Mitigating an NTP Distributed Denial of Service (DDoS) Attack

Pritam Kandel, Applications Engineer, *Orolia*

September 2018

Contents

Who Should Read This White Paper?

Network and System Engineers
Network and System Architects
Network and System Administrators
Directors/Managers of IT Infrastructure
CTOs.

Introduction

Network time service is not something many businesses think about as a key component of their critical infrastructures. In fact, it is often overlooked entirely, and in error. As a result, the network architect or engineer often defaults to an easy alternative: using a server or network switch as the source of the network clock and synchronizing these sources to Internet time servers using Network Time Protocol (NTP).

However, is the "NTP over Internet" really a secure method to solve network timekeeping requirements? Is it okay for some industries, and not others? Let's explore the subject.

NTP Over Internet: How Safe is It?

NTP, one of the oldest internet protocols in use, is the standard for synchronizing clocks between computers over a packet-switched network – such as the Internet.

According to the Akamai global state of the Internet security report (Summer 2018), NTP over Internet is the second most common protocol being attacked by DDoS. And, in just a year, DDoS attacks have increased by 16%.

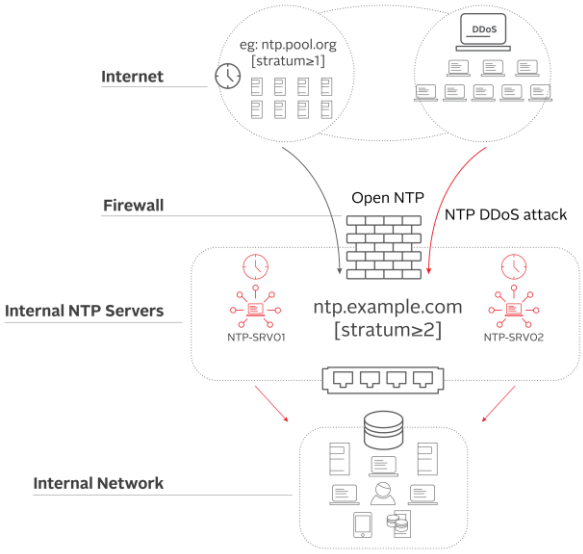

Figure 1: A typical deployment of enterprise timekeeping using NTP over Internet.

Figure 1 shows how a typical NTP over Internet setup works. It consists of a public pool of NTP servers (NTP Stratum 1) that is used as a reference by internal time servers to receive time. This approach requires a communication path between the Internet and internal time servers through the firewall, which opens access to the network and creates a vulnerability that hackers can use to infiltrate your entire system. For networks using this method, not only can the timing infrastructure become ripe for cyberattacks, the quality of time is also compromised, in terms of both precision and accuracy.

A Better Solution: Your Own Stratum 1 NTP Server

If you are using the Internet as the source of your time, it is unfortunately a myth to believe that your firewall -- even the next-gen firewall that comes with IDS (Intrusion Detection System) or IPS (Intrusion Prevention System) functionality – will protect you from DDoS attacks.

So how can you mitigate DDoS for time service?

The expression, "a chain is only as strong as its weakest link," couldn't be truer in the case of DDoS attacks. At Orolia, we recommend a very effective and simple solution to our customers: Eliminate the weakest link in the chain. In other words, don't rely on the Internet for your network time.

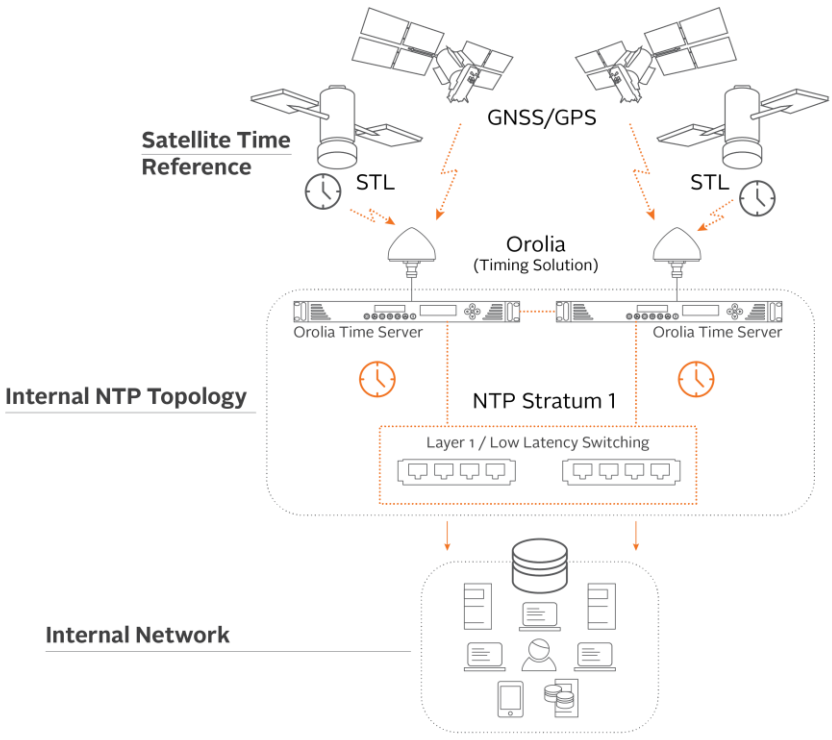

Figure 2. A typical resilient timing infrastructure for enterprise with Orolia time servers.

Figure 2 shows how an enterprise can eliminate the "weakest link" – by building its own resilient and redundant network timekeeping infrastructure internally, using Orolia time servers, such as the SecureSync, VersaSync (for ruggedized environments) or VelaSync (for high-speed trading environments).

Each Orolia time server receives time signals through a GNSS (Global Navigation Satellite System) or GPS (Global Position System) antenna and regulates its internal high-quality oscillator clock with that information. The time, with accuracy under Nano seconds, is then distributed to the network. If NTP is used as the preferred protocol, then the server will operate at NTP Stratum level 1, and distribute safe, reliable time to the remainder of your network without the use of an internet connection.

Other Advantages of Internal Timekeeping

In addition to mitigating danger from DDoS attacks, time servers such as those from Orolia offer several other advantages, including:

1. **Resiliency** – Each Orolia time server unit can use multi-GNSS for its time reference. However, if a GNSS/GPS signal is not available, Orolia time servers also contain an internal holdover oscillator capable of maintaining accurate time for days, or even months, using atomic clock technology in the absence of a valid GNSS signal.
2. **RF Signal Security** – Anti-jamming, anti-spoofing and signal security are engrained in Orolia time servers. Customers in need of even higher levels of security also include our Broadshield ™ and anti-jamming antenna solutions.
3. **High Integrity UTC Traceable Time** – Sophisticated threats can spoof GNSS. Though these threats are detectable by Broadshield, how is traceability to UTC maintained? STL is there for the rescue. As an alternate encrypted antenna signal, STL supplies powerful authentication to confirm that you have true UTC traceability.
4. **Ease of Installation** – Does your environment make it difficult to achieve roof access to capture a GNSS signal? Again, STL to the rescue. Much stronger than GPS or any GNSS signal, STL can be received indoors. At a recent demonstration, STL provided solid reception inside the NYSE building, located in one of the most severe urban canyons in the world, where a view of the sky for GNSS reception is very limited.
5. **Multiple Options** – In addition to full NTP compatibility, Orolia time servers support multiple protocols and options to distribute time, like Precision Time Protocol (PTP), Pulse Per Second (PPS) and other time signals as suited to customer requirements. Plus, industry-leading support is standard.

Conclusion

In today's threat-laden environment, it is only too easy to jam or spoof the network, causing anything from minor disruption to extreme havoc within a critical infrastructure. Reliance upon NTP over Internet has inherent risks, which can easily be mitigated by using your own Stratum 1 NTP server, which will provide high-integrity UTC traceable time. Adding anti-jam and anti-spoof software and antennas will give you an even higher level of resiliency and security. The real question to ask yourself is: Can your company afford the risk of a DDoS attack? If the answer is no, then an upgrade to a Stratum 1 NTP server should be *de rigueur*.

About the Author

Pritam Kandel is an Applications Engineer with over a decade of experience working in design, assessment and implementation of TCP/IP routing and switching infrastructure for network cores/backbones, datacenters, Internet edge and WAN. He is experienced with maintaining IT infrastructure, including Internet peering and ISP services, MPLS and carrier networks, and VoIP global infrastructure. He holds certifications in CCNP, CCNA, JNCIA, MPLS Deployment, Alcatel Lucent and NIX platforms. Pritam is a graduate of the Rochester Institute of Technology with an MBA in Technology Management and holds a Bachelor of Engineering in IT from Pokhara University.

About Orolia

Orolia is the world leader in resilient positioning, navigation and timing (PNT) solutions that improve the reliability, performance and safety of critical, remote or high-risk operations. With locations in more than 100 countries, Orolia provides virtually failsafe GPS/GNSS and PNT solutions to support military and commercial applications worldwide.

USA

Orolia USA Inc.

1565 Jefferson Road

Suite 460

Rochester, NY 14623

Phone: +1.585.321.5800

France

Spectracom SAS

Parc Technopolis, Bât. Gamma

3 Avenue du Canada

91974 Les Ulis, Cedex, France

Phone: +33 (0)1.64.53.39.80

Singapore

Orolia Asia Pacific Office

1 Changi Business Park Crescent

Changi Business Park

Singapore 486025

Phone +65 8725 5543

www.orolia.com

www.spectracom.com

August, 2018 - Rev O