THE ISIS PROJECT:
Fault-tolerance in large distributed systems

Final R & D Status Report
Jan 1, 1993

Prof. Kenneth P. Birman
Prof. Keith Marzullo
Department of Computer Science
Cornell University, Ithaca New York
607-255-9199

This work was sponsored by the Defense Advanced Research Projects Agency (DoD), under contract NAG 2-593 issued by the NASA Ames Research Center, Moffett Field, CA.

The view, opinions and findings contained in this report are those of the authors and should not be construed as an official DoD position, policy, or decision.
Personnel

- Academic Staff:
  - Prof. Kenneth P. Birman, Co-Investigator
  - Prof. Keith Marzullo, Co-Investigator
  - Dr. Robert Cooper, Research Associate
  - Dr. Robbert van Renesse, Research Associate
  - Dr. Patrick Stephenson, Post-doctoral Research Associate

- Graduate Students:
  - Lorenzo Alvisi (Marzullo)
  - Navin Budhiraja (Marzullo)
  - Brad Glade (Birman)
  - Guerney Hunt (Birman)
  - Neil Jain (Birman)
  - Michael Kalantar (Birman)
  - Michael Reiter (Birman)
  - Aleta Ricciardi (Birman)
  - Laura Sabel (Marzullo)
The Isis project

This final status report covers activities of the Isis project during the first half of 1992. This is our 8'th progress report under NASA funding, and we assume that the reader has some background regarding the goals and status of our effort, and focus instead on technical accomplishments during the report period and goals for the next six months. Readers unfamiliar with our work could start by reading some of the papers cited below.

During the report period, the Isis effort has achieved a major milestone in its effort to redesign and reimplement the Isis system using Mach and Chorus as target operating system environments. In addition, we completed a number of publications that address issues raised in our prior work; some of these have recently appeared in print, while others are now being considered for publication in a variety of journals and conferences.

With the completion of this milestone, all major goals for the NASA-funded effort have been successfully completed.

The major accomplishments of the final semi-annual report period are:

- We completed the design and prototype implementation of our new "lightweight groups" facility, which will eventually run in Mach or Chorus. This is a major practical advance for the group, which has been working on this problem for the past two years. Although our new system has yet to be integrated with Mach, it does implement the lightweight causal and atomic multicast protocols of our 1991 ACM TOCS paper, support the causal domain model that we introduced recently, and achieves extremely high performance and parallelism even over UNIX. We are extremely encouraged by this development. Predictions of a 10- to 100-fold performance improvement appear to be justified, but until we have this new software running under native Mach it will be difficult to say anything final on the issue.

- We continued work on a new way of presenting Isis groups that will reduce costs by allowing Isis to map multiple application-level process groups to a single Isis process group. The idea here is to amortize membership changes over multiple groups so as to reduce their effective cost. The technique us expected to avoid high overhead in applications that use very large numbers of nearly identical groups.

- Formation of research ties with other laboratories, including the Los
The semi-annual status report covers activities of the ISIS project during the second half of 1989. The project had several independent objectives: (1) At the level of the ISIS Toolkit, ISIS release V2.0 was completed, containing bypass communication protocols. Performance of the system is greatly enhanced by this change, but the initial software release is limited in some respects. (2) The Meta project focused on the definition of the Lomita programming language for specifying rules that monitor sensors for conditions of interest and triggering appropriate reactions.
Alamos Advanced Computing Laboratory (which focuses on supercomputing), Portugal's INESC research laboratory (known for its work on realtime communication), and with Mach-related research efforts at the Open Software Foundation, Carnegie Mellon, and University of Arizona.

- We continued the development and initial implementation of the new security architecture for Isis, reported in the first progress report for 1992. We view this as an extremely important advance, because the previous version of Isis was almost completely trusting of its users. The secure Isis architecture, in contrast, can tolerate arbitrary failures outside an island of physically secure nodes, and supports a highly sophisticated trust, encryption and delegation architecture within an island of secured nodes. Implementation of this architecture is proving to be a cornerstone of our new system, and substantial parts of the code now exist.

- We completed the implementation of a Meta rule manager. This decentralized Isis program can be thought of as a “run-time” environment that dynamically loads Meta rules onto instrumented components as they become active or recover from crashes. The rule manager operates from a description of the instrumented program (much like the schema of an object-oriented database) and allows a user to make simple queries about the status of the instrumented program.

The lack of such a rule manager has been a major stumbling block to the clients of Meta. We are also continuing to expand its function into a full-fledged runtime system. We plan to add support for interactively debugging active Meta rules and to add graphical tools for monitoring the status of the application.

- We are completed the design of a higher-level language for Meta. This has proven to be more difficult than we thought since the differences between what appear to be reasonable semantics of temporal commands are subtle. The new language is being implemented, and will replace a simpler version of Lomita that only supports Meta-style guarded commands and rules for maintaining the membership of aggregates. This compiler produces object files that are read by the rule manager mentioned in the previous item which in turn activates rules on the instrumented application.
The main drawback with the previous, simple version of Lomita is the lack of control flow structures—for example, recovery when some control rule terminates abnormally. Hence, we are extending the function of the Meta shell actuator to allow sensor values to be passed in as environment variables. Combined with a shell command that accesses Meta (also nearing completion), this will allow a programmer to write shell scripts that are invoked by Meta as actuators. Such scripts can both record state for temporal matching and perform complex control functions by using both Unix features and Meta sensors and actuators.

- Almost all of the applications that Meta has been used for outside of Cornell have used the sensor abstractions of Meta much more than the actuator abstractions. We think that part of this is due to the lack of rule support mentioned above, but it is also somewhat due to the lack of a good example that could be distributed with Meta. Hence, we have built such an example application that uses Meta to load balance requests to a set of simulated computation servers. Writing this application has (not unexpectedly) flushed out a set of subtle bugs in Meta and Isis, and so the example application is not ready for distribution at the time this report was written. It currently exhibits simple rules (such as transparent submission to lightly-loaded servers) and we are currently adding more complex control rules (such as dynamic server creation and removal based on average service load).

We are also rewriting the Isis Resource Manager as a Meta client. Again, this has flushed out a set of problems with Meta (most notably, the lack of support for remote Isis and the lack of support of large aggregates). We expect to have the Isis Resource Manager fully functional as a Meta client by the end of 1992.

- We have made substantial progress in a new experimental effort to understand flow control problems on hardware multicast technologies such as ethernet, FDDI and token ring, and are extending our work to include next-generation technologies such as ATM. The goal of this effort is to develop effective flow-control algorithms for use within the Isis multicast protocols. So far, we have focused on collecting data concerning the behavior of the raw devices themselves, and have obtained fascinating and non-intuitive results concerning packet loss rates in a number of settings. These show that the most significant loss rates are for small packets sent in many-one or many-many situations. Low or
zero loss occurs with large packets and for one-many patterns. This information will be used to develop algorithms that narrow in on the situations in which loss rates are highest, while remaining uninvolved in other situations. Such flow control algorithms are the key element limiting Isis performance on many systems, and development of this new flow control software will be a small but critical activity for us during the coming year.

- We have initiated a new project to explore specialized implementations of Isis for the CM/5 and Intel Touchstone multiprocessors. This work is motivated by the impressive results of Berkeley's Split/C and Active Messages research, demonstrating that asynchronous communication can lead to tremendous performance gains on the most important emerging parallel processors. As we move Isis onto these platforms, we want to build our protocols in ways that exploit the hardware fully and minimize unnecessary work in software - work needed on networks but not on closely coupled machines. We are very excited about this new direction.

With this final progress report, it is interesting to observe that Isis seems also at the end of a period of initial transition. The original version of Isis is no longer a subject of active research at Cornell, and the initial version of the Meta system is also finished. With the successful handoff of these systems to ISIS Distributed Systems (and the widespread release of public; source-form distributions), technology transition for this version of ISIS is well established, and Cornell is now free to focus on the development of the next generation of this technology.

Users of the technology include Sematech, Hughes (EOS), GE/Motorola (Iridium), the military (HiperD), the financial community (New York Stock Exchange, World Bank, many banks and brokerages), CERN, Los Alamos, FermiLab, GTE, SouthWestern Bell Telephone, and many other large and small companies, both for commercial and for research purposes. DARPA and NASA, though support for Isis, have created a new technology that is clearly having an enduring impact on the way that distributed systems are developed in the United States and worldwide.
On the research side, Isis and Meta have launched a major wave of activity in the O/S community. Hundreds of papers have been written by dozens of research groups on variations of the Isis approach. The technology can only improve from this type of activity, and there can be no clearer proof that the approach is valid and viable.

The redesign of Isis has been structured around a much simplified core of protocols and system management routines (a sort of "micro-kernel"). This core is flexible enough to support all existing Isis functionality, as well as real-time applications, secure applications, a version of the Isis toolkit optimized for parallel processing environments, and support for object-oriented and modular programming languages, like C++ and ADA. We are building this new software layer so that it can run directly over the Mach and Chorus kernels, while continuing to support a UNIX-level interface similar to our current toolkit interface.

A final comment relates to our continued and enlarging discussions with industry. We are now actively pursuing standardization of the Isis approach to group computing with Unix Systems Laboratories, Unix International, the Open Software Foundation, the Texas Instruments/DARPA OODB project, Electronic Joint Venture, and other standards organizations. This is having significant impact, as demonstrated by the decision of OSF to integrate Isis into OSF 1/AD and the recent announcements by Unix International and USL concerning the key role that reliable process group technologies will play in their future products. We are increasingly joined by industry strategists in recognizing Isis and META as enablers for a whole new generation of highly reliable, large-scale, self-managing distributed software. We believe that DARPA and NASA can point to this emerging trend as a demonstration of the huge impact that government research activities can have on industry, given sufficient time, sufficient investment, and consistently positive results to point to.
Publications

On the following pages, we reproduce a full list of publications by the effort, including some very recent ones as well as earlier work. A good general review of the project is TR 1216, soon to be published by the Communications of the ACM. We are beginning work on a book that will collect the most important papers into a single volume. Where a paper has appeared in a journal, the TR version will often be out of date, since copyright restrictions prevent us from distributing versions of these papers for which copyright has been assigned to the journal. These revisions are often important, so where a journal version is cited, we urge the potential reader to consult the journal itself and not to rely on the older TR copy stated on the list.
PUBLICATIONS LIST

ISIS Activity


PUBLICATIONS LIST Continued


PUBLICATIONS LIST Continued


PUBLICATIONS LIST Continued


META Activity


PUBLICATIONS LIST Continued


ISIS/META Activity


PUBLICATIONS LIST Continued

Other Distributed Systems Activity


PUBLICATIONS LIST Continued


Technical reports marked with a '*' can be copied from ftp.cs.cornell.edu using anonymous, binary ftp. The reports are in the "pub" subdirectory.