Deep dive into ntp pool's popularity and mapping

Moura, Giovane C.M.; Davids, Marco; Schutijser, Caspar; Hesselman, Cristian; Heidemann, John; Smaragdakis, Georgios

DOI
10.1145/3652963.3655051

Publication date
2024

Document Version
Final published version

Published in
SIGMETRICS/PERFORMANCE 2024 - Abstracts of the 2024 ACM SIGMETRICS/IFIP PERFORMANCE Joint International Conference on Measurement and Modeling of Computer Systems

Citation (APA)
Moura, G. C. M., Davids, M., Schutijser, C., Hesselman, C., Heidemann, J., & Smaragdakis, G. (2024). Deep dive into ntp pool's popularity and mapping. In *SIGMETRICS/PERFORMANCE 2024 - Abstracts of the 2024 ACM SIGMETRICS/IFIP PERFORMANCE Joint International Conference on Measurement and Modeling of Computer Systems* (pp. 9-10). (SIGMETRICS/PERFORMANCE 2024 - Abstracts of the 2024 ACM SIGMETRICS/IFIP PERFORMANCE Joint International Conference on Measurement and Modeling of Computer Systems). Association for Computing Machinery (ACM). https://doi.org/10.1145/3652963.3655051

Deep Dive into NTP Pool's Popularity and Mapping

Giovane C. M. Moura
SIDN Labs and
Delft University of Technology
Arnhem and Delft, The Netherlands
giovane.moura@sidn.nl

Marco Davids
SIDN Labs
Arnhem, The Netherlands
marco.davids@sidn.nl

Caspar Schutijser
SIDN Labs
Arnhem, The Netherlands
caspar.schutijser@sidn.nl

Cristian Hesselman
SIDN Labs and University of Twente
Arnhem and Enschede, The Netherlands
cristian.hesselman@sidn.nl

John Heidemann
USC/ISI and CS Dept.
Los Angeles, California, USA
johnh@isi.edu

Georgios Smaragdakis
Delft University of Technology
Delft, The Netherlands
g.smaragdakis@tudelft.nl

ABSTRACT

Time synchronization is of paramount importance on the Internet, with the Network Time Protocol (NTP) serving as the primary synchronization protocol. The NTP Pool, a volunteer-driven initiative launched two decades ago, facilitates connections between clients and NTP servers. Our analysis of root DNS queries reveals that the NTP Pool has consistently been the most popular time service. We further investigate the DNS component (GeoDNS) of the NTP Pool, which is responsible for mapping clients to servers. Our findings indicate that the current algorithm is heavily skewed, leading to the emergence of time monopolies for entire countries. For instance, clients in the US are served by 551 NTP servers, while clients in Cameroon and Nigeria are served by only one and two servers, respectively, out of the 4k+ servers available in the NTP Pool. We examine the underlying assumption behind GeoDNS for these mappings and discover that time servers located far away can still provide accurate clock time information to clients. We have shared our findings with the NTP Pool operators, who acknowledge them and plan to revise their algorithm to enhance security.

CCS CONCEPTS

• **Networks** → **Application layer protocols**; **Network measurement**; **Naming and addressing**; **Location based services**; **Network monitoring**.

KEYWORDS

NTP; NTP Pool; DNS; Measurements; Client mapping

ACM Reference Format:
Giovane C. M. Moura, Marco Davids, Caspar Schutijser, Cristian Hesselman, John Heidemann, and Georgios Smaragdakis. 2024. Deep Dive into NTP Pool's Popularity and Mapping. In *Abstracts of the 2024 ACM SIGMETRICS/IFIP PERFORMANCE Joint International Conference on Measurement and Modeling of Computer Systems (SIGMETRICS/PERFORMANCE Abstracts '24), June 10–14, 2024, Venice, Italy*. ACM, New York, NY, USA, Article 15, 2 pages. https://doi.org/10.1145/3652963.3655051

SIGMETRICS/PERFORMANCE Abstracts '24, June 10–14, 2024, Venice, Italy

ACM ISBN 979-8-4007-0624-0/24/06
https://doi.org/10.1145/3652963.3655051

1 INTRODUCTION

Global time synchronization underpins modern life. It is crucial to the Internet and to critical systems such as financial markets, power grids, and telecommunications networks, and businesses [5, 6].

On the Internet, many commonly used applications, services, and protocols depend on clock correctness for secure operations. TLS, DNSSEC, DNS caches, RPKI, Kerberos and even Bitcoin transactions are are some of the applications that depend on clock synchronization to prove cryptographic freshness [3, 7, 8, 17].

The Network Time Protocol (NTP) [8] is the Internet's default protocol for clock synchronization. It is designed to mitigate the effects of changing network latency (jitter) between client and server. NTP *servers* synchronize out-of-band with high precision references, such as atomic clocks, radio signals (*e.g.,* DC77 [2]), and satellites (GPS and Galileo).

There are many publicly available NTP servers on the Internet. NIST [11] and the USNO [15] have been providing NTP services for decades. Later, several vendors such as Apple, Google, Cloudflare, Meta, Microsoft and Ubuntu started their own services.

The NTP Pool [14] provides a layer over NTP servers, providing a directory of publicly available NTP servers using DNS [9]; it does not directly operate NTP servers. The NTP servers themselves are run by volunteers, which range from home DSL users to large cloud operators. The NTP Pool currently lists 4,403 volunteer NTP servers, with 3,056 on IPv4 and 1,671 on IPv6 (2023-10-09) [13]. It has been operating for more than two decades.

Numerous organizations operate NTP servers to sync device clocks within their networks. The DHCP protocol [4] allows to clients be configured also with NTP servers, automating the process. However, lacking in-house NTP servers, client clocks resort to synchronization with public, pre-configured NTP servers. Home user devices also typically resort to their pre-configured NTP servers.

Given this context, our study set out the investigate the following research questions:

(1) *What are the most popular public time services on the Internet?* Does the NTP Pool maintain its relevance in the current era, considering the emergence of large vendors offering free time services?

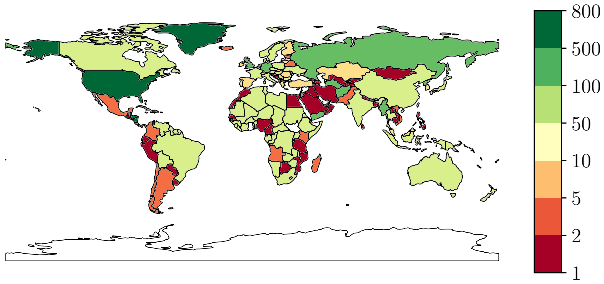

Figure 1: Number of time providers assigned by the NTP Pool to each country.

(2) *What is the methodology employed by the NTP Pool to determine the server-client allocation?* The NTP Pool leverages DNS for client-server mapping, but what is the underlying process? Are there any issues with these mappings?
(3) *Can existing mapping problems be remediated? If so, how?* If the mapping algorithm of the NTP Pool is not optimal, what improvements can we suggest to improve it?

2 CONTRIBUTIONS

Our first contribution is to *demonstrate that the NTP Pool is not only in active use, but it has consistently been the most popular time-service provider on the Internet*, based on DNS traffic at the Root DNS servers [16]. This popularity persists even with the introduction of new time services introduced by large vendors in recent years.

Our second contribution is to *demonstrate how these mappings are executed and which criteria are employed in this process.* We examine `GeoDNS` [1], the NTP Pool customized DNS software that perform the mapping, complemented by measurements taken from the public Internet. Previous studies offered only anecdotal evidence of these mappings. Through our detailed examination and reverse-engineering, we can now forecast client-server mappings for entire nations.

Our third contribution is *to explore the implications of this mapping, from our ability to predict which NTP servers a client will use.* We find that assignments can be heavily skewed, producing time service monopolies. Even with more than 4k NTP servers, 27 countries are assigned to a single time provider—one operator serves 767M people and 465M Internet users, as shown in Figure 1. In addition, we find that another 101 countries and territories (comprising 260M Internet users) could be monopolized with the deployment of a *single* NTP server. This monopolization bestows immense power upon a single actor [12], which can then be misused (or exploited) to execute nation-wide scale time-shift attacks, particularly worrisome in today's world where conflicts extend into cyberspace.

Our fourth and final contribution is to *show that the current `GeoDNS` mapping algorithm can be changed to improve server distribution without compromising service quality.* Conversations with NTP Pool operators indicate that these mappings are designed to avoid asymmetric routing and alleviate concerns about packet loss. However, our experimental results contradict these apprehensions about substantial packet loss from distant servers: we demonstrate that far away NTP servers can also deliver high-quality timing services with minimal packet loss ratios. Consequently, we recommend that NTP Pool operators consider modifying their mapping algorithm to address these monopolization issues, which could potentially result in a complete or partial time synchronization takeover for entire countries.

An extended version of this paper is available at [10].

ACKNOWLEDGEMENTS

The work of Giovane C. M. Moura, Marco Davids, Caspar Schutijser, and Cristian Hesselman was carried out as part of the SIDN Labs funded project, `time.nl` (https://time.nl). Cristian Hesselman's work was also part of the Network Security program of the Twente University Centre for Cybersecurity Research (TUCCR, https://tuccr.nl).

John Heidemann's work on this paper is partially supported by NSF projects CNS-2212480 and CNS-2319409.

Georgios Smaragdakis' work on this paper was partially funded by the European Research Council under starting grant ResolutioNet (679158), the Dutch 6G flagship project "Future Network Services" with funding from the National Growth Fund, and the European Union research and innovations programme Horizon Europe under grants SEPTON (101094901), MLSysOps (101092912), and TANGO (101070052).

REFERENCES

[1] Ask Bjørn Hansen. 2021. GeoDNS servers. https://github.com/abh/geodns/.
[2] Physikalisch Technische Bundesanstalt. 2022. FDCF77 - PTB.de. (Nov. 5 2022). https://www.ptb.de/cms/en/ptb/fachabteilungen/abt4/fb-44/ag-442/dissemination-of-legal-time/dcf77.html
[3] Omer Deutsch, Neta Rozen Schiff, Danny Dolev, and Michael Schapira. 2018. Preventing (Network) Time Travel with Chronos.. In *NDSS*.
[4] Ralph Droms. 1997. *Dynamic Host Configuration Protocol.* RFC 2131. IETF. http://tools.ietf.org/rfc/rfc2131.txt
[5] Nate Hopper. 2022. The Thorny Problem of Keeping the Internet's Time. *The New Yorker* (Sept. 30 2022). https://www.newyorker.com/tech/annals-of-technology/the-thorny-problem-of-keeping-the-internets-time
[6] Leslie Lamport. 2019. *Time, Clocks, and the Ordering of Events in a Distributed System.* Association for Computing Machinery, New York, NY, USA, 179–196. https://doi.org/10.1145/3335772.3335934
[7] Aanchal Malhotra, Isaac E Cohen, Erik Brakke, and Sharon Goldberg. 2016. Attacking the Network Time Protocol. In *Proceedings of the 23rd Network and Distributed System Security Symposium (NDSS 2016)* (San Diego, California).
[8] David Mills, Jim Martin, Jack Burbank, and William Kasch. 2010. *Network Time Protocol Version 4: Protocol and Algorithms Specification.* RFC 5905. IETF. http://tools.ietf.org/rfc/rfc5905.txt
[9] Paul Mockapetris. 1987. *Domain names - concepts and facilities.* RFC 1034. IETF. http://tools.ietf.org/rfc/rfc1034.txt
[10] Giovane C. M. Moura, Marco Davids, Caspar Schutijser, Cristian Hesselman, John Heidemann, and Georgios Smaragdakis. 2024. Deep Dive into NTP Pool's Popularity and Mapping. 8, 1, Article 15 (feb 2024), 30 pages. https://doi.org/10.1145/3639041
[11] NIST. 2022. NIST Internet Time Service (ITS). (Nov. 5 2022). https://www.nist.gov/pml/time-and-frequency-division/time-distribution/internet-time-service-its
[12] M. Nottingham. 2023. *Centralization, Decentralization, and Internet Standards.* RFC 9518. IETF. http://tools.ietf.org/rfc/rfc9518.txt
[13] NTP Pool. 2021. All Pool Servers. https://www.ntppool.org/zone.
[14] NTP Pool. 2021. pool.ntp.org: the internet cluster of ntp servers. https://www.ntppool.org/en/.
[15] United States Naval Observatory. 2022. Information about NTP, the time backbone of the Internet. (Nov. 5 2022). https://www.cnmoc.usff.navy.mil/Our-Commands/United-States-Naval-Observatory/Precise-Time-Department/Network-Time-Protocol-NTP/
[16] Root Server Operators. 2021. Root DNS. http://root-servers.org/.
[17] Teemu Rytilahti, Dennis Tatang, Janosch Köpper, and Thorsten Holz. 2018. Masters of Time: An Overview of the NTP Ecosystem. In *2018 IEEE European Symposium on Security and Privacy (EuroS P).* 122–136. https://doi.org/10.1109/EuroSP.2018.00017