Eliminating GPS Dependency for Real-Time Wide-Area Syncrophasor Applications

White paper by Net Insight

Net Insight AB, Sweden
September 2012

WHITE PAPER

net insight™

ABSTRACT

Today's society is becoming increasingly dependent on GPS timing for many critical everyday services, such as digital TV and radio distribution systems, power grids, digital studios and mobile networks. The problem is that it is very easy to jam or spoof the reception of the Coordinated Universal Time (UTC) signal via the GPS and reception quality can be significantly affected by weather conditions. In many environments, the cost of the GPS receivers and antennas also represent a major cost.

This paper describes a new solution for delivery of UTC, independent of GPS. The solution enables distribution of real-time information over the same infrastructure that is used for transport of multi-service payloads. This solution is secure, cost-effective and can be built resiliently. Moreover it provides the accuracy needed (~1 µs) for real-time wide-area network applications, such as synchrophasor monitoring and control, which would not have been possible in large-scale deployments with traditional synchronization methods. The paper describes the new two-way time and frequency transfer method, showing how a stable, robust absolute time representation across the network is achieved, including automatic corrections for intrinsic delays and diurnal wander.

Introduction
There are many network applications that require accurate timing to work properly. Today this is achieved by installing GPS receivers at all, or key, locations across the network. However, GPS receivers may easily be jammed, as reported e.g. by Volpe[1], and represent an additional cost to the network. The GPS is also military controlled. Previously, there was no alternative solution that could deliver UTC time in a wide-area network with the accuracy needed for real-time applications. It has also not been economically feasible to build proprietary dedicated synchronization networks.

Alternative solutions
The European Union has for a long time considered launching its own "GPS" satellite system through a project called Galileo. Launching and maintaining several tens of satellites is a major, very expensive undertaking, a reason why the project has been continuously delayed. However, such a solution would still be sensitive to jamming and spoofing like the GPS system. The signal transmitted from a satellite can be compared to light from a light bulb seen from the other side of the Atlantic, i.e. it is a very weak signal.

IP networks utilize a protocol called NTP (Network Time Protocol) to synchronize different clocks, using time stamps sent in data messages. In non-dedicated networks it is difficult to reach accuracies below a few milliseconds using NTP, which is not accurate enough for many real-time applications.

A new standard for transferring time information over IP networks has emerged, called IEEE1588, promising time accuracy down to below 1µs in controlled network environments. The issue with IEEE1588 is that it typically requires dedicated hardware in network switches to ensure such accuracy. This means that for mission-critical applications, there needs to be separate networks for transferring the time to eliminate data-load interference with the time transfer. In most deployments, where a dedicated network for timing is cost prohibitive, the varying load on the network changes the network delay, resulting in frequent corrections to the wide-area network time. Scalability then becomes an issue, as it becomes more difficult to maintain accuracy across larger wide-area networks.

Therefore, there is a need to find a more scalable solution for delivering both time and data in an integrated solution over large wide-area networks for real-time applications like synchrophasor monitoring and control. This paper describes such a solution that solves this problem handling both payload and absolute time synchronization in a single integrated network. This solution has the additional benefit of offering a secure delivery that does not show the same vulnerability to malicious external behaviour and cyber threats as traditional data networks and current IEEE1588 implementations.

INTEGRATED TIME TRANSFER
The new solution, based on a protocol called Time Transfer, allows highly accurate distribution of absolute time over the same network that carries other services, like video and data. This protocol has been used commercially in a very large "GPS-free" DTT (Digital Terrestrial Television) network of over 600 nodes, which requires an absolute time across the network for frequency and phase synchronization of TV signals, and is used herein as our example of a large scale nation-wide network handling absolute time in combination with real-time data and video delivery over the same infrastructure and equipment.

1 Volpe, J.A., 2001. Vulnerability assessment of the transport infrastructure relying on the Global Positioning System. US Department of Transportation.

At the headend site the transport equipment receives the same reference signals (1PPS and 10MHz) as the SFN adapter (see figure 2). These synchronization signals could be provided by any high-precision clock source e.g. an atomic clock or a GPS receiver backed up by an atomic clock. The time and frequency synchronization is distributed through the transport network and at the transmitter site the transport equipment delivers the same synchronization interfaces to the Sync subsystem that was previously delivered by a GPS receiver.

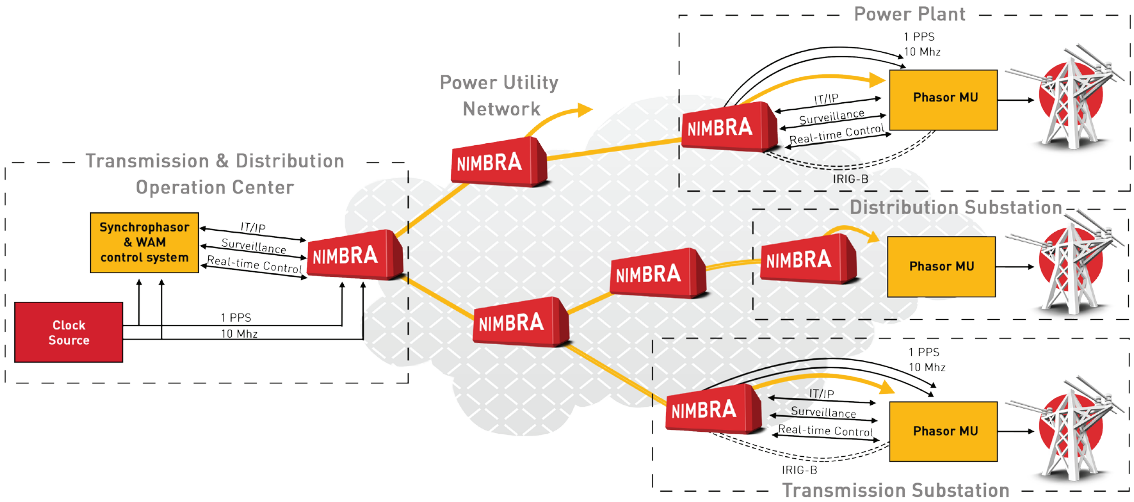

Figure 1 - Distribution network for SFN transmission using integrated time transfer

Initially, such a solution could be used as a complement to GPS in order to enhance the robustness and resilience of the UTC distribution. However, with a redundant network architecture and redundant synchronization interfaces it is possible to fully rely on the integrated Time Transfer functionality.

DTM Technology

The Time Transfer protocol is enabled by a signaling and resource reservation protocol called Dynamic Synchronous Transfer Mode (DTM) which has been standardized by ETSI[2]. DTM is designed to provide a guaranteed QoS for multiple services with zero packet loss, constant delay, and very tight bounds on jitter and wander. The transport mechanism of DTM is based on time division multiplexing and in this sense is similar to SDH/SONET, but has much more flexible bandwidth and service provisioning, and has better meshed-based protection switching architecture ideal for real-time, mission-critical applications in large wide-area networks. DTM offers improved quality transport and synchronisation over both IP/Ethernet and SDH/SONET networks, as well as directly over dark fibre or wavelengths.

The signaling plane of DTM used for end-to-end provisioning, resource reservation and protection could be compared to that of packet-based technologies such as ATM and MPLS. The corresponding features in DTM however were designed to simplify end-to-end service provisioning and operation, dramatically reducing network operating costs.

In DTM transport, the resource granularity is 512 kbps. This means a service can be allocated resources in steps of 512 kbps. Due to the strict resource allocation in combination with the synchronous time properties, a service is guaranteed its allocated capacity and cannot be interfered by other services. This means that a real-time critical

2 Dynamic synchronous Transfer Mode (DTM). ETSI ES 201 803 (2001-05).

service e.g., carrying measurement data or a control channel carrying Time Transfer information cannot be maliciously attacked or interfered. Critical payload traffic such as real-time synchrophasor data and system control signals may hence be carried on channels with a granularity of 512 kbps, providing guaranteed end-to-end "channelized" bandwidth, zero packet loss, constant deterministic delay, and tight bounds on jitter and wander. The resultant deterministic network allows automatic control loops and applications to be implemented over a wide area, which would not be possible on a network with variable packet loss and delay.

DTM also provides scalable layer-2 multicast functionality, allowing the ability to multicast real-time synchrophasor and system data and other services, like video, in a distributed system (i.e. local control systems with centralized SCADA) with the same accuracy and resiliency that DTM provides with point-to-point communications.

Synchronization Protocol

All nodes of a DTM network are inherently synchronized, preserving both frequency and relative phase in the network. Net Insight's network switches use a Synchronization Protocol (DSYP) which automatically determines the network synchronization topology to ensure optimum distribution of the synchronization reference clock and Time Transfer from a master node to all other nodes in the network (figure 4).
In case of failure of a synchronization path, DSYP will recalculate the synchronization tree enabling automatic synchronization restoration and avoiding synchronization loops in the network.

Two-way Time and Frequency Transfer

With the introduction of the Time Transfer protocol, every node is synchronized to maintain also the same absolute phase. This is obtained using a method called "two-way time and frequency transfer". The two-way time and frequency transfer works such that the source node transfers its time to the neighbouring nodes in the network, these nodes return their time and compensate so that the neighbouring nodes work with the same time as the source node. This repeats itself until all nodes in the network operate on the same time.

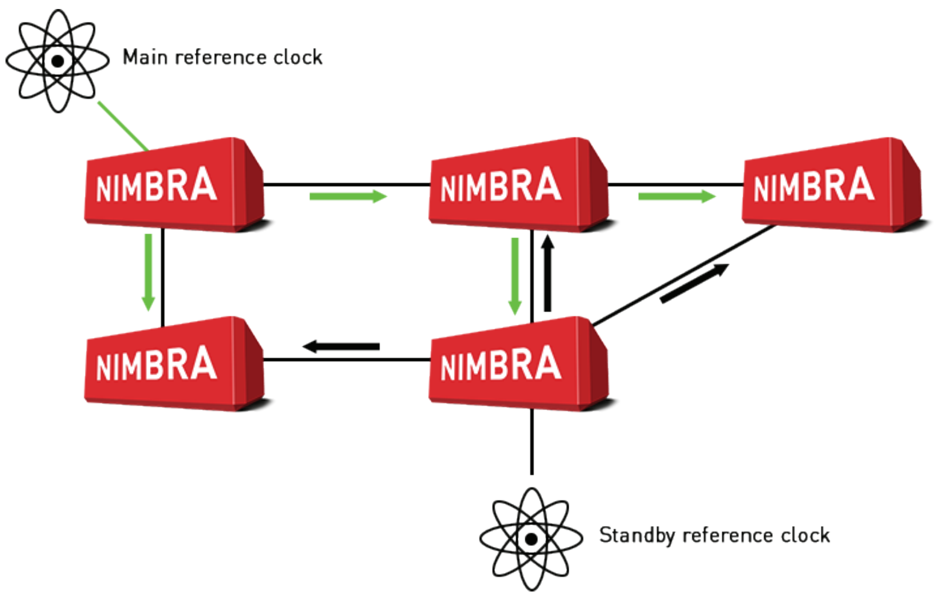

Figure 2 – A signalling protocol enables automatic network synchronization

In basic operation, the clock tracks a 8 kHz synchronization timing received on one of the incoming line interfaces, as selected through DSYP signalling. For Time Transfer, the clock establishes a local time scale using International Atomic Time (TAI) and maintains that time scale based on two-way time and frequency measurements in the network. Measurements include the time of the local and remote node in order to resolve the ambiguity between nodes.

This turns the functionality of the clock into a Time Locked Loop (TLL). Time Transfer is able to measure round-trip delays, compensate for intrinsic, static and dynamic delays and to synchronize TAI and UTC time between nodes. It is able to distinguish uncalibrated links and nodes from calibrated and to achieve traceable time. In order to execute the round-trip measurements and calculate the time scale errors, the measured time error of one node needs to be relayed back to the remote node. In order to provide for this information flow a control channel is set up in each direction for all interfaces involved in time transfer. This is the Time Transfer Channel. Within this channel the Time Transfer Channel Protocol transports time stamps, time difference measurements, correction factors and various statistics between nodes involved in time transfer.

The main principle of the two-way time transfer is illustrated in figure 5. Time is to be distributed from node A, which has received traceable time from an external clock source, to all other nodes in the network. Through the DSYP protocol node B has received the information that it is going to receive its timing reference from node A. In this example, when the local time in node A (TA1) is 10:00 it inserts this time stamp in the time transfer channel and sends it to node B. The transfer of the time stamp is subject to a delay (dAB) and reaches node B when the local clock in node B is 10:20 (TB, Rec). The local clock in node A is then TA2. In the same way Node B will send a time stamp to node A. In this example node B sends a time stamp when its local clock (TB1) is 10:10. The transfer to node A is subject to a delay (dBA) and reaches node A when the local clock in node A is 10:06 (TA, Rec). The local clock in node B is then TB2.

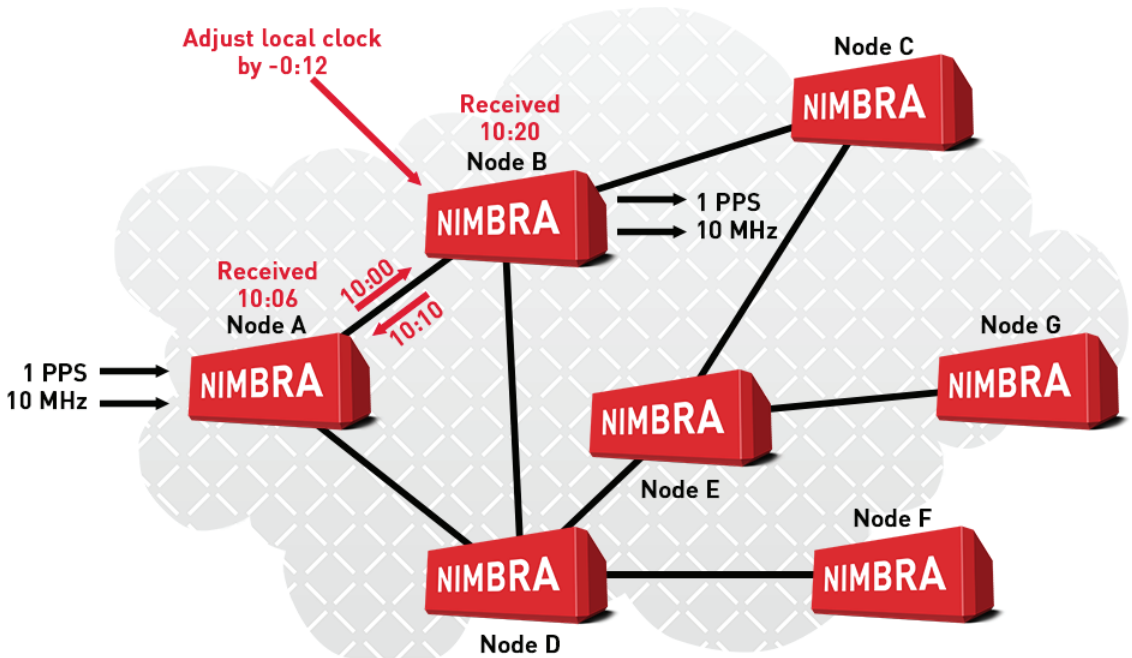

Figure 4 – Example of two-way time transfer

The following relations exist:

$$TA2 = TA1 + dAB \quad (1)$$
$$TB2 = TB1 + dBA \quad (2)$$

The time error TE between the clocks in node B and node A can be expressed as:

$$TE = ((TB, Rec - TA2) + (TB2 - TA, Rec)) / 2 \quad (3)$$

Inserting (1) and (2) the time error becomes:

$$TE = ((TB, Rec - TA1) + (TB1 - TA, Rec) + dBA - dAB) / 2 \quad (4)$$

With the actual values in the example, and assuming a symmetric delay dAB = dBA, the time error becomes TE = (0:20+0:04)/2 = 0:12, i.e. the clock in node B should be adjusted by –0:12 to be locked to node A. It can also be seen that the delay dAB = dBA = 0:08 in this hypothetical case.

Time Transfer works on bi-directional point-to-point links between a pair of interfaces. In its basic operation the time transfer function assumes that the delay over the link is essentially symmetric, i.e. the transmission delay from A to B is equal to the transmission delay from B to A with an accuracy of +/- 100ns. The delay over the links is allowed to vary slowly (e.g. due to changing temperatures), as long as the delay is symmetric all the time.

However, the time transfer protocol is also able to handle asymmetric delays and to divide the link into multiple segments from delay point of view:

$$dAB = dA, tx + dAB, link + dB, rx \quad (5)$$

where the total delay dAB from A to B is the sum of the output delay of the transmitter in node A (dA, tx), the delay of the transmission link (dAB, link), and the input delay of the receiver in node B (dB, rx). The transmitter and receiver delays are typically known in advance and may be entered manually. If the link delays dAB, link and dBA, link are known to be asymmetric, this may also be entered manually following a calibration at the time of installation.

Figure 5 – Switch with Time Transfer

Time Transfer provides a transfer accuracy of better than +/- 1.5µs over 10 hops in the transport network. To maintain this high accuracy, SDH/SONET systems that do pointer adjustments cannot be used as underlying links. It is also not possible to run Time Transfer on links that use an intermediate system with automatic protection switching, since this can introduce a sudden change in the transmission delay.

Resilience

In case of link failure, the DSYP protocol will automatically reroute the Time Transfer signals using an alternative path through the network. In the example in figure 5 node B normally receives its time reference from node A. If the link between nodes A and B fails, DSYP will change the time distribution path to A-D-B, i.e. node B will now receive its time reference from node D. However, the Time Transfer protocol is continuously executed on all links so the reroute is only performed locally in that the node chooses to work on the alternative path's incoming clock. Since the system keeps a local clock and ensures that the 1 PPS is within the 1 us accuracy, the system will not experience any distortions or jumps in the phase when changing incoming routes. Any variance in the phase between the two paths will be smoothed out through the local TLL system.

Several sources such as atomic clocks, located far apart from each other, may be used to create a system with full redundancy also for the master clocks. The interfaces used at the ingress and egress nodes (1 PPS and 10 MHz) may also be duplicated for redundancy purposes.

Network Protection Switching

DTM provides a variety of different protection schemes that can be chosen per service. Each node inherently supports mesh protection switching with automated re-routing, supporting any type of network topology. It is also possible to source route up to 3 different paths with the last path reverting back to automated re-routing to find any available path in the network. For critical services which may exist in a synchrophasor networks, DTM provides hitless 1+1 protection switching, with dual channels active over diverse paths through the network. With hitless protection switching, frequency, phase, and packet sequence remain intact, providing resiliency not found in any other type of wide-area network protection architecture.

Inherent Resistance to Cyber Attacks

Due to the channel and service separation throughout the network, it is not possible to maliciously affect traffic on these separate channels. Communications across the network are secured since it is not possible to insert traffic to interfere with the Time Transfer or mission-critical synchrophasor or control system payload. Time Transfer information is also sent in the control plane which is fully separated from the data plane making it secure from denial attacks.

Furthermore, it is not possible to access network nodes remotely since any control and management information is sent in private, separated channels unlike in public Internet routers. In addition, the framing structure also offers an inherent scrambling feature making it very hard to snoop traffic on a link. In brief, the key features of DTM offer a high-level of security, making the network extremely resistant to cyber attacks.

Implementation

DTM resource reservation with Time Transfer and DSYP has been implemented on multi-service switches with slots available for plug in modules supporting a variety of interfaces. Data, video, and voice traffic can be transported over the same network used for synchrophasor and system data acquisition and control signals, which significantly reduces total infrastructure cost. Time Transfer is supported regardless of the traffic signals carried.

For instance, real-time high-definition video surveillance feeds (with remote camera control) can be transported, with frame-by-frame absolute time. If required, the video surveillance feeds could be multicast in real-time to several key locations across the network. Voice traffic for field communications can also be transported in the event that radio signals are weak or compromised. Figure 6 shows a multi-service access switch where dual pairs of Time Transfer interfaces (1PPS and 10MHz) have been integrated in the chassis. The Time Transfer ports are configurable to support either input or output signals. The chassis also comes with integrated Gigabit Ethernet and multi-rate SDH/SONET network ports. Two slots are available for plug-in modules for other services or trunk network interfaces.

CONCLUSIONS

This paper has described a novel, integrated solution for high-accuracy distribution and synchronization of absolute time over a wide-area network. The solution has the following main advantages:

- **GPS Independence.** Time Transfer may replace or complement the GPS in SFN networks. GPS has high accuracy but has the disadvantages of being military controlled and that it is possible to externally jam the signals. Until DTM with Time Transfer, there was no alternative solution that could deliver UTC time in a large wide-area network with the accuracy needed for realtime applications.

- **Scalability.** The described solution within has been designed for scalability and resiliency for mission-critical wide-area network applications. This scalability has been validated through several large commercially deployed networks in operation today. Time Transfer has been commercially deployed since 2007 in a large country-wide GPS-free DTT network of over 600 nodes.

- **Wide-area Real-time Control.** Guaranteed end-to-end channelized bandwidth, zero packet loss, constant deterministic delay, and tight bounds on jitter and wander allows automatic control loops and applications to be implemented over a wide area. Integration of Time Synch and Payload. Timing information can be sent over the same infrastructure that provides data for realtime and non-realtime applications. Time Transfer introduces a more secure and less costly way of achieving the necessary SFN synchronization.

- **Fault Tolerance.** The synchronization protocol (DSYP) automatically determines the network synchronization topology to ensure optimum distribution of the synchronization reference clock from a master node to all other nodes. In case of failure of a synchronization path, DSYP will recalculate the synchronization tree enabling automatic synchronization restoration and avoiding synch loops in the network. DSYP also supports standby reference clocks at geographically separated locations.

- **Hitless 1+1 Protection Switching**. DTM provides both rerouting and hitless 1+1 protection switching, insuring the realtime availability required for wide-area synchrophasor networks. With hitless protection switching, frequency, phase, and packet sequence remain intact.

- **Inherent Security against Cyber Attacks.** The solution offers secure communication throughout the network where traffic within separate channels can never interfere with each other due to the deterministic switching and resource allocation. In addition, all control and time transfer payload is sent in protected private channels making remote attacks towards nodes not possible.

REFERENCES

1. Volpe, J.A., 2001. Vulnerability assessment of the transport infrastructure relying on the Global Positioning System. US Department of Transportation.

2. Dynamic synchronous Transfer Mode (DTM). ETSI ES 201 803 (2001-05).

Net Insight AB

Phone +46 (0)8 685 04 00 • info@netinsight.net • **www.netinsight.net**