Summary: This CAST technical bulletin gives a description of the updated effort on Oak Ridge National Lab (ORNL) Center for Alternative Synchronization and Timing (CAST) project's work investigating a terrestrial-based high precision timing infrastructure intended for time synchronization of the next generation power delivery infrastructures. We will provide a high-level description of the CAST application context, key protocols, critical architectural issues, and how GPS/timing data traverse through the system.

CONTEXT

Modern power delivery infrastructures involve wide arrays of Operation Technology (OT) systems, controllers, relays, and sensors, all requiring extremely precise timing synchronization for correct operations. Furthermore, migration toward the next generation green Distributed Energy Resource (DER) is further transforming the legacy hierarchical power grids toward a collection of more complex and distributed point-to-point networks. Under such circumstances, highly precise timing distribution and synchronization across all points in the modern power delivery infrastructure has become a highly critical operation requirement with significant security implications.

Today's default synchronization/correlation methods are primarily based on wireless technologies such as GPS GNSS, E-Loran signal reception or remote subscriptions to public timing authorities (e.g. NIST - National Institute of Standards and Technology) as in NTP. Such approaches are facing difficult challenges. Satellite communication comes with the inherent risks of jamming and spoofing. Large number of remote timing subscriptions pokes holes on enterprise firewalls thus creating open-loop security vulnerabilities. Legacy timing protocols are also failing to deliver the high precision timing demanded by modern power delivery OT systems.

In this context, CAST is performing research, testing, and evaluation to provide the best practice of a terrestrial-based high precision timing distribution/synchronization infrastructure, as a GPS alternative/backup, as a solution to close the loop on our nations power grid.

KEY PROTOCOLS

High precision timing delivery over network primarily involves two communication protocol options: Network Time Protocol (NTP) - RFC 5909, and Precision Time Protocol (PTP) - IEEE 1588. NTP has a precision at the microsecond level. PTP has a much higher precision at the sub-microsecond (nanosecond) level. Both PTP and NTP uses a distributed architecture that supports point-to-point communication paradigm via a Master/Slave architecture such as communication between Grand Master Clock (GMC) and multiple slave/boundary clocks. On the security front, NTP mainly uses secure hashing function for content integrity protection while PTP uses even stronger cryptographical implementations. NTP runs on top of UDP (layer 4) through port 123, and PTP can run directly over Ethernet at Open Systems Interconnection (OSI) layer-2, or on top of IP (OSI layer -3)/UDP (OSI layer-4). The CAST architecture supporting both PTP

and NTP provides a means to close loop the OT network from generation thru distribution on net and off net public and private communications providers.

PTP also has industry specific profiles. For example, ITU-T defines the G.8265.1, G.8275.1, and G.8275.2 profiles in telecommunication networks. IEEE C37.238 defines a PTP power profile intended for power system applications, notably power grid measurement and control. PTP packets could be software timestamped at the system kernel or Network Interface Card (NIC) driver levels. Alternatively, for higher precision implementations, PTP packets are often timestamped at the OSI MAC or physical layers by Network Interface Card (NIC) hardware.

In addition to NTP and PTP, there are also Internet Engineering Task Force (IETF) driven Network Time Security for NTP (NTS4NTP, RFC 8915) [1] and Network Time Security for PTP (NTS4PTP, an RFC in progress) standards [2]. Both NTS4NTP and NTS4PTP contain a preceding Key Establishment (KE) session that utilizes cryptographically strong PKI (Public Key Infrastructure) to establish a symmetric key for high level of NTP/PTP security such as cryptographic key based authentication and secure authorization to unicast/multicast timing services.

SECURITY and PRECISION ISSUES

OPEN LOOP vs CLOSE LOOP SUBSCRIPTION ARCHITECTURES

When designing timing service subscription architecture, security is of critical importance, as it eventually impacts the fundamental underpinnings of the overall power delivery infrastructure's reliability, availability, authenticity, and confidentiality. Today's common implementation is largely a collection of NTP-based subscriptions connecting to external and remote timing servers, such as services hosted by NIST. NTP utilizes UDP port 123 for its request-response communication. This leads to an open-loop style of subscription architecture. When scaled up, the implication is a large number of internal clients would be frequently contacting and connecting to numerous external public NTP timing servers (e.g. NIST, Google, Apple, Facebook, universities), with all the traffic jamming through firewall UDP port 123. This implies the firewalls must also be configured to accommodate large number of complex and inefficient forwarding rules. Such open-loop and NTP-based subscription architecture inevitably leads to unacceptable timing packets delivery delays and presents significant security vulnerability to attacks such as denial-of-service (DOS) against the UDP port 123.

In contrast, CAST takes a more secure and efficient close-loop approach on subscription architecture, utilizing a combination of highly efficient terrestrial PTP backbone(s) for remote GMC connection and a mix of PTP/NTP connections for high volume internal timing subscriptions. To do so, CAST can establish Boundary Clocks (BC) Remote Synchronization Unit (RSU) at the enterprise boundary. Through highly efficient terrestrial PTP tunnels, BC are synchronized to remote timing authority (e.g. GMCs at NIST, Google). No hole on UDP port 123 was necessary and only very limited BC PTP tunnels are required. Such close-loop approach enhances manageability and reduces security vulnerability. From withing the enterprise, the BC functions inwardly as a highly reliable GMC, supporting both NTP or PTP, in both unicast and multicast modes, synchronizing a large number of internal timing service subscribers. This closed-loop implementation being investigated by CAST logically achieves higher level of scalability and security, more appropriately addressing the alternative terrestrial timing synchronization requirements in support of the modern power delivery infrastructures.

COVERT CHANNELS

A covert channel is a method of communication that hides unintended/unauthorized information by means of disguise. For example, a covert channel could look like a normal NTP communication session on the surface while carrying malware communication underneath. Covert channels are often leveraged for malicious purpose, such as data theft or disruption of communication. It has been shown NTP is subject to convert channel attacks. By utilizing the NTP extension fields allowed in between the NTP header and Message Authentication Code (MAC), a convert channel can be constructed between NTP client and external servers without breaking protocol format [3]. No error will be generated and hence could go unnoticed. Even though a Snort rule monitoring port 123 might catch basic covert channels in NTP, it has been shown by hiding encrypted high entropy data in a high entropy field of NTP, the covert channel is practically undetectable [4].

On the other hand, PTP is a one-way communication, which means GMCs typically get their reference time only from GNSS/GPS/Cesium /Atom clocks for the best time accuracy (rather than from peers), it reduces the attack surface. Also due to the high prevision synchronization process in PTP, it requires an adversary's careful implementation and prior reconnaissance to fit the covert channel [4]. To remain undetected, the adversary must monitor PTP traffic and assess which PTP fields could serve as storage channels, while determining the extent to which timestamp modification can occur without disrupting the time synchronization process. That is, constructing a covert channel in PTP becomes much more challenging than in NTP. CAST's close-loop PTP/NTP driven subscription architecture minimizes NTP channels usage excepts for enterprise internal subscriptions, thus reducing the public NTP channel associated possible coercion using covert channels.

HIGH PRECISION TIMING

A terrestrial timing infrastructure largely based on NTP comes with precision challenge. NTP was introduced almost 40 years ago (1985), primarily intended to address computer network general timekeeping requirements (computers/servers/network devices). Designed to address Information Technology (IT) synchronization needs, it achieves a sub-millisecond precision at the local network level, but it could drop to a few milliseconds when deployed across the internet. NTP is based on a hierarchical, client-server, request-response subscription architecture, which is prone to network variability such as congestion and jitters [5]. However, modern OT, such as distributed power grid synchronization, requires higher level of precision in the nanoseconds. For this purpose, PTP, on the other hand, is a newer (2002) and with higher precision level (nanosecond) timing specifically designed for high-precision applications such as energy section substation synchronization. The protocol is based on a peer-to-peer topology and uses multi-step, two-way messaging exchange which also takes into consideration of network propagation delay and compensation. PTP implementations primarily run on OSI layer-2 (Ethernet) where UDP timing packets are timestamps by NIC hardware right before departure to minimize any system-induced delays, thus achieving higher level of nanosecond precision more suitable of power delivery infrastructure critical components synchronization. In this "close-loop" subscription architecture approach, CAST utilizes both PTP's OSI layer-2 hardware timestamp characteristics to address high precision timing requirement demanded by modern power delivery infrastructure, as well as the established NTP channels to achieve high flexibility and enterprise internal synchronization. This combined PTP/NTP architectural approach further enhances the performance of existing NTP synchronization delivery with additional high availability terrestrial-based GMCs for legacy power distribution infrastructures or off-net technologies such as inverters where only NTP is available but not PTP.

CAST TIMING FLOWS

ORNL CAST team is presently utilizing PTP 2.0 (IEEE 1588-2008) from a Grand Master Clock (GMC) disciplined by a 10 MHz Cesium source and calibrated to UTC. CAST team is also actively pursuing the even more secure NTS4PTP implementations, that utilize PTP 2.1 (IEEE 1588-2019) integrated security mechanism (prong A), with vendors and international researchers.

In this section, we provide an example architecture design that describes CAST GNSS/GPS and PTP/NTP timing data flow. Figure-1 conceptually illustrates such a high-level CAST implementation option showing the data traversal.

GMC and Trusted Timing Source

CAST presently maintains multiple GMCs at the ORNL lab, receiving GNSS/GPS signals as the timing reference input. The trusted timing source, such as NIST time, GNSS/GPS, serves as the authoritative timing reference for the initial calibration of GMCs. A timing device that is configured as a GMC can receive the authoritative time reference on one of its interfaces while, on the other inward interfaces, deliver timing and synchronization to the time services subscribers. A cesium atomic clock is also connected to the GMCs, delivering the accurate phase and frequency and serving as oscillator reference for GMCs. So when the trusted timing reference is disconnected, or becomes unavailable for whatever reason during the actual deployment operation, GMCs will continue to keep time with extremely high accuracy with the reference provided by the high-frequency cesium clock. This realizes a true terrestrial based timing/synchronization alternative solution. The length of the GMC's ability to maintain accurate timing in absence of external reference is defined as holdover.

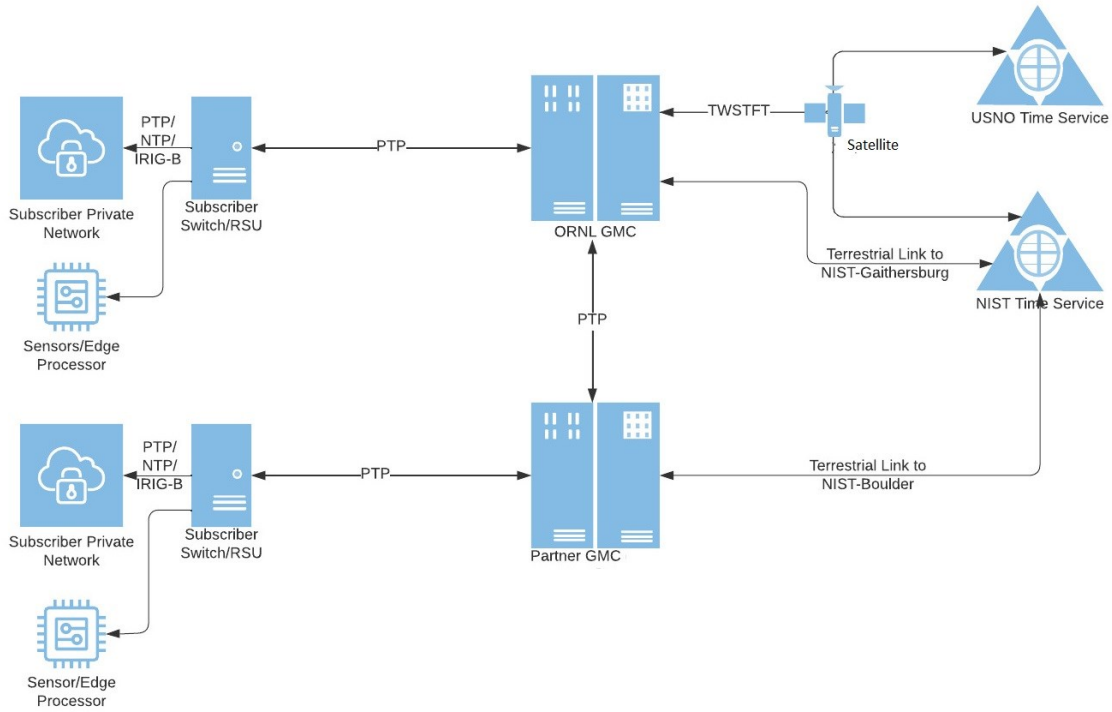

Figure-1 Example CAST High Level Conceptual Architecture

Many of CAST timing devices are multi-functional. One single device can be configured as a PTP GMC, PTP boundary clock, or as a PTP slave clock. For example, when configured as a GMC, the devices could use its embedded GNSS/GPS receiver, connected to an external GPS antenna, to receive timing data. This timing data is then used by the device's Network Interface Card (NIC) to hardware timestamp Ethernet PTP frame right before they are sent out. This minimizes delay due to system internal processing.

CAST further investigates GMC's holdover performance by running the GMC in Enhanced Primary Reference Time Clock (E-PRTC) mode. In this mode, CAST GMC uses both the primary reference that receives a one pulse per second (1pps) GPS signal, and the secondary reference that receives 10 MHZ signal from the cesium clock, as active references. Over the period of 72 hours, E-PRTC GMC learns how the two references should behave relatively. After the learning period, if one of the references becomes inaccessible, E-PRTC GMC will continue to function as if both references are present, thus ensuring high availability of extremely accurate timing reference.

Meanwhile, using the satellite antenna and modem, CAST runs Two-Way Satellite Time Frequency Transfer (TWSTFT) via satellite between a GMC in a lab located at ORNL main campus and NIST at Boulder, Colorado for synchronization. It's worthwhile to note that NIST Time Service is also synchronized via TWSTFT with the US Naval Observatory (USNO) Time Service via satellite, and both are mutually authoritative sources.

Partner GMCs and PTP Terrestrial Synchronization

As illustrated in Figure-1, CAST plans to have the ORNL GMCs further synchronized with GMCs of other national laboratories in a wide are synchronization geo redundancy configuration. The purpose of maintaining highly synchronized partner GMCs is for geographical service coverage and failover backup. Terrestrial PTP traffic is used for synchronization between partner GMCs.

PTP Timing Service Delivery

GMCs deliver timing service to subscribing customer enterprises via secure PTP traffic. At the entry point of the CAST PTP traffic, a subscriber's boundary Remote Synchronization Unit (RSU) device can be configured in multiple ways based on subscriber's requirements:

- As an Ordinary Clock (OC) that runs PTP on only one of its interfaces receiving CAST timing service. This is typically an end device such as an edge processor or a sensor that needs its time synchronization.
- As a Boundary Clock (BC) on one end acting as a slave clock receiving CAST PTP traffic to synchronize. And on the other, often through multitude of interfaces, acting as a master clock provisioning inward synchronization service to internal OC/TC/BC in either PTP or NTP traffic. A BC residing in between a GMC and a multitude of slave clocks offers scalability benefits by reducing the direct communication load on the GMC. A BC also acts as a repeater refreshing the PTP signal when long network paths are in play. Furthermore, a BC sitting at the boundary of a subscriber's internal network also provides security advantage, as it enables internal network synchronization and reduces the number of connections to external timing sources as well as their associated vulnerabilities.
- As a Transparent Clock (TC) that passes through CAST PTP traffic inward to the specific destinations within the subscriber's private enterprise. These destinations could be additional network segments containing multiple OC to be synchronized for a broader coverage. TC RSUs can compensate for own queuing delays but cannot function as time references. Essentially, TC functions as a PTP traffic switch.

CONCLUSION

CAST has conducted research and testing to showcase the viability of an alternative terrestrial-based high precision timing delivery and synchronization infrastructure for the modern power grid. This technical bulletin describes CAST timing service's subscription architecture that utilizes high precision PTP for remote GMC access. Combined with using PTP and NTP for local timing subscriptions, CAST's close-loop architecture improves overall system cybersecurity by reducing the vulnerability of large numbers of inefficient external NTP subscriptions tunnels constantly running through the enterprise firewall. CAST PTP utilization further markedly improves timing accuracy from microseconds to nanoseconds.

This technical bulletin further illustrates CAST timing data flows, as an example realization of time synchronization. Leveraging PTP-based synchronization between external GMC and enterprise BC, CAST ensures not only high timing accuracy but also robust security measures, tailored to meet the demands of next generation power delivery.

References

[1] IETF, Network Time Security for the Network Time Protocol, Sept. 2020
[2] IETF, NTS4PTP - Key Management System for the Precision Time Protocol Based on the Network Time Security Protocol, Feb. 2024
[3] Tsapakis N, Alternative Communication Channel Over NTP, Virus Bulletin, 2019.
[4] Lamshöft K, Hielscher J, Krätzer C, Dittmann J, The Threat of Covert Channels in Network Time Synchronization Protocols, in Journal of Cyber Security and Mobility, Mar. 2022
[5] Shrivastav V., Lee K.S., Wang H., and Weatherspoon H., Globally Synchronized Time via Datacenter Networks, in IEEE/ACM Transactions on Networking, Aug. 2019

For additional details, please contact CAST@ornl.gov.

The Center for Alternative Synchronization and Timing (CAST) at Oak Ridge National Laboratory (ORNL) performs research, development, testing, evaluation, and technical assistance to enable resilient timing and synchronization for the power grid. Working closely with power utilities, timing hardware and software vendors, network operators, and federal stakeholders, CAST helps develop and validate alternative timing architectures to augment GPS time. CAST also translates and transfers ORNL's research and development (R&D) advances in secure timing and grid communications to power sector applications, and engages across the broader timing community to develop best practices to ensure the resilience of US critical infrastructure. CAST is sponsored by DOE's Office of Electricity. Visit https://cast.ornl.gov for more information.