Survivable, Real Time Network Services

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

Final Project Report

Quarterly Progress Report
1 July 2002 - 30 September 2002

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 final project report and 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 report contains 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. The web collection including these works currently has over 17,000 files and over 200 web pages totalling over 500 megabytes and is maintained on a daily basis.

In brief summary, we have passed the following milestones during the quarter. These include

1. IPv6 support for the software distribution for the Network Time Protocol. This includes the Unix/Windows daemon ntpd, as well as various utility programs.

2. Certain changes in the Autokey Version 2 security protocol in order to operate with multiple security domains. A new identity scheme MV has been added to the suite of identity schemes available. The MV scheme operates as a zero-knowledge proof both with respect to the trusted agent and the clients. It also allows individual client keys to be revoked without changing other client keys.

3. The final draft of the Autokey Internet Draft has been submitted to the IETF for approval as a RFC.

4. Continue to tested and verify sample ephemerides with the NTP discrete event simulator in the Interplanetary Internet. These measurements are designed to calibrate the time error due to residual errors in the ephemerides and the polynomial approximation routines.

Occasionally for record, these paper reports will include a more extensive discussion drawing on the work reported on the web. This report includes information about all projects contributing to the combined effort. Funding is from DARPA unless specified otherwise.

2. Autonomous Authentication

The missions considered in this project involve autonomous sensors that might be deployed from a reconnaissance vehicle over a battlefield or from a space probe over a planetary surface. Once deployed, the sensor network must operate autonomously using an ad-hoc wireless infrastructure as sensors are deployed or destroyed or the network is damaged or compromised and then repaired. In the traditional fog of war scenario, sensors may be able to communicate directly only with nearby neighbors and in particular may be able to assess trust only intermittently and not always directly from a trusted source.

The goal of this project is to develop and test security protocols which resist accidental or malicious attacks on the servers and clients in a sensor network. Clients must determine that received messages are authentic; that is, were actually sent by the intended server and not manufactured or modified by an intruder. In addition, they must verify the authenticity of any server using only public information and without requiring external management intervention.

We have developed a security model and protocol called Autokey. It is designed to work with NTP and the Manycast scheme described below to provide completely autonomous cryptographic authentication and identity verification. Autokey version 2 has been implemented in a wide range of machine architectures and operating systems using both IPv4 and IPv6 address families. It has been tested under actual and simulated attack and recovery scenarios. It is documented in detail in a set of web pages and briefings beginning at www.eecis.udel.edu/~mills/autokey.html. These pages include a statement of mission, method of approach, implementation and assessment of results. The software and documentation are provided for public retrieval on the web www.ntp.org. It has been deployed in our research network DCnet, the CAIRN research network and at several sites in the public Internet.

3. Autonomous Configuration

The missions considered in this project funded by DARPA also involve autonomous sensors that might be deployed from a helicopter over a battlefield or from a space probe over a planetary surface. As in Autokey, once deployed, the sensor network must operate autonomously using an ad-hoc wireless infrastructure as sensors are deployed or destroyed or the network is damaged or compromised and then repaired. Appropriate algorithms and protocols must be developed to facilitate automatic, quasi-optimal configuration of sensor applications in response to network damage and repair and without requiring external management intervention.

Our approach involves IP multicasting and distributed, goal-oriented algorithms that survey the current service topology to discover, authenticate and configure a quasi-optimal forest of spanning trees rooted on the primary service providers. We have developed a protocol called Manycast and heuristic algorithms that attempt to minimize a distance metric corresponding to the most accurate time, subject to constraints designed to protect the server and network resources. These algorithms are designed to work in real time with minimal impact on other services that might share the sensor platform.

Manycast has been implemented in a wide range of machine architectures and operating systems using both IPv4 and IPv6 address families. It has been tested under actual and simulated attack and recovery scenarios. It is documented in detail in a set of web pages and briefing slides beginning at www.eecis.udel.edu/~mills/autocfg.html. These pages include a statement of mission, method of approach, implementation and assessment of results. The software and documentation are provided for public retrieval on the web www.ntp.org. It has been deployed in our research network DCnet, the CAIRN research network and at several sites in the public Internet.

Fpr future study, it is likely that some sort of whisper campaign protocol will be necessary in order to balance the load among the available servers. Load leveling can be implemented using an extension field which carries, for example, a list of the current servers mobilized by the Manycast client. A MRU list of recently heard servers is already available in the NTP reference implementation and used for access controls. Manycast servers can use the MRU list and combined extension field lists to compute a decision threshold for each server. Each server compares a random roll to its threshold to determine whether to respond to a client request. Details remain to be worked out.

4. Multivariate Trust Models

The missions considered in this project funded by Army Research Laboratory under a Cooperative Technology Agreement involve autonomous sensors that might be deployed from a helicopter over a battlefield or from a space probe over a planetary surface. While the Autokey protocol requires cryptographic values that are either trusted or untrusted, the goal of this project is to determine from various security related variables maintained in a possibly damaged distributed database the level of trust that can be determined from all the information available. For this purpose the security variables can have either discrete or continuous values reflecting the degree of confidence in some related cryptographic function such as certificate trail authentication or identity verification.

The CTA provided only limited support for this activity and all allocated funds have been depleted. Nevertheless, significant progress was made on defining the model, refining the identity schemes and developing a containment model. Background, approach and initial progress is documented on the web www.eecis.udel.edu/~mills/cta.html and other pages linked from there. Of particular relevance is the multiple-compartment security model developed on the www.eecis.udel.edu/~mills/autokey.html and identity schemes linked from there.

The security model and identity schemes have been implemented in a wide range of machine architectures and operating systems using both IPv4 and IPv6 address families. They have been tested under actual and simulated attack and recovery scenarios. The software and documentation

are provided for public retrieval on the web www.ntp.org. It has been deployed in our research network DCnet, the CAIRN research network and at several sites in the public Internet.

5. Timekeeping in the Interplanetary Internet

There is a long tradition in the planetary science community of controlling experiments entirely from Earth, although there is some progress using semi-autonomous vehicles for Mars surface exploration. Most missions require some kind of clock to determine windows of communication opportunities, for example. During periods where communication with Earth is not possible, there is need to synchronize clocks among the orbiters, base stations and exploration vehicles participating in the mission.

The Interplanetary Internet (IPIN) consists of Earth stations, Mars planetary orbiters, base stations and exploration vehicles participating in a space mission. This project explores synchronization issues in the IPIN using suitable modifications to the Network Time Protocol (NTP). NTP is widely used to synchronize computers in the Earth Internet and has been deployed in low-orbit Earth orbiters, but not in interplanetary missions. There are three issues which distinguish the Earth Internet from the IPIN: bodies are moving, connectivity between them is necessarily not continuous and transmission delays can be very long.

WThe general plan is to evaluate the above approach in detail, especially the impact of ephemerides jitter and oscillator wander. We can simulate the effects of oscillator wander, but the effects of ephemerides jitter will need to be explored in more detail. Our immediate plans are to run experiments with different clock discipline tuning parameters.

Our current progress is documented on the web www.eecis.udel.edu/~mills/ipin.html. The NTP simulator used in the study is available for download at www.ntp.org.

6. 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 over 500 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.

6.1 Papers and Reports

1. Li, Q., and D.L. Mills. Control architecture for tuning intensity and burstiness of traffic. *Proc. 2002 IEEE GLOBECOM 02 Symposium*. Accepted for publication; please do not cite or redistribute.

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

3. Mills, D.L. Public-Key cryptography for the Network Time Protocol. Internet Draft draft-ietf-stime-ntpauth-02.txt, University of Delaware, July 2002, 45 pp.

4. 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

5. 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.

6. 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.

7. 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).

8. 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.

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

10. 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.

11. 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.

12. 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.