Survivable, Real Time Network Services

Defense Advanced Research Projects Agency
Contract F30602-98-1-0225, DARPA Order G409/J175

Quarterly Progress Report
1 October 2001 - 31 December 2001

David L. Mills
Electrical Engineering Department
University of Delaware

1. Introduction

This report covers the work done in support of the DARPA Information Technology Office program in computer networking. Contributors to this effort include Prof. David L. Mills, graduate student Harish Nair and undergraduate research student John Conner. MS student Tamal Basu has graduated and taken a position at Acorn Networks. Phd student Qiong Li has graduated and taken a position with Phillips Research.

The project continues research in network time synchronization technology funded by DARPA, US Army ARL and NASA/JPL. The technology makes use of the Network Time Protocol (NTP), widely used in the Internet, together with engineered modifications designed to improve accuracy in high speed networks. Specific applications benefiting from this research include multicast topologies, multimedia, real-time conferencing, cryptographic systems, and management of distributed, real-time systems and sensor networks.

This quarterly report is submitted in traditional report form on paper. As the transition to web-based information dissemination of research results continues, almost all status information and progress reporting is now on the web, either on pages belonging to the principal investigator or to his students. Accordingly, this and future progress reports will contain primarily schedule and milestone data; current status and research results are reported on web pages at www.eecis.udel.edu/~mills in the form of papers, technical reports and specific briefings.

2. Autonomous Authentication

Version 2 of the Autokey protocol has been installed in the core routers of the CAIRN network and is operating normally. The protocol is now included in the general release software distribution available from the NTP web site www.ntp.org. Various minor problems have been reported by other users and corrected. Linux continues as the single largest source of bug reports, almost always because of some idiosyncratic incompatibility with respect to Solaris, Tru64 and FreeBSD.

The current state of Autokey development and plans are at www.eecis.udel.edu/~mills/autokey.htm.

3. Autonomous Configuration

Work continues on the development and test of the Manycast autonomous configuration scheme. In this scheme a multicast client sends an ordinary request packet to a multicast group address and potential multicast servers in TTL range have the opportunity to respond with an ordinary unicast message. Each received message causes the client to mobilize an ephemeral association, which then proceeds as if the server were originally explicitly configured.

The problem reported previously with an incompatibility with the OpenSSL cryptographic library has been found and fixed. This avoids the hassle of upgrading all CAIRN routers to FreeBSD 4.2 and, in particular, fixing an elusive bug in FreeBSD 3.4 with the T1 driver.

The current status of the Manycast mode and implementation is available via the web at www.eecis.udel.edu/~mills/autocfg.htm.

4. NTP and IPv6

Some progress has been made on the IPv6 port of NTP by the folks at Viagenie in Canada. Some bugs have been fixed, but the Autokey and Manycast features still do not work. One important contribution is a script that performs the same function as the ntptrace utility. That utility works backwards through the NTP subnet from the client to the primary server and reveals each server on the path. The problem is that the NTPv6 packet format does not provide the back pointer that the NTPv4 packet does. The script uses the NTP control/monitoring protocol to extract the back pointer. We expect to continue with this project in a collaboration with Viagenie and UCL.

5. Timekeeping in the Interplanetary Internet

With support from Jet Propulsion Laboratories (JPL) and NASA, we are working on a study of timekeeping issues in the Interplanetary Internet, specifically for Mars missions and supporting infrastructure. Currently, the clocks for all space vehicles are coordinated on Earth using a software library called SPICE. With new technology, timekeeping in space would be distributed so that timed experiments could be accurately controlled autonomously and without intervention from Earth. There are three issues which distance the new technology from current practice: bodies are moving, connectivity between them is necessarily not continuous and transmission delays can be very long. An outline of the proposed activity was presented in the last report.

In order to study the issues with interplanetary timekeeping, we are building a simulator using the stock NTP software suitably modified to measure the response to programmed test variations in time and frequency. The plan is to insert ahead of the NTP algorithms a software shim that simulates range and range rate variations typical of spacecraft navigation. We plan to develop a test script typical of current missions using SPICE. The script would include time and frequency variations for interplanetary distances and near-MARS orbits. Then, selective algorithms in the SPICE library would be incorporated in the shim to normalize these real-time variations according to ephemerides data available to the simulator. The object is to study the NTP response and in particular the errors that may accrue.

We have completed an initial test vehicle for the NTP simulator. It includes provisions to program step offsets in time and frequency, as well as a synthetic noise generator that was developed for a previous project. The noise generator faithfully models the behavior of a typical computer clock

oscillator jitter and wander. A particularly attractive feature is that the stock NTP algorithms required very few intrusive hooks and the statistical data collection provisions continue to work.

The current status of the Interplanetary Internet timekeeping project is available via the web at www.eecis.udel.edu/~mills/ipin.htm.

6. Infrastructure

There have been a continuous stream of contributions to the NTP software distribution from the developer's group. Recent contributions include a driver for the TrueTime IRIG timecode reader and a driver for the Japan time and frequency standard station JJY.

7. Future Plans

Our plans for the next quarter include further work on the NTP book mentioned in the previous report. All eleven chapters in about 150 pages have been converted from O'Reilly format to a more friendly format which can be easily adapted to whatever book publisher takes the bait. The chapter on time metrology been updated due to recent changes recommended by the International Astronomical Union. Most of the other chapters are in good shape, but the theory sections need to be fine tuned and verified. All the chapters need appropriate introduction and summary sections.

We plan to extend the Autokey protocol to include dynamic trust dependencies involving host groups similar to PGP. We also plan to upgrade to version 3 of the X.509 certificate and include provisions for automatically verifying the certificate trail. Eventual plans are to integrate a certificate discovery function in the manycast scheme, which is necessary for a field-deployable sensor network.

We plan to continue work on the Autoconfigure scheme, in particular a rewrite of the configuration code and name resolution code. This would allow certificates to be retrieved from other than the manycast servers found, in particular from public repositories should this be useful. An interesting problem yet to be resolved is how to develop a security metric which could be used in conjunction with the current synchronization to refine the server selection algorithm.

We plan to continue investigation of timekeeping issues for the Interplanetary Internet, including synchronization paradigms where connectivity between moving objects is not continuous.

We plan to continue the refining of the Autokey protocol specification, as defined in the current Internet Draft, eventually to Internet Standard status. Eventual plans are to update the NTP Version 3 specification to reflect the current NTP Version 4 architecture, protocol and algorithms.

8. Publications

All publications, including journal articles, symposium papers, technical reports and memoranda are now on the web at www.eecis.udel.edu/~mills. Links to the several publication lists are available on that page, as well as links to all project descriptions, status reports and briefings. All publications are available in PostScript and PDF formats. Briefings are available in HTML, PostScript, PDF and PowerPoint. The project descriptions are cross-indexed so that the various interrelationships are clearly evident. Also included are the documentation pages for various public software distributions. Links to other related projects at Delaware and elsewhere are also

included on the various pages. Hopefully, the organization of these pages, which amount to a total of about 300 megabytes of information pages and reference documents, will allow quick access to the latest results and project status in a timely way.

Following is a retrospective list of papers and reports supported wholly or in part on this project and the immediately preceding project "Scalable, High Speed, Internet Time Synchronization," DARPA Order D012. The complete text of all papers and reports, as well as project briefings, status reports and supporting materials is at www.eecis.udel.edu/~mills.

8.1 Papers

1. Li, Q., and D.L. Mills. Jitter-based delay boundary prediction of wide-area networks. *IEEE/ ACM Trans. Networking 9, 5* (October 2001), 578-590

2. Levine, J., and D. Mills. Using the Network Time Protocol to transmit International Atomic Time (TAI). *Proc. Precision Time and Time Interval (PTTI) Applications and Planning Meeting* (Reston VA, November 2000), 431-439.

3. Mills, D.L., and P.-H. Kamp. The nanokernel. *Proc. Precision Time and Time Interval (PTTI) Applications and Planning Meeting* (Reston VA, November 2000), 423-430.

4. Mills, D.L. A brief history of NTP time: confessions of an Internet timekeeper. Submitted for publication; please do not cite or redistribute.

5. Li, Q., and D.L. Mills. Investigating the scaling behavior, crossover and anti-persistence of internet packet delay dynamics. *Proc. 1999 IEEE GLOBECOM 99 Symposium* (Rio de Janerio, Brazil, December 1999).

6. Mills, D.L. Cryptographic authentication for real-time network protocols. In: *AMS DIMACS Series in Discrete Mathematics and Theoretical Computer Science, Vol. 45* (1999), 135-144.

7. Mills, D.L. Adaptive hybrid clock discipline algorithm for the Network Time Protocol. *IEEE/ACM Trans. Networking 6, 5* (October 1998), 505-514.

8. Mills, D.L., T.S. Glassey, and M.E. McNeil. Authentication scheme extensions to NTP. Internet Draft draft-mills-ntp-auth-coexist-01.txt, University of Delaware and Glassey-McNeil Technologies, September 1998, 9 pp.

9. Li, Qiong, and D.L. Mills. On the long-range dependence of packet round-trip delays in Internet. *Proc. IEEE International Conference on Communications* (Atlanta GA, June 1998), 1185-1191.

10. Mills, D.L., A. Thyagarajan and B.C. Huffman. Internet timekeeping around the globe. *Proc. Precision Time and Time Interval (PTTI) Applications and Planning Meeting* (Long Beach CA, December 1997), 365-371.

11. Mills, D.L. Authentication scheme for distributed, ubiquitous, real-time protocols. *Proc. Advanced Telecommunications/Information Distribution Research Program (ATIRP) Conference* (College Park MD, January 1997), 293-298.

12. Mills, D.L. The network computer as precision timekeeper. *Proc. Precision Time and Time Interval (PTTI) Applications and Planning Meeting* (Reston VA, December 1996), 96-108.

13. Mills, D.L. Improved algorithms for synchronizing computer network clocks. *IEEE/ACM Trans. Networks 3, 3* (June 1995), 245-254.

8.2 Technical Reports

14. Mills, D.L. Public key cryptography for the Network Time Protocol. Electrical Engineering Report 00-5-1, University of Delaware, May 2000. 23 pp.

15. Mogul, J., D. Mills, J. Brittenson, J. Stone and U. Windl. Pulse-per-second API for Unix-like operating systems, version 1. Request for Comments RFC-2783, Internet Engineering Task Force, March 2000, 31 pp.

16. Sethi, A.S., H. Gao, and D.L. Mills. Management of the Network Time Protocol (NTP) with SNMP. Computer and Information Sciences Report 98-09, University of Delaware, November 1997, 32 pp.

17. Mills, D.L. A precision radio clock for WWV transmissions. Electrical Engineering Report 97-8-1, University of Delaware, August 1997, 25 pp.

18. Mills, D.L. Clock discipline algorithms for the Network Time Protocol Version 4. Electrical Engineering Report 97-3-3, University of Delaware, March 1997, 35 pp.

19. Mills, D.L. Proposed authentication enhancements for the Network Time Protocol version 4. Electrical Engineering Report 96-10-3, University of Delaware, October 1996, 36 pp.

20. Mills, D.L. Simple network time protocol (SNTP) version 4 for IPv4, IPv6 and OSI. Network Working Group Report RFC-2030, University of Delaware, October 1996, 18 pp.

21. Mills, D.L. Simple Network Time Protocol (SNTP). Network Working Group Report RFC-1769, University of Delaware, March 1995, 14 pp.

22. Mills, D.L. Simple Network Time Protocol (SNTP). Network Working Group Report RFC-1769, University of Delaware, March 1995, 14 pp.

8.3 Internet Drafts

23. Mills, D.L. Public-Key Cryptography for the Network Time Protocol. Internet Draft draft-ietf-stime-ntpauth-01.txt, University of Delaware, April 2001, 45 pp.

24. Mogul, J., D. Mills, J. Brittenson, J. Stone and U. Windl. Pulse-Per-Second API for UNIX-like Operating Systems, Version 1.0. Internet Draft draft-mogul-pps-api-05.txt, Compaq Western Research Laboratory, August 1999, 30 pp. (obsoleted by RFC-2783)

25. Mills, D.L., T.S. Glassey, and M.E. McNeil. Authentication Scheme Extensions to NTP. Internet Draft draft-mills-ntp-auth-coexist-01.txt, University of Delaware and Glassey-McNeil Technologies, September 1998, 9 pp. (expired)