Survivable, Real Time Network Services

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

Quarterly Progress Report
1 July 2000 - 30 September 2000

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 and graduate Tamal Basu. Graduate student Qiong Li has completed his dissertation and been granted the PhD degree. The project continues previous research in network time synchronization technology jointly funded by DARPA and US Navy. 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.

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. Autokey

The main focus of work during the last quarter continued to be the implementation, test and deployment of the Autokey public-key cryptographic authentication scheme in NTP Version 4. The Autokey protocol design is summarized on the web status page and briefing slides at www.eecis.udel.edu/~mills/autokey.htm. These documents have been updated to the current state of the security model and authentication scheme. The latest design, which is documented in a technical report cited in the bibliography at the end of this report, has been submitted as an Internet Draft to the IETF.

As of late May, the Autokey design has been implemented, tested and deployed at selected sites in CAIRN. There were several unanticipated problems in this deployment which were discussed in previous quarterly progress reports. The most recent previous report proposes a protocol redesign which would eliminate most of the security holes identified in the initial rollout. The proposed redesign has been completed and integrated with the NTP daemon. The daemon has been deployed in selected DCnet hosts and in several CAIRN routers. Exhaustive tests with the many mode combinations and keying media options have been completed and some bugs fixed. The key

generator program has been revised to search the machine filestystem environment in order to simplify and eventually to eliminate specific key configuration.

3. Simulation of Large Scale Networks

The following status report is submitted by graduate student Tamal Basu.

As documented in previous status reports, we have developed a network simulator capable of simulating very large networks of the order of 10,000 nodes and 30,000 links. Preliminary experiments show that the simulator is capable of meeting these. Following is a summary report on our progress.

The simulator itself consists of three main parts

1. Random Topology generator
2. Routing Algorithm
3. Simulation Engine

The three components have been implemented and are now being used to carry out experiments for any given network size. There does however remain an issue of the degree of realism in the topology and subsequent simulation being carried out. The issue will be dealt with below.

The routing algorithms which are the heart of the simulator have been chosen to be the most generic possible. The algorithms which were chosen to be implemented include the venerable Bellman Ford (BF) algorithm and the Distance Vector Multicasting Routing Protocol (DVMRP). Either of these algorithms can be selected by a command line switch and, with BF, the simulator provides a split-horizon option.

The simulation engine itself is a discrete event simulator and contains an entity known as the Global Event Queue (GEQ). Discrete events are put on the GEQ to be implemented at the correct time. After the event has been simulated the queue entry is discarded and the wallclock and date are upgraded.

An especially important issue in the design of the simulator is the makeup of the network topology, which is based on random topology generator (RTG) based on the Waxman model. This model is based on a two-dimensional representation of a probabilistic clustering algorithm in which the density of interconnections varies from relatively high for short distances to relatively low for long distanced. In the current design, the RTG is an offline process calculated before the simulation on the topology actually begins. This saves a great deal of time and effort during the simulation, which is of great importance considering the size of the networks in question and the processing time involved in simulating them.

The RTG creates a network based on random topologies, rather than fixed topologies used in commercially available simulators such as OpNET and NS. It generates output to an ASCII file, which is then used by the simulator engine. The case to make here is that, in spite of the fact that a completely random topology generator is used to develop the topology, it still is unable to mirror the real life scenario of networks which are built upon each other. Instead it simply provides a planar network, albeit random, a structure which is rarely found in real networks.

We plan to implement the random topology in a different manner, i.e., to continue to harness the inherent advantages of the Waxman model but at the same time to implement the overall topology using the properties of fractals which are believed to be a better model for real networks. Our initial approach is to use the RTG to generate different networks of varying sizes and stack them one upon the other in various ways. The next step would be to use the RTG to generate several networks of similar size (having different topologies due to the random nature of the process with which they were created) and then use them to populate the rims of circles of increasing diameter stacked upon one another.

A number of issues have to be considered in a realistic implementation, the most important of which is the connections between the networks. A natural approach is to consider a node at one level to be expanded as a network at the next level of abstraction. We believe this would be a useful initial experiment, but experience with real networks suggests this model would have to include some number of backdoor links between the fractal networks, just like today many service providers are connected directly to each other rather than via a default-free routing exchange.

Another focus of the experimentation which is also currently underway is to see how the network reacts to a severe break in the network fabric by splitting the network into two parts and then joining them back again. This is a major issue of interest and a strategy would need to be developed if the topologies were to be used to carry out such experimentation. We propose that the new fractal model will be in place and ready for experimentation by the end of May. This is because significant changes have to be made not only to the RTG itself but separate modules will need to be created in order to address the interconnectivity issues between the different layers of the composite network.

4. Project Management

As the result of an apparent misunderstanding somewhere in the management chain, we were told to close down the project earlier than the end of the second contract year. This caused quite a bump in staff morale and grave concerns about continuing funds for the graduate students. This concern was the reason Mr. Basu left the project to be an intern at Ericsson. We were able to fund Mr. Li until the end of June, at which time he completed and submitted his dissertation.

Subsequently, funding was restored for the current contract year, which ends on 30 September and subsequently one-half the funds originally budgeted for the third (option) year. Originally, we were asked to budget at the original burn rate for six months, which would make it impossible to replace Mr. Li and probably force the remaining graduate student, Mr. Basu, to leave the project. This investigator saw no choice but to rebudget the funds to at least allow Mr. Basu to continue until his graduation in June 2001.

In order to sustain operations through the third contract year, which ends on 30 September 2001, all equipment purchases have been cancelled along with all except local travel. Mr. Li will not be replaced. Something less than a month of summer salary will be available for this investigator to write the final report. The effect on the deliverables and expected research progress is not clear at this time.

5. Infrastructure

NTP with Autokey has been deployed to several CAIRN routers running FreeBSD 3.4 and now in regular operation. Unfortunately, for the reasons mentioned above, the Autokey function itself does not always work properly. Nevertheless, the experience does confirm the autonomous and automatic key refreshment strategies do work properly and the protocol itself is resilient and reliable in the face of node and link fractures.

Progress on a standard application program interface for the pulse-per-second interface for a generic kernel continues with the publication of RFC-2783. The functionality of this document has been implemented for SunOS, Solaris, Alpha, Linux and FreeBSD and confirmed by experiment using local hosts and those CAIRN routers equipped with GPS receivers at ISI-W, SAIC, UDel and UCL.

6. Future Plans

The latest enhancements of the autokey protocol and algorithms provide for a completely automatic generation, transmission, installation and validation of public keys and agreement parameters. However, the ultimate security of the public-key protocols depends on certificate validation. High on the list for future work is rewriting the NTP daemon name resolution code, which has been heavily encrusted with useless stubs and excessively rigid format checking, making new features almost impossible to implement. A complicating factor is that the resolver code is closely bound to the remote configuration code and shares its awkward authentication mechanism (which is a separate scheme quite different from Autokey).

However, the highest priority task right now is fixing the problem mentioned in several previous reports where the Autokey function does not work properly in machines with more than one interface. It was hoped to do this over the summer, but there was a shortage of willing hands that could do this work. Mr. Li was totally distracted finishing up his dissertation, while Mr. Basu was off to Ericsson as a summer intern. This left the hands of this investigator were deep in the Autokey redesign and implementation.

7. 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.

7.1 Papers

1. 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.

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

3. 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.

4. 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.

5. 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.

6. 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.

7. 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.

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

7.2 Technical Reports

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

10. 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.

11. 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.

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

13. 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.

14. 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.

15. 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.

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

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

7.3 Internet Drafts

18. Mills, D.L. Public-Key Cryptography for the Network Time Protocol. Internet Draft draft-ietf-stime-ntpauth-00.txt, University of Delaware, June 2000, 36 pp.

19. 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)

20. 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)