

Reliable and Secure Group Communication (RSGC)

D. Agarwal, O. Chevassut, K. Berket, and G. Egles

Lawrence Berkeley National Lab

Summary

Collaborative applications need support for communication among members of dynamic groups and scalability to large numbers of users. The natural alternative to a server-based model is to provide a reliable and secure group communication infrastructure to support a dynamic and scalable peer-to-peer model. This project is developing and implementing the components necessary to provide reliable and secure group communication that scales to the Internet. The InterGroup protocols provide the reliable group communication services. These services include reliable delivery of messages, ordered delivery of messages, and membership. The Secure Group Layer (SGL) provides the secure group communication services including authorization and access control, key exchange, authenticity, integrity and confidentiality.

1. Introduction

With the advent of the grid and the availability of distributed resources, comes the need to provide distributed information sharing, support for replicated servers, and coordination capabilities. Group communication provides a natural mechanism for helping to maintain consistent state among a set of replicated servers or a distributed application. A peer-to-peer model inherently makes these applications easier to design and to operate. Since there are no servers, groups can form ad hoc and there is no setup or scheduling with a centralized authority.

There are two primary components to a reliable and secure group communication (RSGC) system: a reliable group communication protocol and a security layer. This project is completing the research and development required to build both these components. Our goal is to implement and support these capabilities for a select group of application developers, with the long-term goal of integrating these components into the grid infrastructure.

The reliable group communication protocol being developed in this project is called InterGroup. InterGroup provides reliable delivery of application messages, ordered delivery of application messages, and membership services to the application. InterGroup was designed with scalability to the Internet in mind. The key to InterGroup scalability is the separation of the membership into senders and receivers.

The security is provided by the Secure Group Layer (SGL), which provides authorization and access control, session key establishment, authenticity, integrity and confidentiality to the group. SGL is being designed and implemented in this project. It employs the reliability properties provided by an underlying InterGroup system but does not require these properties. The core of SGL is algorithms for distributed key agreement. The agreed key forms the basis for the shared session key once it is established. The cryptographic algorithms used in SGL's key agreement have been developed and proven secure in this project. Algorithms have also been developed to allow use of passwords and public-key

infrastructure to authenticate and to handle incremental changes in the membership.

2. Progress to Date

The current release of the InterGroup protocols consists of two components: a node and a client. The node runs the core of the protocol stack, communicating with the other nodes using IP multicast. The client contains a light-weight protocol stack and the APIs. The node software is available in Java. The client software is available in Java, python, and C++.

Theoretical work on the InterGroup protocols has focused on developing formal specifications of the desired properties of the system and proving that the employed algorithms provide these properties. We are using the I/O automata model to represent the formalisms.

Work on SGL began with development of the required cryptographic algorithms. We studied and developed group Diffie-Hellman key exchange algorithms. We provide a provable-security framework to assess the security of group Diffie-Hellman key exchange protocols. The model captures the capabilities of the adversary and the security definitions. Initially the members of the group come together and use a static group Diffie-Hellman algorithms to agree on a session key. Then the parties run incremental group Diffie-Hellman key exchanges to update the session key after each join, leave, merge and partition event.

We developed formal models to prove the correctness of the group Diffie-Hellman key-exchange primitives for different settings (public-key infrastructure and password-based) and, through a series of papers provided major contributions to the solution of the group Diffie-Hellman key exchange problem.

A prototype implementation of the Secure Group Layer has been completed along with a demonstration chat application.

3. Future Directions

There are still many features of the system that are missing. The reliable multicast algorithms and the models that the current system is based on still need further development. The delivery model and performance need to be investigated and implemented more completely. The group security implementation needs to be formally analyzed as a whole. A robust implementation of the system needs to be completed and the performance of the combined system must be investigated.

One of the features that will need to be added is the security mechanisms for reliable and secure group communication in wide-area environments. Our plan is to enhance and extend the primitives for group Diffie-Hellman key exchange to combine the group Diffie-Hellman key exchange of the sender group with a group key distribution scheme for the receivers. After the senders have established a session key, the control nodes (i.e. sender group) will use a key distribution scheme to disseminate this key to the receiver group. As the new scheme emerges it will also need to be proved secure in the paradigm of the “practice-oriented provable security”.

For further information on this subject contact:

Dr. Deborah Agarwal

Lawrence Berkeley National Lab

1 Cyclotron Rd, MS50B-2239

Berkeley, CA 94720

Phone: 510-486-7078

E-mail: DAAgarwal@lbl.gov

URL: <http://www.dsd.lbl.gov/CIF/GroupComm>