Scalable, High Speed, Internet Time Synchronization

Defense Advanced Research Projects Agency
Contract DABT 63-95-C-0046

Quarterly Progress Report
1 March 1998 - 31 May 1998

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 students Qoing Li and Robert Redwinski, and undergraduate student Douglas Miller. The project continues previous research in network time synchronization technology jointly funded by DARPA, NSF, US Navy and US Army. 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.

Recent quarterly reports have been 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. Network Time Protocol Version 4

Work continued on the implementation and refinement of the NTP Version 4 distribution for Unix, Windows and VMS. The GNU *autoconfigure* system (not to be confused with the NTP autoconfigure technology), which is the basis supporting the over two dozen ports of the distribution to various architectures and operating systems, continued to evolve as each new bug in each new operating system became exposed. The GNU toolset, including its autoconfigure system, is maintained by volunteer contributor Harlan Stenn at no cost to the Government. His expertise has been invaluable to the success of the porting effort.

The encryption interface in the NTP Version 4 implementation was overhauled to use the cryptographic routines from the RSA Data Security package *rsaref20*. As the result, the native DES routine crafted by many domestic hands has been excised from the distribution. This routine was included in the NTP software intended for domestic distribution, but only in encrypted from in the software intended for distribution to other countries. However, it is well known that drop-in replacements for this routine are available from many places, specifically at sites in Finland and Australia. Use of the rsaref20 package provides arms-length separation of the engineering and political issues, since now only the RSA MD5 routine is included in the distribution and an export-sanitized version is no longer necessary.

In the near future, we expect to incorporate public-key cryptography in the autokey scheme as described previously. Using the rsaref20 package provides a way to do this with minimum effort. To assess the difficulty when extending the autokey scheme to servers and clients outside the US, a routine fishing expedition found that alternate rsaref20-compatible versions of all routines are readily available on the web outside the US.

The design of the cryptographic interface is such that the rsaref20 routines can be simply copied into the distribution and the GNU autoconfigure system does the rest. However, it turns out that the rsaref20 DES routine is endian-sensitive; that is, a Sun client of a Sun server works fine, as does an Alpha client of an Alpha server, but not a Sun client of an Alpha server and vice versa. This is easily fixed by modifying the DES source in rsaref20, but doing this and redistributing the modified source would break the carefully crafted export model. Ordinarily, a bum DES is not a problem, since DES is considered legacy and inadvisable in new configurations.

Progress on the autonomous configuration implementation has been slow since the departure of its implementor Ajit Thyagarajan. Mr. Thyagarajan has not finished his dissertation, which would involve in part fixing the bugs remaining in the implementation. So far, a sufficiently attractive carrot has not been found to persuade him to do that, although hope remains. This work may have to be delayed while other more pressing issues are resolved. Investigation of this issue will continue into the next quarter.

In an effort to explore other ways to connect reference clock signals to NTP primary (stratum 1) servers, drivers were constructed for two signal formats, the Inter-Range Instrumentation Group IRIG-B/E signal and the signal modulation used by the Canadian time/frequency station CHU. Both of these drivers use the standard audio codec and system device driver for the Sun workstation. Experience with prior implementations of DSP demodulator/decoder programs for the Texas Instruments 320C25, reported previously, provided a good basis for this work. Algorithms were implemented in C code for filtering, demodulation and decoding of the IRIG and CHU signals. The algorithms are described in detail, both in the distributions packaged for access via the web and in the documentation included in the NTP Version 4 distribution.

Performance of the IRIG demodulator/decoder is better than expected, given the resolution of the modulation and carrier in this signal format. With extensive signal filtering, conditioning and matched-filter algorithms, the residual errors with an UltraSPARC workstation are in the order of 10-30 microseconds. This performance is bettered only by use of a precision pulse-per-second signal and modified kernel. As it happens, the Sun Microsystems adaptation of the precision-time kernel modifications designed in this laboratory is broken in Solaris 2.6, so the IRIG signal represents the best performance available.

3. Infrastructure

With the kind assistance of the CAIRN Testbed Network Operations Center, we have obtained a Pentium-class machine to replace the aging Sun SPARC DARTnet router. While hardware and FreeBSD operating system are doing fine, we would like to use the IRIG audio driver as the source of synchronization, rather than the more conventional serial port and PPS signal, which requires a gadget box with level converter and pulse reshaper. While work continued on an erratic basis with part-time help, we have not yet found success. Work will continue on this in the coming quarter.

As it happens, out local power utility has spun off another company, Connectiv, which hopes to capture a significant fraction of the communications business in this part of the country. In fact, their Nortel DMS 250 telephone switch is larger than the incumbent DMS 150 used by Bell Atlantic in the same area. One happy result is that they are looking for new markets in the small business community. At the same time, the campus networking unit is looking at ways to increase bandwidth to off-campus faculty, staff and students. This PI stuck his hand up and became one of two beta-test sites to receive T1 service and a Cisco router. The link is now up between campus and our Backroom Test Facility (BTF). The configuration and population of the BTF is described, although not entirely without humor, on the web pages cited previously.

4. Plans for the Next Quarter

Our plans for the next quarter include continued testing and refinement of the NTP Version 4 protocol model, specification and implementation. Specifically, we plan to resolve the problems with the Unix socket interface mentioned in the previous report, so that the NTP autoconfigure feature is really useful. In addition, we plan to continue the collaboration with Coastek InfoSystems in the design and implementation of the cryptographic certification algorithm. The daemon is to be tested first in the research net, then the DARTnet/CAIRN community. As the extensions are backwards compatible, the new features can be activated and tested in regular operation without impacting current users.

5. 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 Proponent. The project descriptions are cross-indexed so that the various interrelationships are clearly evident. 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.