services and infrastructure.

Finally, it is more common than ever for businesses and residents to not only consume energy but produce it. The cost of solar, wind and other private power generation

Utilities cont.

infrastructure has declined significantly in the past two decades. It is often the case that these systems produce more power than is consumed by the functions they support, especially during off peak times. Excess power is fed back into the utility power distribution network for use by other consumers. These private systems typically derive their timing from the larger distribution grid for this to work properly.

Like wireless networks, power infrastructure is distributed, is largely outdoors, and can operated by multiple entities. IEEE 1588 indicates that power networks should not rely on GPS alone for network timing reference. The proper means of providing reliable network timing is by providing it from a central source with adequate protection and holdover.



Real Time Alarm Simulation

Government Mandate

Executive Order 13905, issued in 2020, is an affirmation of the critical role positioning, navigation, and timing (PNT) services play in American national security. EO 13905 calls for government agencies and private sector entities to conduct comprehensive risk assessments inventorying their dependencies on PNT references like GPS and isolating vulnerabilities they create. Based on this objective assessment, they are required to develop and implement mitigation strategies to ensure resiliency from disruptions. In addition, EO 13905 requires the establishment of some infrastructure and governance both domestic and across global political boundaries.

This executive order has influenced private and public sectors in two ways.

Firstly, it has raised awareness among chief security officers in ownership and consumption roles, highlighting the potential liability arising from inadequately designed or protected network timing and synchronization systems. Secondly, it has integrated the subject into routine planning and operational discussions among network architects, prompting them to strategize for backup, availability, and security, moving beyond a mere basic reference. Although network timing was not previously a paramount concern in design and operation, it has now become a forefront consideration.

Federal
Communications
Commission

Developing Technologies

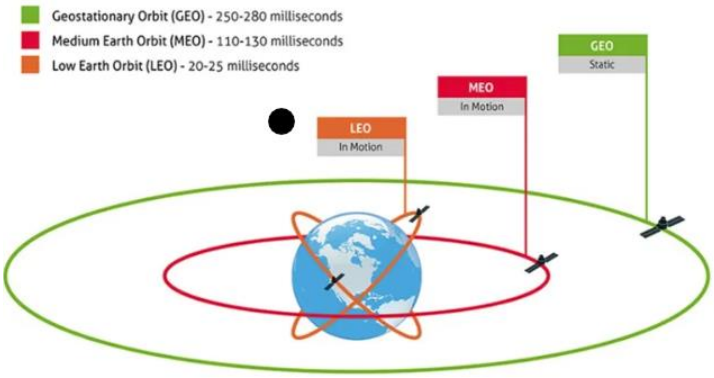
As an acknowledgement to the evolving threats and requirements for modern networks, steps are being taken globally to improve the options for sources of PNT. They can be used as alternatives or as redundant sources to GNSS reference.

GNSS signals are emitted from medium to high orbit satellites, which are rather far from the earth's surface and the devices utilizing their services. As a result, the signal is quite weak. It is also well documented. Methods of jamming or spoofing the signal are relatively easy to develop at low cost. It takes only a small, low-cost transmitter to jam the signal and the well documented interface makes it easy to spoof. While dependency on these systems is growing, alternative PNT sources are being discussed and developed globally.

eLORAN is one such initiative. For over twenty years, Enhanced Long Range Navigation has been in development and discussion as an alternative to GNSS satellite PNT services. It is a successor to LORAN-C which was long used for maritime navigation. eLORAN would be land based, have large very strong transmitters positioned strategically around the globe, and provide a fine alternative or backup to GNSS services. Because they are terrestrial, they are easy to maintain and inexpensive to operate.

Low Earth Orbit (LEO) satellite constellations are quickly developing as a secondary source to GNSS networks. LEO systems are less vulnerable sources for the PNT signals because the signal will be stronger than existing services and therefore more difficult to jam or spoof. Also, that strong signal penetrates buildings better than GPS so it can be used without an external antenna. Satelles has provided their STL service commercially since 2016, and the devices needed to receive it are now widely available.

Finally, private or public land-based timing distribution networks are under consideration by local and federal governments and private interests. Because governments recognize disruption of network timing as a common method of undermining the security and economy of countries, there are discussions in the US and in Europe about providing a terrestrial "timing as a service" offering that covers large geographical regions. Enterprises and utilities would be able to connect to their data centers via fiber to get access to this service, ensuring a quality backup to satellite based PNT services. In America, this has not gone to the point of funding or planning for rollout, but it could be something that network operators can depend on in the future. This is a development worth watching.


🟩 Geostationary Orbit (GEO) - 250-280 milliseconds
🟥 Medium Earth Orbit (MEO) - 110-130 milliseconds
🟧 Low Earth Orbit (LEO) - 20-25 milliseconds
GEO
Static
MEO
In Motion
LEO
In Motion

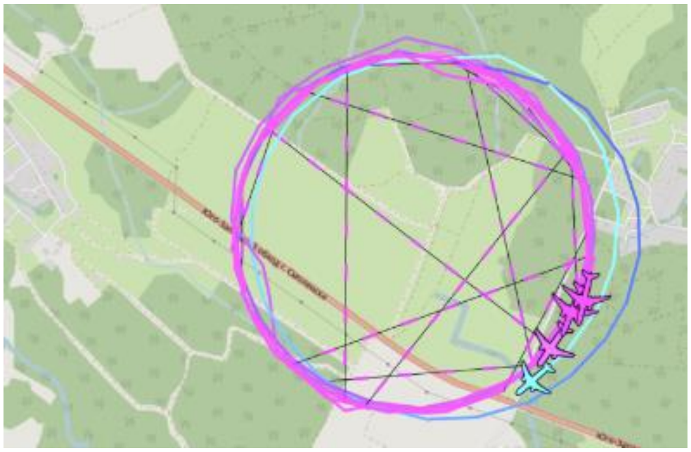
Satellite Orbits

Current Means of Mitigating GNSS Spoofing and Jamming

Simple methods are employed to protect networks against disruption of GNSS signals, at varying levels of efficacy. One example is the practice of aiming directional antennas at a specific part of the sky, ensuring the strongest possible signal. This reduces the chance that a signal could be interfered with from a terrestrial or otherwise non-GNSS source.

The best practice is to design the potential for disruptions out of a network. The most important means of mitigating Spoofing and Jamming is to implement a redundant Primary Reference and Timing Clock (vPRTC) in addition to rudimentary GNSS reception equipment in all mission critical networks. Today's systems provide both synchronization of legacy elements, and network timing for newer elements. And they do so with the support of rubidium or cesium clocks providing accurate hold over of the timing reference for days (or even weeks) in the event of any GNSS outage. These systems are configured as primary or secondary sources for the PNT data and sync signal, and they are built in a redundant manner. This ensures that both the reference and the systems providing the reference cannot fail. Compared to the network elements they support; these systems are extremely economical. If implemented correctly, they can provide a significant improvement to network performance, up time, and security.

Another common component used to ensure resiliency of PNT and synchronization services is the GNSS firewall. Even vPRTC systems currently utilize GNSS antennas to acquire a reference signal, and, because they are typically installed in data centers or central offices, they also can provide services to thousands of network components. A GNSS firewall is positioned between the GNSS antenna and receiver. It not only detects when the signal from the satellite is degraded because of jamming, it uses machine learning to detect minor differences in data received at the antenna to detect when a signal is spoofed. Alarms are triggered when either type of disruption is detected, and priority is given to the vPRTC elements providing signal hold over to ensure that service is not affected.



Denver Airport GPS Spoof - January 2022

Summary

This paper has explored some of the reasons for and threats against network timing and synchronization in the networks currently being operationalized globally. In addition, it highlighted current and developing technologies that could reduce the threat or impact of spoofing or jamming of GNSS signals widely used as a primary source for clocking. The intent was to encourage network operators to make intentional, educated decisions in the design and support of their timing network to reduce vulnerabilities. The threat is real and growing, so it is important to move network timing to the top of the list of priorities.

About the Author

For over twenty years, Syncworks has been evaluating, testing, designing, and implementing timing networks for telecom, cable, utility, and enterprise customers in the US and the Caribbean. We are a well-known and trusted partner and critical supplier to major network operators. As a diamond partner to Microchip and a skilled integrator of other vendor products, we can provide options for the most performant, resilient, and economical timing network possible. We specialize in ensuring that critical networks can survive disruptions like GPS jamming and spoofing. And we provide expert support, sparing, and repairs for everything we install leveraging the largest inventory of related products and components in the industry.

Syncworks.com

Ponte Vedra Beach, Florida, USA

Sales@Syncworks.com

+1 (904) 280-1234 main