C&I Network

1

Indigenous Secure NTP Server for Time Synchronization

Abhishek Borana*, Ashutos Mohanty, Suraj Mukade, D. A. Roy and U. W. Vaidya

Reactor Control Division, Electronics and Instrumentation Group, Bhabha Atomic Research Centre, Mumbai 400085, INDIA

Front View of NTP Server

ABSTRACT

In a distributed network environment, time synchronization across different components is critical for proper chronological sequencing of messages for plant data logging and post-event analysis. In this context, a secure stratum-1 Time-Server module has been indigenously designed and developed for accurate time synchronization across computer-based C&I systems, plant servers and data loggers. It uses GPS time as primary source and provides accurate time synchronization using Network Time Protocol over existing Ethernet network. The indigenous NTP server uses an Operating System (OS)-less design with firmware on Field Programmable Gate Array (FPGA). In this article, we present the design, implementation and deployment scenario of indigenously developed NTP server suitable for use not only in C&I networks, but also in IT infrastructure.

KEYWORDS: *Global Positioning System (GPS), Time Synchronization, Network Time Protocol (NTP), Denial of Service (DoS)*

Introduction

Synchronizing clocks accurately in distributed systems has been an important long-standing challenge. Accurate clocks enable applications to operate on a common time axis across different nodes, which, in turn, enables key functions like consistency, event ordering, causality and scheduling of tasks and resources with precise timing. Time synchronization is of vital importance in variety of applications like distributed data acquisition, event analysis, blackout analysis and stability control of power grid[1], real-time networks based on Time Division Multiple Access(TDMA), financial online trading, large-scale experiments such as particle accelerators[2] etc.

Clock generators and communication channels are not ideal in reality which leads to inaccuracies in time synchronization. In clock generators, quantization, frequency drift due to temperature or ageing, jitter, wander etc. are practically expected. For communication channels, variations in the network delay and variable processing time are problematic and need to be compensated.

Most common protocols governing time transfer are Inter-Range Instrumentation Group (IRIG) time code, Network Time Protocol (NTP) and Precision Time Protocol (PTP). IRIG systems use dedicated coaxial cabling and has disadvantage of added expense and increased time skew. NTP is used to synchronize time across an Internet Protocol (IP) network. In addition to the advantage of accessibility of Ethernet, it also provides synchronization accuracy within 1 to 2 milliseconds which is limited only by network induced jitter. Taking advantage of the existing Ethernet infrastructure allows considerable reuse of in-place hardware and cabling, helping to reduce costs for the physical layer. The PTP has hardware-assisted time stamping, for better accuracy. PTP in ideal conditions with hardware time stamping and transparent clocks can eliminate the effect of the network delay and jitter on the offset measurement and synchronize the system clock with sub-microsecond accuracy. However, NTP is highly resilient. It works with multiple sources, estimates their errors, and selects only good sources for synchronization. In addition, NTP supports authentication with symmetric keys in order to allow clients to verify the authenticity and integrity of received packets and prevent attackers from synchronizing them to a false time.

Commercial NTP Servers have standard software packages running over operating systems like Linux. Unpatched, outdated software along with unused features introduce vulnerabilities making the network prone to concentrated attacks. Keeping in view the concerns and challenges, an indigenous NTP server has been developed in RCnD. Indigenous development will be advantageous from security aspects and will make the design transparent and amenable to verification and validation. The time synchronization functions in the NTP server are implemented on FPGA making it completely OS less. Implementation in FPGA provide accurate time keeping and better network throughput. The device has added features for security like blacklisting or white listing of each client IP. The indigenous design with extensive documentation makes the device amenable to V&V and suitable for deployment in applications having safety and security concerns. In this article, we present the design and implementation of this indigenously developed NTP server which is suitable for use in Control and Instrumentation networks of nuclear power plants and for other general applications.

Network Time Protocol (NTP)

NTP is a networking protocol for clock synchronization between computer systems/embedded systems over packet-switched, variable-latency data networks. NTP provides Coordinated Universal Time (UTC) including scheduled leap second adjustments.

A basic NTP network is composed of a time server and

*Author for Correspondence: Abhishek Borana
E-mail: aborana@barc.gov.in

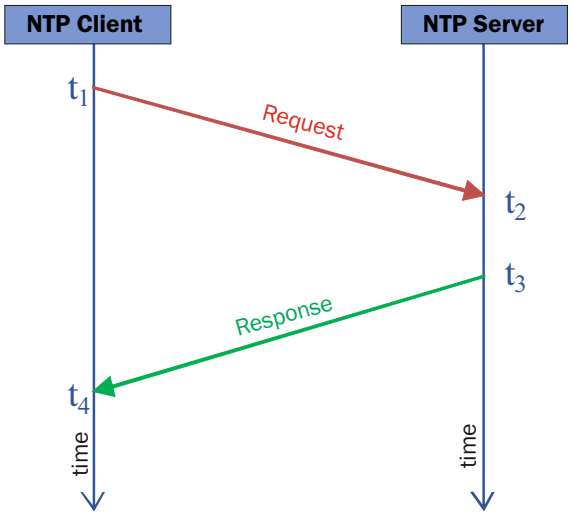

Fig.1: Timing Diagram of NTP client synchronization to a NTP Server.

clients (embedded nodes, workstations etc.). The function of time server is to provide accurate time to the clients. The individual clients run a small program as a background task that periodically queries the server for a precise UTC time reference. These queries are performed at designated time intervals in order to maintain the required synchronization accuracy for the network. In a local network, clients can be synchronized within 1 millisecond.

As depicted in Fig.1, client transmits query packet at time instance t_1. NTP server receives this request at time t_2 and transmits response packet at time t_3. Request and response packet consists of all required time stamps. The client process the response packet and calculate the time offset and the network induced delay as under:

$$\text{Offset} = [(t_2 - t_1) + (t_3 - t_4)] / 2$$

$$\text{Delay} = (t_4 - t_1) - (t_3 - t_2)$$

Client uses intersection algorithm to select accurate time servers and the algorithm is designed to mitigate the effects of variable network latency.

NTP Server is a stand-alone equipment which will maintain accurate time using GPS. Clients will synchronize using NTPv4 (as standardized in RFC5905). A standard NTP server operates in Client/Server, Symmetric Active/Passive or Broadcast modes. However, in our design, NTP server and clients will operate only in Client/Server mode along with client authentication for increased network security. It will also be possible to perform embedded C&I client authentication by server. NTP server is designed and developed such that it will also work with other Windows/Linux based PC nodes having built-in NTP client/server.

The synchronization architecture uses a stratum concept, which is a hierarchical model (tree type) with each server on one level (stratum) serving as a time server to the lower levels. Primary servers are set at the root of the tree as stratum-1 and are synchronized to external clock reference sources such as atomic clocks/GPS/IRNSS (stratum 0). Each of the subsequent levels has a stratum which is one higher than the preceding level as shown in Fig.2. The maximum allowed value for the stratum is 15.

NTP is designed for use by client and server machines with a wide range of capabilities and over a wide range of network delays and jitter characteristics. Commercial equipment and systems use a software package that include

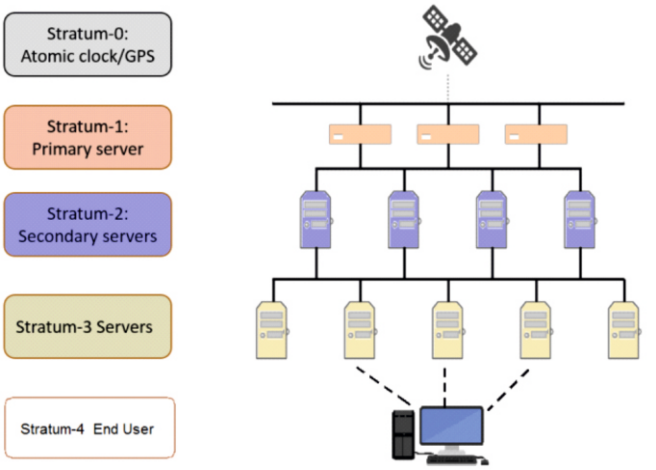

Fig.2: NTP Stratum Model.

Fig.3: Front View of NTP Server.

full suite of NTP options and algorithms, which are relatively complex. The software is ported to a wide variety of platforms ranging from personal computers to supercomputers, its sheer size and complexity is not appropriate for many applications. Server-side software, which do not require clock filtering, selection, clustering or combining algorithm also include a full set of complex software. The design is proprietary in nature, poses security issues and is not amenable to verification and validation. Accordingly, it was useful to explore alternative indigenous strategies using simpler software appropriate for high security applications.

Design

The NTP server, designed and developed as a stand-alone product as shown in Fig.3, works on stratum-1 level as a primary server. It is compatible with NTP clients implemented on commercial operating systems. It also provides configurable relay contact output for interface with existing/legacy C&I systems.

The design consists of NTP Agent implemented using FPGA, GPS receiver with Oven Controlled Crystal Oscillator (OCXO), and a Configuration Agent implemented using microcontroller as shown in Fig.4. The GPS receiver receives GPS signal through antenna. It provides UTC time and a synchronized 10MHz clock to NTP Agent. The NTP Agent (FPGA) is the core element which incorporates concurrent processing for better performance and accurate timing. It acquires time from GPS receiver and uses the synchronized 10MHz clock for time keeping. The FPGA is responsible for time keeping and processing and it acts as the primary NTP server to provide accurate time to various clients.

The NTP agent provides 4 Ethernet interfaces and processes concurrent NTP requests in parallel. It maintains a UTC time and also generates pps signal as a digital output. An internal battery operated RTC is provided to maintain the time till GPS lock is not achieved. For interface with existing plant C&I systems, relay contacts with configurable on-off time and pulse output is provided. Four independent RS485 interfaces are provided over which digital slave clocks can be interfaced using custom protocols.

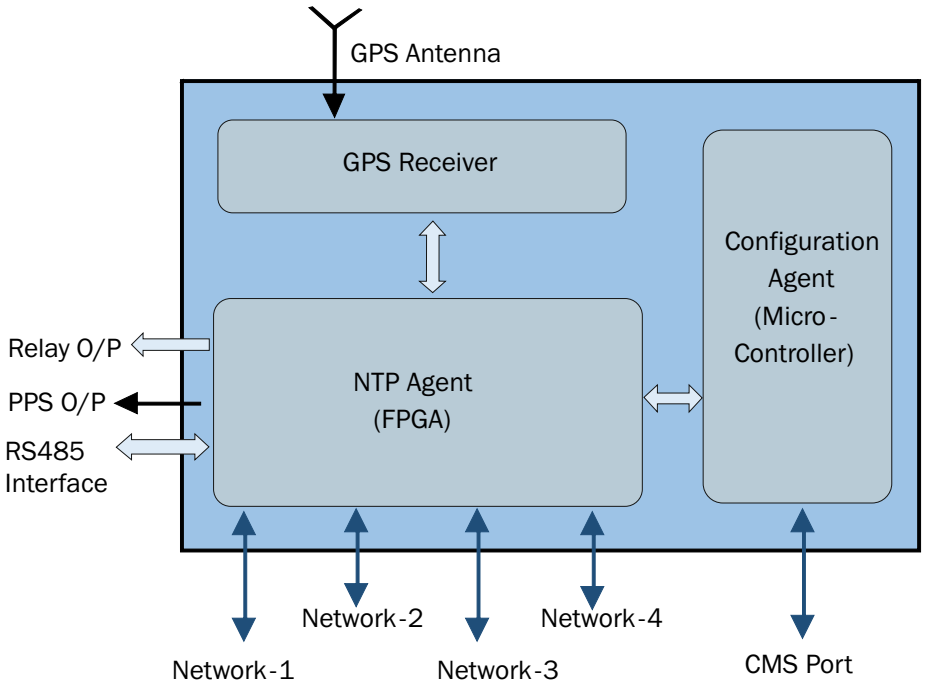

Fig.4: Block Diagram of NTP Server.

The Configuration Agent interfaces with Configuration management software (CMS) for configuration download and transfer of device statistics. It provides a secure web-server interface to a PC through a separate CMS Ethernet port.

Salient Features

The NTP server offers the following general features:

- GPS based Stratum-1 Network Time Protocol Server
- OS less implementation in FPGA
- Four independent NTP engines catering to 4 user ports
- 30,000 NTP requests per second per port
- Oscillator: OCXO ±5ppb
- 1U High 19" Rack mount, Dual Redundant Power Supply
- Power Consumption less than 10 watts
- Qualification: Climatic (Dry Heat and Damp Heat as per IS-9000)

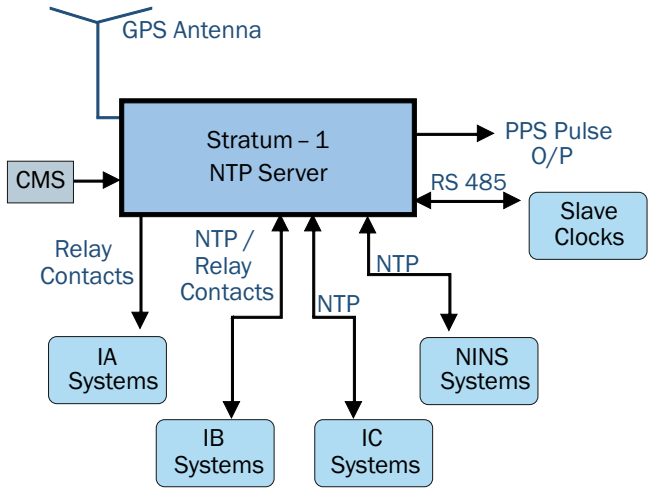

Fig.5: Typical deployment scenario for C&I systems of NPPs.

It offers the following performance features.

- GPS Accuracy: Max ± 35 nsec
- 24 Hour Holdover: Max ±10µsec/day at 25°C (on GPS signal loss)

It provides the following interfaces:

- GPS Interface : TNC
- Network Interface: 4x10/100/1000 Mbps
- Configuration Port : 1x10/100 Mbps
- Relay Output: 32 Contacts
- Digital Output (pps): 2 x Isolated Digital Output
- RS485 for Slave Clock: 4 Nos./10Mbaud

The following security features are incorporated in design:

- One Time programmable NTP stack in FPGA
- OS less NTP stack operation
- Encrypted FPGA configuration
- Whitelisted Clients with specified rate limiting

Security

Millions of hosts use the Network Time Protocol (NTP) to synchronize their computer clocks through timeservers on the Internet. Recently, the security of NTP over internet has come under new scrutiny. NTP plays a major role in UDP amplification attacks[3,4]. Now, there is a new focus on attacks on the NTP protocol itself, both in order to maliciously alter a target's time (*'timeshifting attacks'*) or to prevent a target from synchronizing its clock (*'denial of service' - DoS attacks*)[5]. These attacks are of concern because the correctness of time has a bearing on many other basic protocols and services. For instance, cryptographic protocols use timestamps to prevent replay attacks and limit the use of stale or compromised cryptographic material (e.g., TLS, HSTS, DNSSEC, authentication protocols). Rate limiting of incoming traffic, client authentication and better timing achieved using FPGA

Fig.6: Deployment in ITS lab of RCnD.

implementation makes the indigenous device better in terms of the above mentioned security concerns against the commercially available devices.

Deployment Scenario

Fig.5 depicts a typical deployment scenario of a Master clock System.

The NTP server provides time synchronization services to various C&I systems and time keeping equipment in the plant. Slave clocks provide the interface to the large station clock in control room which is synchronized to the GPS time broadcast by server on a RS485 link. The NTP server unit was designed, fabricated and tested, and it has been installed in Integrated Test Station (ITS) lab of RCnD in BARC. Different C&I systems in the lab were interfaced with the server unit over Ethernet as shown in Fig.6. Subsequently, it was installed and tested for time synchronization in networked seismic stations across Mumbai and Bengaluru. It has also been installed in Dhruva and interfaced to slave clocks in the plant.

Conclusions

Accurate Time synchronization is not only useful in event data logging in a distributed plant environment but is also important in IT infrastructure, distributed sensor network etc. NTP is most common protocol for time synchronization providing accuracy, cost and maintainability benefits over existing Ethernet infrastructure. An indigenous stratum-1 GPS based NTP Server has been designed and developed to provide accurate time synchronization among various C&I systems, plant servers, station clocks, etc. This helps in proper chronological logging of messages for post-event analysis. It is designed to support existing relay-based synchronization of C&I systems and servers. The FPGA based design provides inherent benefit of timing accuracy and stability, and gives an edge over the commercial devices that are equipped with standard software packages and unused features which make the entire network vulnerable to security attacks. Various security features of the device make it suitable for use in plant C&I network and critical IT infrastructure. This device offers an indigenous solution to replace the central clock system in nuclear plants which are expensive and available from limited vendors.

References

[1] Steinhauser, F.; Riesch, C.; Rudigier, M., IEEE 1588 for time synchronization of devices in the electric power industry, Proceedings of the International IEEE Symposium on Precision Clock Synchronization for Measurement, Control and Communication (ISPCS), Portsmouth, NH, USA, 27 September–1 October 2010, 1–6.

[2] Lipinski, M.; Wlostowski, T.; Serrano, J.; Alvarez, P., White rabbit: A PTP application for robust sub-nanosecond synchronization, Proceedings of the 2011 IEEE International Symposium on Precision Clock Synchronization for Measurement, Control and Communication, Munich, Germany, 9–12 September 2011, 25–30.

[3] Czyz, J., Kallitsis, M., Gharaibeh, M., Papadopoulos, C., Bailey, M., Karir, M., Taming the 800 pound gorilla: the rise and decline of NTP distributed denial-of-service (DDoS) attacks, Proceedings of the 2014 Internet Measurement Conference, 2014, 435–448.

[4] Kramer, L., Krupp, J., Makita, D., Nishizoe, T., Koide, T., Yoshioka, K., Rossow, C., AmpPot: monitoring and defending against amplification DDoS attacks, In: Bos, H., Monrose, F., Blanc, G. (eds.) RAID 2015. LNCS, Springer, 2015, 9404, 615–636.

[5] Malhotra, A., Cohen, I.E., Brakke, E., Goldberg, S., Attacking the network time protocol, In: NDSS 2016, February.