Technical Innovations deployed by the MERCI Project

Peter T. Kirstein <p.kirstein@cs.ucl.ac.uk>

Roy Bennett <r.bennett@cs.ucl.ac.uk>

Abstract

The paper reviews some of the important recent developments within the MERCI project in the technical improvement and deployment of Multimedia conferencing. The developments address four of the known limitations of the Mbone technology heretofore: lack of security, absence of QoS guarantees, inability to interwork with conferences using the ITU-T standards and lack of good access over low bandwidth unicast links. Description of the developments is coupled with a discussion of future improvements and plans for further deployment.

1. Introduction

MERCI (Multimedia European Research Conferencing Integration) is funded by the CEC under the Telematics for Research initiative of the Telematics Application Programme. The objective of the project is to provide all the technology components, other than the data network itself, to allow proper deployment of the tools for multimedia collaboration in Europe. We are pursuing this end by improving the tools and verifying their usability.

The project, now into its second year, has made good progress in the achievement of this objective. MERCI is primarily involved in deploying the multimedia conferencing technology and ensuring that it is both usable and used by the research community in Europe. This paper reviews several technical innovations which have been introduced in pilot operations in Europe to improve usability and describes our plans to improve them and to further deploy them.

2. Piloting of RSVP

A number of the MERCI partners have ongoing pilot activities in the deployment of RSVP [1]. The aim of this work is to improve the quality of MBONE conferencing by providing Quality of Service guarantees to users. The project as a whole will run RSVP on its dedicated European Mbone links over JAMES, extending these within countries as conditions allow. Detailed plans for deployment of RSVP within the project will be finalised early in 1997 and many of the pilot implementations will be running by the time of Networkshop25.

UCL has a stable RSVP implementation on a Cisco which has been running now for some months. At the December 1996 IETF meeting there was agreement to explore the use of resource reservation on CAIRN. Further proposals have been made recently to use RSVP to link specific SuperJANET sites in the near future to facilitate the effective deployment of multicast conferencing; this will be particularly important if the present videoconferencing arrangements for SuperJANET have to be modified.

TUB in Berlin have a version for IPv6 for HP machines and SICS for Sparcstations; these are under evaluation. INRIA will run a pilot network using RSVP with IPv6 starting in the first quarter of 1997. UiO, our partner in Norway, will start national testing with 4 sites in early January 1997 and there are plans to extend this to 10 sites in the spring. Finally, we propose to pilot RSVP over the London MAN.

The project is working to provide an updated user interface to the reservation facility. This may be provided in the tools only, or it may be deployed in a session level controller.

3. Mechanisms for secure conferencing

The whole question of secure conferencing is considered both at the level of the individual component tools and that of the overall conference session.

3.1 Securing the tools

A prerequisite for secure conferencing is the ability to encrypt the streams produced by the multimedia tools. While it might have been possible to do this in a tool-independent way using secure IP (IPSEC) [2], the extent to which this will be implemented in IPv4, and the timescale of the implementation, were too uncertain for our purposes. We have chosen to secure the individual tools; this has the advantages that it can be done using the full infrastructure of the RTP transport protocol and of Multicast.

We have arranged for encryption to be provided for the audio tool RAT, the video tool VIC, the shared text editor NTE and the shared whiteboard WB; we expect to encrypt the new shared whiteboard tool TeleDraw shortly. The media tools themselves require the provision of information specifying the encryption algorithm used, other parameters to describe the encryption and the encryption key. In the only version of this implemented so far for the MERCI tools, the encryption algorithm used is the symmetric single DES [3], and the only parameter needed is the encryption key. In each case, we are using an initiation vector and an encryption key. The developers of the tools have agreed to pass information about the symmetric key in the form of a PassPhrase; this is conformant to [4], which has been agreed in the IETF. This PassPhrase is passed through an MD5 [5] module, to ensure true randomness of the encryption key; the first 56 bits after passing through the module are used as the Encryption Key; this mechanism has been built into the above existing media tools. Because the PassPhrase is 7 bit printable ASCII, as are all the other parameters provided by the tools, it is possible to provide the whole Description Payload as a printable block.

One aspect of security is the interworking of the tools. This has been demonstrated between the secured VAT from LBL and the secured RAT from UCL, and between the secured VIC from LBL and the secured VIC from UCL. There are also secured versions of the shared workspace tools WB and NTE.

3.2 Security at the Session level

3.2.1 Secured SAP

Conference control and security functionality are intricately related, and the SAP, SDP and SIP protocols all include explicit security mechanisms to perform key exchange for multicast sessions [6]. The security requirements and implementations require full papers by themselves; these are being prepared, but are not yet available.

SAP broadcasts information on future sessions; as part of this it provides a full description of the parameters to be used to start the tools in the form of a SDP parameter string. This parameter string includes the provision of encryption keys for each tool. While the Standard envisioned a set of keys for each session, the current implementations allow for only one key for each tool - as described above. SAP allows not only for a Session to be announced, but also for its being modified; sending a new announcement should automatically modify the parameters of a previous announcement. Thus there are two distinct requirements for security:

1. Mechanisms for authenticating modification announcements, to ensure that they are from an authorised source;
2. Mechanisms for allowing announcements of private sessions.

We have implemented the first by constructing a digital signature of the announcement, produced by performing an MD5 sum on the contents of the message and encrypting this with the Private Key of the sender. The message is sent with this signature and the Public Key of the sender. Thus any Session modification request must be issued by someone having the same Public Key as the original organiser of the Session. If an appropriate Public Key Infrastructure exists, it is also possible to authenticate the Originator of the message.

For making the private announcements of the second type, we assume that a group Secret key has been distributed to all the parties who are entitled to participate in the conference. We then adopt the traditional mechanism for secure message transmission. A Message Encryption Key (MEK) is chosen, and a Header, which includes the MEK, is encrypted using the group Public Key. The body part of the announcement, i.e. essentially the SDP string (including its encryption keys for the individual tools, is then encrypted with the MEK. The whole message, including the Public Key used to encrypt the Header, the encrypted Header and the encrypted body part are then sent as the announcement. Thus only persons holding the group Secret Key can decrypt the Header, and thus the announcement.

In both cases, initial implementations use both PGP and X.509 versions of the system [7]. PGP is made available because the PGP software is fairly widely used, and X.509 [8] versions of certificates are used because such an infrastructure is envisaged both in the IETF and the European ICETEL [9] project.

We are still experimenting with different methods of key distribution. We expect to use three methods of key distribution: Secured WWW access, Secured E-mail and Secured X.509 Directory access. Further details are presented in [10].

3.2.2 Secured SIP

In addition to announcing public sessions as a *table of contents*, an alternative mechanism to initiate multimedia sessions follows a telephone style analogy - a user wishes to call another user to start a session immediately. Using SIP, a user may call another user who has SDR running, and invite them to join an existing advertised session or a new private "on-demand" session. The current implementation of SIP in SDR is minimal, but performs well. SIP, however, allows for relays to provide user-location, firewall transition, etc. An alternate proposal, a Simple Conference Invitation Protocol (SCIP) [11], had a partially complementary and partially overlapping functionality. It has been agreed that SCIP will be incorporated into a new version of SIP which will replace the individual activities. A draft of this new version of the SIP protocol was presented to the December IETF meeting [12].

We have gone far in the design of a secured version of SIP. This follows much the same lines as the private announcements, but now the Public Key used is that of the individual being invited to the conference. The invitation will initially be via UDP; however, we also will provide an implementation based on the S-MIME message mechanism. One version of this has been implemented by GMD [13]; their specific implementation makes certain assumptions on the message system used, but a more general version will be developed over the next few months.

The implementation of a secured SIP has been slightly delayed pending the completion of the integration of SCIP into SIP.

4. Mbone over ISDN

4.1 Mbone Relays and Mixers

Multicast routing is not yet ubiquitous, and so there are sites that wish to participate in Mbone sessions but cannot do so. This applies in particular to workstations situated at the end of ISDN lines running IP (usually PPP) over ISDN. Such workstations often do not wish to run full multicast routing, or cannot do so if they are running any Microsoft operating system without a local multicast router, and so an alternative solution is required.

UCL have been working on a set of solutions collectively known as the Umbone (Unicast Mbone). These are components that can be put together to form a relay between the multicast world and a single, multicast-deprived, end-system. Sessions will be initiated using a modified SDR Session Directory, which can obtain a list of available sessions on demand (rather than continuously for a multicast-capable site), and can send a SIP request to initiate the mixing and relaying functionality.

Currently work on the audio mixer has been started, drawing upon experience gained in writing the RAT audio tool. In addition, a video switcher has been developed. This allows the forwarding of specific sets of video packets (as required for the hierarchical coding or for the forwarding of only a small number of video streams). Eventually a queuing module will be needed and a modification of the Session Directory to allow the set-up of these relays.

4.2 ISDN and Low Speed Support

A major effort was undertaken between Hewlett-Packard and UCL to ensure that the ISDN access facilities, using a Primary Rate ISDN Router (with ASCEND hardware [14]), worked well with multiple B-channels. This has now been completed, and n x 64 Kbps channels can be supported. It is possible to run IP over multiple B-channels (between 1 and 30) into the primary rate devices at UCL and HP. KTH and RUS have installed similar equipment, but it has not been used extensively.

It is planned to integrate this into the MERCI system in two ways.

1. Using Mbone routers, with appropriate audio mixing and video filtering, we will facilitate interoperability between Mbone terminals accessing the Internet via the ISDN over a small number of B channels.
2. Using the interoperability gateways of Section 5 below, we expect to interconnect full ITU terminals into Mbone conferences. Both these activities are expected to be operational by the time of Networkshop25.

5. Interworking between ITU and Mbone

5.1 The two standards

Two major families of standards-based videoconferencing systems exist today.

5.1.1 ITU

The ITU developed its H.3xx and T.12x series of recommendations to support multipoint multimedia conferencing - originally for circuit switched networks (H.320, H.324) where transmission bandwidth is guaranteed. In its latest recommendation in this area - H.323 - the ITU also defines how to perform multimedia conferencing on top of packet switched networks. ITU members have developed this recommendation together with IETF members so that IETF protocols are employed by the MBONE Tools as well as by H.323.

The development of these ITU-T recommendations was followed with great interest from the communications- and IT industries. All major vendors which are active in the field of multimedia conferencing have joined IMTC, an industry forum which propagates the usage of these standards, organises interoperability trials, develops implementation guidelines and provides feedback to the ITU. Many of these vendors have already developed products on the basis of these standards. Desktop Multimedia Conferencing (DMC) systems based on the ITU recommendations of the H.3xx / T.12x series were developed in the RACE II project EuroBridge and have been applied in field trials on a European scale in other projects such as AREA, ICARE and others.

5.1.2 MBONE

MBONE videoconferencing tools such as RAT, VIC, SDR and others were designed to operate over packet switched networks. They make use of multicasting to distribute audio and video data streams, are based on IETF standards and are widely used in the academic community. Parts of the development of these tools as well as their application in international field trials was initiated by MICE and is being continued in the MERCI project. A specific focus of the work within MERCI in this context concentrates on security issues (WP 10).

5.2 Interworking

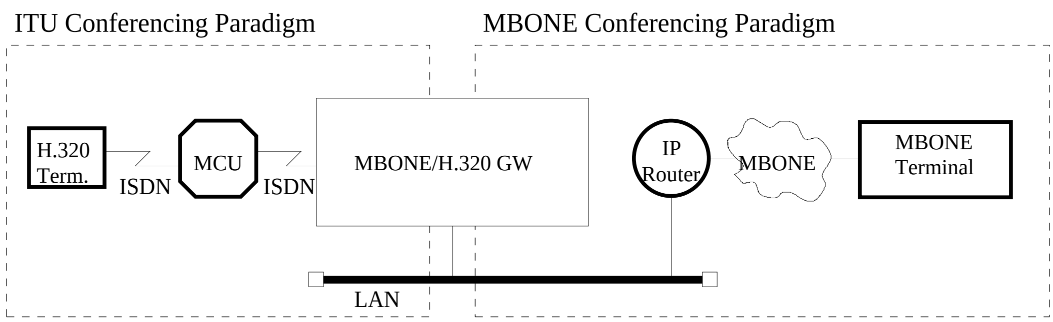
Due to their differing backgrounds and development histories, these DMC systems are currently not compatible although they employ, to some extent, the same communication protocols. There is a major workpackage to develop means which will allow MBONE videoconferencing tools and DMC systems based on the H.3xx / T.12x - series of ITU-T recommendations to interoperate, thus allowing them to enter the same conference. Mechanisms for achieving this have been designed [15], and the first implementation is largely complete.

For a faithful interoperability, the two systems must have the same models; hence interoperability between the ITU tools and tightly coupled Mbone conferences are the most successful. TELES, one of the MERCI partners (represented by TU Berlin and TU Bremen), have been developing the Simple Conference Control Protocol (SCCP) in the IETF. This will provide an IP multicast-based mechanism upon which T.124 semantics can be built. Work on SCCP is less advanced than that on SDP/SAP/SIP; as it started later, running code is not yet publicly available. An SCCP implementation should be available during the second year of MERCI, which will facilitate the participation by Mbone users in the ITU style conferences.

We will not give more details of this work for two reasons:

- It really requires a paper in its own right, and we do not have space here
- We would like experience of the inter-operation before we discuss it in detail.

To give an idea of how TELES is proceeding in this activity, a block diagram is shown below:



Diagrammatic view of ITU-Mbone gateways

Here there may be several such gateways in the system. Moreover, it may well be necessary to put relays like those of Section 4.1 at the MBONE side of such gateways.

The gateway is in two-stages. The first operates between the ITU H.320 and their H.323 system; the latter already uses the same transport protocol (RTP) as the MBONE. The second is a gateway between the ITU and MBONE style of conferencing. A limited functionality should be available with present MBONE workstations; added functionality will be achieved when the tight conference control (SCCP) is deployed.

6. Future plans

Most of the developments described here have only just been completed; thus deployment is planned to continue through the remainder of 1997. The key distribution for security must still be aligned with the emerging IETF standards. The gateway between ITU and MBONE worlds requires the added functionality which will be feasible only with the deployment of SCCP. Finally, there is a continued need to deploy a more consistent and higher performance MBONE; we believe that this will result mainly from the RSVP activity, but intelligent use of ATM may have an important impact.

7. References

[1] Braden, R; Zhang, L; Berson, S; Herzog, S; Jamin, S : "Resource ReSerVation Protocol (RSVP) - Version 1 Functional Specification", draft-ietf-rsvp-spec-14.txt|ps, November 1996

[2] Atkinson, R : "Security architecture for the Internet Protocol", draft-ietf-ipsec-arch-sec-00.txt, June 1996

[3] National Bureau of Standards: "Data Encryption Standard" FIPS 46, Government Printing Office, Washington, 1977.

[4] Schulzrinne, H: "RTP Profile for Audio and Video Conferences with minimal control", RFC1890, January 1996

[5] Rivest, R : "The MD5 Message-Digest Algorithm", RFC 1321, MIT, April 1992.

[6] Handley, M : "SAP: Session Announcement Protocol, draft-ietf-mmusic-sap-00.txt|ps, December 1996

Handley, M; Jacobson, V : "SDP: Session Description Protocol, draft-ietf-mmusic-sdp-02.txt|ps, November 1996.

Handley, M; Schooler, E : "SIP: Session Invitation Protocol", draft-ietf-mmusic-sip-00.ps, June 1996 (original version before consolidation with SCIP).

[7] Handley, M : "Session Description Rendez-vous", URL: ftp://cs.ucl.ac.uk/mice/videoconference/sdr/README

[8] Housley, R; Ford, W; Polk, W; Solo, D: "Internet Public Key Infrastructure Part I: X.509 Certificate and CRL Profile", draft-ietf-pkix-ipki-part1-03.txt, December 1996.

[9] The ICETEL Project : URL: http://www.darmstadt.gmd.de/ice-tel/
[10] Bahr, K; Braun, S; Hinsch, E; Kirstein, P : "Security Architecture for MERCI", MERCI Project deliverable, URL: http://www-mice.cs.ucl.ac.uk/merci/deliverables/d10.1/d10.1.html
[11] Schulzrinne, H : "Simple Conference Invitation Protocol", draft-ietf-mmusic-scip-00.txt, February 1996.
[12] Handley, M; Schulzrinne, H; Schooler, E : "SIP: Session Invitation Protocol", draft-ietf-mmusic-sip-01.txt|ps, December 1996.
[13] Hinsch, E; Jaegemann, A; Wang, L : "Experience with the Secure Conferencing User Agent: A Tool to Provide Secure Conferencing with Mbone Multimedia Conferencing Applications", Proc JENC7, Budapest, May 1996.
[14] URL: http://www1.shore.net/%7Edreaming/ascend-faq/
[15] MERCI Project Annual Review Report 1996, pp 46-52, September 1996 URL: http://www-mice.cs.ucl.ac.uk/merci/reports/ar1.html|rtf

8. Acknowledgements

The MERCI Project (Telematics 1007) is funded by the Commission of the European Community.

9. Biography

Peter Kirstein is Professor and Director of Research in the Department of Computer Science, University College London. He has been active in the areas of computer networks, document systems, multimedia and security for many years. Recently he has been Director of the PASSWORD project on piloting security applications, the MICE project on piloting multimedia conferencing projects and various ARPA-funded network activities. He is currently Director of the European Telematics MERCI project in collaborative multimedia conferencing and is responsible for UCL activity on the ICETEL project in deploying a Public key infrastructure for the European research and development communities.

Roy Bennett spent the academic year 1992/3 in the department of Computer Science at UCL gaining an MSc in Data Communications, Networks and Distributed Systems, after some 25 years in a variety of IT positions in Industry and Commerce. He then joined the Computer Science department as a Research Fellow working on the EMMA project, a major objective of which was to encourage the use of the SuperJANET ATM network for multimedia conferencing. He is currently Project Manager of the MERCI project and heads the MICE-NSC for England.