Recent Activities in the MERCI Conferencing Project

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

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

Abstract

This paper outlines the advances made in the MERCI multimedia conferencing Project during its first year. It describes the improvements made in the basic media tools and highlights the advances made in session control and announcement. Attention has been paid to porting the tools to PCs and to interworking between the Mbone and ITU-T protocol suites. Mechanisms for incorporating security in all the tools, and of deploying secure conferencing, have been implemented. The advances are described both to obtaining higher quality - by better tools and faster networks, and being able to support conferencing over the ISDN. The activities on integrating media servers are mentioned. Finally some of the work on User feedback, user support and applications are described.

I Introduction

Multimedia conferencing using Multicast protocols over the Internet has been in use for some five years. From late 1992 to 1995, the ESPRIT Programme supported the MICE project in piloting multimedia conferencing in Europe, with links to the US. Starting in December 1995, the Research and Technological Development section of the European Commission’s Telematics Programme started a two year project called MERCI to develop the technology further, and deploy it in a number of applications. The partners in the current project are: University College London (Co-ordinating Partner, UK), INRIA (France), GMD, RUS and TELES (Germany), Oslo U (Norway), KTH (Sweden); in addition, Hewlett Packard, Shell Research and UKERNA are sponsoring partners - providing both valuable resources and important User feedback to the project.

Many papers have described the work in MICE [1], [2] - including ones at JENC. The MERCI project has the same basic mission, to develop and deploy the use of multimedia over the Internet; by this we mean video, audio and shared workspace tools for synchronous collaboration. It continues to be concerned with packet use of networks, mainly with IP as the bearer technology. It continues to be focussed heavily on the use of multicast IP. The partners include many of the MICE ones, namely: UCL (Co-ordinating Partner), GMD and RUS (Germany), INRIA (France), KTH (Stockholm) and Oslo U (Norway); UKERNA (UK) is still a sponsoring partner.

In spite of the above, MERCI is quite different in many respects. Many MICE partners are not in MERCI; only TELES (Germany) is a new funded partner. Also Hewlett Packard and Shell Research are now also sponsoring partners. This considerable increase in industrial participation in the project is not merely cosmetic; it reflects a deliberate attempt to ensure that the project is of interest to industry. The MICE project took the initial Mbone tools from LBL, and either extended or replaced some as needed. There were new activities in Servers and Security; we also supported the tools over the European ATM pilot, and showed, somewhat crudely, that they could operate over the ISDN. In MERCI, we have looked more fundamentally at the architecture we are supporting, and have added some key new requirements:

The Mbone tools run not only on UNIX workstations, but also on PCs running Microsoft Operating Systems - as demanded by commercial companies;

Facilities should be provided for interworking between the Mbone tools and those obeying the ITU-T set of recommendations for multimedia conferencing;

Security facilities should be provided in a way that is deployable on a substantial scale;

There should be an emphasis on being able to support higher quality A/V - albeit only over higher speed networks - even if this requires more tool development;

Both workstations and conferences rooms should be supported;

There should be routine support for multi-channel ISDN;

Mechanisms should be provided to support conferences over heterogeneous networks; not all participants should need to receive the same A/V quality;

There should be easy to use Servers that can record conferences, and introduce pre-recorded material into the conferences.

User interfaces and control facilities should be provided, that sessions are easy to set up, and tools are simple to use;

All the Mbone tools we use should operate over current IETF transport layers;

Source versions of tools should be available of each media type, so that we can make the changes implied by some of the above requirements; we develop tools if we are unable to obtain them meeting the above requirements.

A key new aspect of the MERCI project is that the partners established a high degree of credibility in Europe that they were capable of making significant technical advances in their own right. As a result, each partners has significant additional activity, funded mainly from National sources, to augment the funds provided under the MERCI project. Thus, for example, the majority of the work on advanced audio tools from UCL is supported under National funds, as is its equivalence in hierarchical video coding from INRIA, most of that in the applications of remote teaching by the Norwegian partner, the work in high speed networks by the Swedish and RUS partners, that of GMD in security and of TELES in T120 workstations. Thus the total activity greatly exceeds the 1.5 MECU provided by the European Commission.

Here we will discuss the recent developments in several areas: Tool improvements (Section II), Session announcement and control (Section III), Interworking between Mbone and ITU-T workstations (Section IV), Network Support (Section V), Multimedia Servers (Section VI), National Support Centres (Section VII), Multicast measurements (Section VIII), New applications (Section IX), and Conclusions (Section X).

II Tool Improvements

The objective of this activity is to provide high quality multimedia components to meet the conferencing needs of diverse users over a variety of platforms. Work has therefore focused on improving the quality of the components, and on increasing the range of platforms on which they can be run.

II.A. High quality audio

Many studies have shown that the quality of the audio data delivered from a source to its intended destinations is one of the most important factors in the overall quality of a videoconference. Already in MICE, two audio tools were implemented: the Robust Audio Tool (RAT) [3] from UCL and FreePhone [4] from INRIA. While both these tools derived originally from the LBL tool VAT [5], they provided better quality in the event of loss, by carrying a lower quality version of one talkspurt in the packet containing the following one. This allowed repair of a lost packet, at the cost of some extra delay. During the first few months of MERCI, both groups added mechanisms to provide high quality audio; these mechanism include high quality audio coding at the source and delivery of high quality audio even in the face of network congestion.

To provide the higher quality audio coding at the source, both groups have added high frequency sampling (up to CD quality sampling) and higher resolution coding/decoding (16 bit vs. the previous 8 bit coding) to their audio tools [6].

To improve the quality of the audio even in the face of network congestion, we continued the work on rate and loss control. Rate control aims at matching the audio source rate to the capacity available in the network to minimise losses. Loss control aims at reconstructing lost packets at the destination using redundant information sent by the source. Subjective quality tests have shown that these mechanisms provide a huge increase in quality [7]. The two groups have developed a packet format for redundant audio encodings, which is being accepted in the relevant IETF working group for as a Proposed Standard [8]. UCL is currently working on adding support for sound localisation and externalisation.

II.B. High quality video

The most commonly used video tool is the VIC videoconferencing software [9] from LBL. Many recent improvements have been incorporated in the tools over the last few months. There will shortly be a version incorporating a layered DCT scheme; this will allow adaptation of the video quality to the network bandwidth available - and the adaptation need not be made at the source (cf. Section III.D).

INRIA is developing a successor to its IVS videoconferencing tool, called Rendez Vous [10]; this includes two new features, namely a resource scheduler and new coding methods. The scheduler allocates explicitly resources such as CPU power to audio and video processing/transmission/reception, so as to optimise the quality of the data delivered to the end user. The scheduler is expected to provide better quality to the end user by allowing resources such as CPU power to be allocated in a flexible way to a specific audio and/or video stream. The new coding schemes will include both the layered coding being introduced by the new version of VIC, and Wavelet coding. The latter is expected to provide better video quality for low bit rates and better robustness to loss. Rendez Vous will be released early in 1997.

II.C. Stream Synchronisation

User experiments have shown [11] that for many applications it is essential for a perceived higher quality of A/V interaction to have synchronisation between the audio and the video. In the ITU methods of carrying the A/V information, this is achieved by interleaving the audio and video information at the transport level. In the Mbone environment, the information is carried in separate streams. For this reason, UCL has developed a method to achieve inter-stream synchronisation. Time-stamp information in RTP packets is used to co-ordinate the audio and video presentation on receiving hosts to achieve lip synchronisation; RAT is used for audio, and a modified version of VIC with play-out adaptation for video presentation. Co-ordination information is exchanged between the two tools using a local conference bus [12].

II.D. Shared workspace

We are still using the wb [13] from LBL. It is not ideal for MERCI purposes for two reasons:

- We do not have source; this makes it more difficult to insert encryption, to link it with ITU-T based shared workspace tools, and to enhance it with improvements needed by some applications;
- It does not run on PCs under Microsoft operating systems.

One alternative, the UCL shared text editor, Network Text Editor (NTE) [14] is now a rugged tool. RUS has made the first delivery of a Java-based (and, thus, easily portable) shared whiteboard application called TeleDraw [15]. Both of these tools require reliable multicast transport protocols. NTE has incorporated a version of Scaleable Reliable Multicast (SRM) [16]. INRIA has started work on implementing SRM over the Real Time Transport Protocol (RTP), developed in the IETF for multimedia applications and used in the other Mbone tools.

II.E. Porting activities

At the start of the MERCI project, RAT was running on UNIX workstations from Sun and Silicon Graphics only. UCL has ported RAT and NTE to many systems including HP workstations and multimedia PCs running Windows 95 and Windows NT. Free-Phone is running on Sun UNIX workstations, with ports to Silicon Graphics and UNIX-based PCs underway; ports to Windows-based PCs are planned for next year. VIC has been ported to many systems, including all the above. Because it is written in JAVA, TeleDraw should move over easily to PCs running MicroSoft operating systems

Although most of the tools now work on PCs, we have found these very sensitive to the exact configuration. There are many multimedia cards for PCs, and their software is programmed to many different APIs. We have concentrated to the Windows APIs for both the audio and video; this reduces the range of peripheral cards supported at present.

II.F. Securing the MBONE tools

The whole question of secure conferencing is considered further in Section 3.5; a prerequisite 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) [17], the extent to which it 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 [18], 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 [19], which has been agreed in the IETF. This PassPhrase is passed through an MD5 [20] 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 7bit printable ASCII, as are all the other parameters provided by the tools, it is possible to provide the whole Directory Payload, as in Section 3.1 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.

II.G. Availability

The tools developed in the project are made available on the Internet. Furthermore, specific Web pages describing the audio tools and ongoing work on high quality audio have been set up at [21] A Web page describing the Rendez Vous video tool has been set up at [10].

III. Session Announcement, Control and Start-up of Mbone Tools

The work done in this area falls under several headings: lightweight sessions, tightly coupled sessions, local session control, relays and mixers, and security.

III.A. Lightweight Sessions

For a lightweight session, no explicit session control or membership control is required, but a rendezvous mechanism is required to communicate information about the existence of a session to its potential participants. To this end, the Session Description Protocol (SDP) [22] and Session Announcement Protocol (SAP) [23] were devised by UCL and LBL, originally by the MICE project, and have continued to evolve and be revised by the MERCI project. These protocols are implemented in the UCL Session Directory tool SDR. At the start of the MERCI project, Mbone conferences were being announced by an early session directory tool, SD [24], from Lawrence Berkeley Labs (LBL). SD had limited functionality, and a number of problems including an inability to announce RTP based sessions. SDR solved these problems, and has become used ubiquitously by the Mbone community. In fact it has been so successful that compatible tools have started to emerge. SDP and SIP are currently Internet-drafts, and will be progressed to IETF "Proposed Standard" status during the second year of MERCI.

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 Programme (SCIP) [25] that has a partially complementary and partially overlapping functionality. It has been agreed that SCIP and SIP will be combined and will replace the individual activities. A draft of this new protocol was presented to the December IETF meeting, and is expected to be completed early in 1997.

III.B. Tightly Coupled Sessions

Another requirement in multimedia conferencing is for tightly coupled conferences. This is the style expected in the ITU-T series of recommendations. TELES, one of the MERCI partners (represented by TU Berlin and TU Bremen), has been developing the Simple Conference Control Protocol (SCCP) [26] in the IETF, which 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, but an SCCP implementation should be available during the second year of MERCI.

III.C. Local Session Control

Both the LBL Mbone conferencing tools (VIC and VAT) and the UCL audio tool (RAT) support inter-tool local communication using a multicast-based local conference bus. Currently no standard is available for such a local bus. Although UCL presented a proposal for this at the IETF, the IETF MMUSIC session control working group has decided that such local protocols fall into the category of APIs rather than network protocol and thus do not fall under the auspices of the IETF. However, LBL has agreed with UCL to work towards standardising this interface mechanism outside of the IETF; this work should be completed in the second year of MERCI.

III.D. 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; thus an alternative solution is required.

UCL has 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 of Section 2.2, for example, or for the forwarding of only a small number of video streams). Eventually there will also be needs for a queuing module and a modification of the Session Directory to set up these relays.

III.E. Security

III.E.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 [27]. 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 indicated in Section 2.6. 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:

a) Mechanisms for authenticating modification announcements, to ensure that they are from an authorised source;

b) Mechanisms for allowing announcements of private sessions.

We have implemented (a) by constructing a digital signature of the announcement by performing an MD5 sum on the contents of the message, and sending this, encrypted with the Private Key of the sender, and the Public Key of the sender, with the message. Thus any Session modification request must be issued with 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 (b), 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 a system [27]; PGP [28] is made available because the PGP software is fairly widely used, and X.509 versions of certificates are used [29] because such an infrastructure is envisaged both in the IETF and the European ICETEL [30] project. The PGP version of the code has been distributed; the X.509 one is still being developed.

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 [31].

II.E.2. Secured SIP

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 think that there is a place for message-based implementations. One version of this has been implemented by GMD [32]; 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 is being slightly delayed pending the completion of the integration of SIP and SKCP mentioned in Section III.A.

The second revision of the SCCP document will also incorporate security, but no details are yet available.

IV. Interworking between Mbone Tools and ITU ones

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

- The ITU developed its H.3xx and T.12x series of recommendations to support multipoint multimedia conferencing - originally for circuit switched networks where transmission bandwidth is guaranteed. In its latest recommendation in this area, H.323 [33], 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.

- 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. One specific focus of the work within MERCI in this context concentrates on security issues.

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 inter-operate, thus allowing them to enter the same conference. Mechanisms for achieving this have been designed [34], and the first implementation is largely complete. For a faithful interoperability, it is necessary that the two systems have the same models; hence interoperability between the ITU tools and the tightly coupled conferences of Section III.B are the most successful.

We will not give 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:

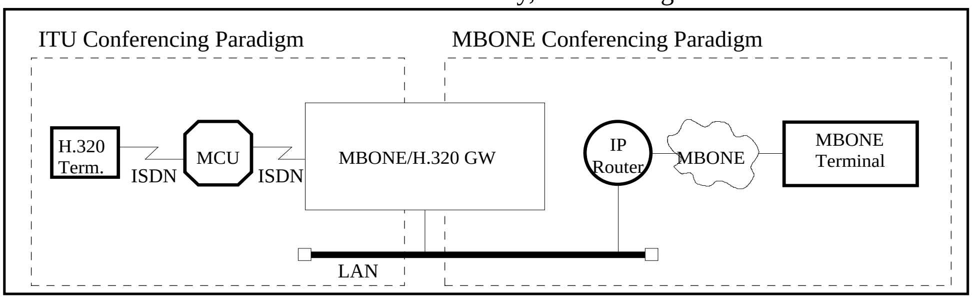

Fig. 1: Diagrammatic view of ITU-Mbone gateways

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

The implementation of the gateway is well advanced, and should be deployed during the first quarter of 1997. Initially the gateway is being implemented in two distinct components in series; one gateways between H.320 and H.323; the other between H.323 and Mbone styles of working. We should be able to give some more details at the time of the JENC conference.

V. Different Networks

Fundamental to successful operation of multimedia conferencing is an adequate network infrastructure. We operate the MERCI suite over the normal Internet, but intend to support two additional types of network: High speed ATM networks and low speed ISDN. The first is in our desire to achieve high quality where it is available; the second is allow broad coverage - even where normal Internet access is inadequate.

V.A. Higher Speed Working

V.A.1. Network Connectivity

The move to the use of higher speed networks was delayed by coming into force of the TEN'34 and JAMES contracts. However, we have now set up a minimal set of connections, which are adequate for our current work. The connectivity is indicated in Fig. 2.

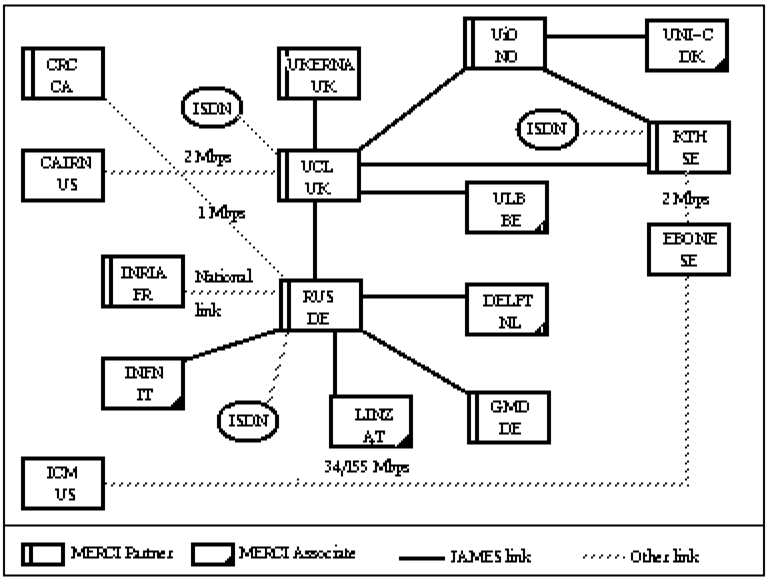

Figure 2: Schematic of current MERCI connectivity using the JAMES Network

In addition to the normal MERCI partners, there are several others either planned or operational. CRC is the Canadian Research Centre; it has been associated with the project since its beginning, but at the time of writing is not yet officially a member. At present most of the international JAMES links shown have 1 Mbps links on a continual basis, though some are at higher speeds; the National links are usually at higher speeds. Figure 2 also shows a set of other centres with planned connection. These are the MERCI National Support Centres (cf. Section VII), who are scheduled for connection during the first half of 1997. One of the connections shown, between UCL and CAIRN in the US, is of a different nature, and is discussed in Section V.A.2.

V.A.2. Resource Reservation

An important aspect of attaining good quality multimedia, is the assurance of adequate bandwidth for specific streams. One way of achieving this is to reserve bandwidth for specific conferences - or at least to provide higher priority for The MERCI project is setting up an RSVP pilot between

UCL is part of the DARPA-supported CAIRN project which is working with Resource Reservation [35] and IPv6 [36]. Because of the importance of both technologies in the future of Mbone services, and the need for transatlantic compatibility, UCL is associating its MERCI work with its CAIRN one in this area.

V.A.3. Measurements and Monitoring

INRIA has started a new round of measurements to characterise the delay and loss processes of audio packets over the Mbone. The goal is to come up with better characterisations and models than are available today, so as to design better play-out adjustment algorithms, and rate and error control mechanisms (cf. Section II.A).

V.B. 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 [37]), worked well with multiple B-channels [38]. 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. Using the Mbone routers of Section III.D, 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. Secondly, using the interoperability gateways of Section IV, we expect to interconnect full ITU terminals into Mbone conferences. Both these activities are expected to be operational by the time of JENC-8.

VI. Multimedia Server

Again the provision of a multimedia server is considered vital to the project. This should have the capability to record sessions, and to introduce material previously recorded. Early versions of such servers were created at UCL during the MICE project [2], and also at many other sites including UC Berkeley [39]. The UCL tool, called VCR, is discussed in detail elsewhere [2]; it currently has a basic, but robust, functionality; many extensions are still required, however. It can participate in a conference - but it must be started manually; eventually this initiation will be via SIP. Currently all operations are local; Standards for remote operations are being developed in the IETF [40], which will be adopted.

The architecture of VCR allows for annotation and indexing of each media stream; it allows also for synchronisation between streams. In addition, we envisage an index of the stored material, which can be searched in a sophisticated manner, and tools for editing stored material. All these extensions are still for the future.

The considerations for secure operation of the Server are complex. There is no problem in storing encrypted media streams, though it would be necessary also to store the encryption keys used. We need to consider carefully, however, mechanisms of access control and key management for accessing the data stored.

VII. User Interactions

An assessment of currently existing guidelines has been completed to determine which of these are applicable and relevant to MERCI. Having surveyed existing literature on usability and assessment of multimedia conferencing systems, a framework for usability evaluation has been developed. A number of evaluation methods have been selected for further development on the basis of this literature survey and an informal survey on emerging methods at the partner sites. MERCI evaluation will begin with qualitative methods (observation, interviews, open questionnaires) and then use this material to formulate quantitative assessment methods via system logging, closed questionnaires etc.

Work has now been completed on Laboratory experiments evaluating redundancy and audio-visual synchronisation - mainly under the aegis of other projects [7], [11]. A list has been established of trials to be completed with an associated timetable. A schedule of user trials has been drawn up, and some user trials are currently in progress. We aim to produce a modular MERCI questionnaire, consisting of a general part, to be completed by participants in all conferences, and then a number of specific question modules which can be applied depending on user group, application, stage of trial etc. This will be a partner-wide effort, co-ordinated from UCL. Both users directly from the MERCI project, and from other projects using the MERCI tools will be included.

VIII. National Support Centres

During the MICE project, a number of centres were set up in different countries to assist users nationally; these centres were the first line of defence if the users have problems. It was assumed in MICE, and this has carried over to MERCI, that at least one of the partners in each country in MERCI will act as such a National Support Centre. Thus INRIA (France), KTH (Sweden) Oslo U (Norway), RUS (Germany) and UCL (UK) have taken on this role. In the UK, Scotland, Northern Ireland and Wales have all had such centres set up. Otherwise Linz U (Austria), INFN (Italy), Delft U (Netherlands), INESC (Portugal) have all set up such centres.

IX. Multicast Measurements

In the course of the several of the activities described in this paper, it has been necessary to do extensive traffic measurements. It is now routine that packet loss is measured at each site during a MERCI seminar (see Section VIII); this allows congestion and error conditions to pin-pointed accurately. We have instituted an extensive measurement activity around many of our uses of the different networks of Section III. With the ISDN, this has been essential to identify traffic forwarding limitations in the routers as the number of ISDN channels have been increased; this has led to changes being required in buffering strategies in the gatewaying equipment. In the SMDS activity, the measurements have identified some rather weird behaviour - like a traffic capacity of 2 Mbps in one direction and only 1 Mbps in the reverse; again allowing the identification of problems in intervening nodes. In the ATM case, this style of measurement has identified the lack of traffic shaping by I/f cards, or inability of switches to deal well with both CBR and VBR traffic.

The measurements have been invaluable in deciding how to route traffic. The results are often not obvious intuitively. For example, a CISCO router has better traffic shaping characteristics than some of our ATM switches; we can obtain better traffic shaping by merely going into, and then again back out of, such a router from one of our ATM switches to another than going through the switch alone.

As part of the design of the VCR of Section VII, there has been extensive measurement of the actual traffic characteristics of the multimedia tools themselves. Ideally, all traffic would be presented to the network at regular intervals, such that there would be a constant inter-packet gap. Our measurements show that some tools present packets with varying inter-packet gaps together with bursts of back-back packets. When this traffic is introduced to switches with their own buffering problems, one introduces delay, jitter and traffic loss. With many of the tools, we can only inform the tool developers, and suggest that the traffic forwarding be modified. With the VCR, however, while these characteristics cannot be eliminated in playout, they can be magnified by certain playout strategies. Again another set of measurements are designed to see what is really occurring.

X. New Applications

From the beginning, it was intended to carry out substantial user trials in the project. MERCI is demonstrating that adequate technology is available, and high quality advice can be brought to bear by applying the technology to three important applications: a Distance Learning seminar series, workshops in experimental surgery, and trials trials under commercial conditions. In each case the applications require audio, video and shared workspace.

The seminar series requires rugged regular use of the technology to a wide number of sites; the demands on the video and audio is high but not too stringent; there is a need to distribute slide and OHP material as part of the seminars. The capability for the tools to be put together in interesting and innovative ways has been demonstrated by the interface developed by the ReLaTe project for language teaching [41]. We maintain our interest in and support of the development of such interfaces for new educational uses. The newer higher quality tools provided by MERCI will enable the Surgery Workshop to satisfy the tighter demands on the quality of the video; the catheters used are often extremely narrow, and the detail is of interest to surgeons. In these uses of conferencing, the introduction of multimedia servers allows an important improvement to the quality of the seminars as educational experiences. The access to high bandwidths also improves quality. The availability of a secure conferencing environment to be provided by MERCI will ensure the confidentiality of the procedures to be multicast and thus an approved audience. This is vital for many reasons - of which patient protection is an important one.

XI. Conclusions

We have described how we have been reviewing many aspects of multimedia conferencing under the auspices of the MERCI project. The software suites developed include many modules developed under complementary projects in which the partners are involved; the whole is much more powerful than the system available at the start of the project. The advances in the media tools, allow for higher quality, better incorporation of heterogeneous networks, use of the PCs popular in industry, and the deployment of security. The announcement and control augmentation allows a much broader set of conferences to be set up with relative ease; this area has been found pivotal in the development of the technology.

Mechanisms for interworking between the Mbone and the ITU-T world have finally been defined and partially implemented; this should turn out to be of very considerable importance. We have extended our support at the high end to ATM networks - albeit only using IP - and at the low end to ISDN in a much more powerful way than hitherto. The methods of introducing Servers has been revised, and a reliable set of recording and playback tools have been introduced.

Feed back from user groups have been used to revise some of the HCI interfaces; nevertheless, they indicate that much more work needs to be done in this area. The work on applications and user support has been mentioned; clearly they are both vital.

This paper has not tried to provide details of what has been achieved in the first year of the MERCI project; it provides a Road Map on the areas that have been tackled, and provides references to the activities themselves.

XII. Acknowledgements

The work described here is due to many of the people who have been working on the MERCI project. While the list below is not complete, special acknowledgement must be made to the following: John Bolot (INRIA), Peter Feil and Andreas Roszek (RUS), Elfriede Hinsch (GMD), Stefan Braun (TELES), Joerg Ott (TUB), John Andrews, Mark Handley, Vicky Hardman, Isidor Kouvelas, Lambros Lambrinos, Colin Perkins, Angela Sasse and Jin Yang (UCL). It is their work which is really summarised here.

We acknowledge the support given by the European Commission under the Telematics Project RE1007. In addition, Hewlett Packard, one of the sponsoring partners, has made available a

substantial amount of equipment, and the OpenView network management facilities to the academic partners. The paper also describes contribution made to the MERCI project from other research projects too numerous to name.

XIII. References

[1] Handley, M; Kirstein P T; Sasse, M A : “Multimedia Integrated Conferencing for European Researchers, (MICE): Piloting Activities and the Conferencing Management and Multiplexing Centre”, *Comp. Netw. and ISDN Sys*, 26, 275-290 (1993). Also published in Proc. 4th JENC, 18-31 (1993).

[2] Kirstein, P T; Handley, M J; Sasse, M A; Clayman, S : “Recent Activities in the MICE Conferencing Project”, *Proc. INET’95*, 445-453, the Internet Society, Washington, 1995.

[3] Hardman V J et al : Robust Audio Tool (RAT) http://www-mice.cs.ucl.ac.uk/mice/rat/

[4] Vega-García, A et al : FreePhone audio tool, INRIA, Sophia Antipolis, France, part of MERCI project deliverable D1, August 1996. http://zenon.inria.fr/rodeo/fphone/

[5] Jacobson, V : Visual Audio Tool (VAT), manual pages, Lawrence Berkeley Labs (LBL), February, 1993.

[6] Hardman V J; Iken M : “Enhanced Reality Audio in Interactive Networked Environments”, Proc Framework for Interactive Virtual Environments (FIVE) conference, Pisa, Italy, December 1996.

[7] Watson, A; Sasse, M A : “Evaluating Audio and Video Quality in Low-Cost Multimedia Conferencing Systems”. Interacting with Computers, Vol. 8 (3), pp. 255-275, 1996

[8] Perkins, C et al. : “Payload Format Issues for Redundant Encodings in RTP”, Internet draft draft-perkins-rtp-redundancy-01.{txt,ps}, July 1996.

[9] McCanne, S; Jacobson, V : “*vic*: a flexible framework for packet video”, Proc. ACM Multimedia’95, 1995.

[10] Lyonnet, F : Rendez Vous video tool, INRIA, Sophia Antipolis, France, part of MERCI project deliverable D1, August 1996. http://www.inria.fr/rodeo/rendez_vous/

[11] Watson, A; Sasse, M A : “Assessing the Usability and Effectiveness of a Remote Language Teaching System”. Presentation at ED-MEDIA 96 Conference in Boston, Mass, June 1996.

[12] Kouvelas, I; Hardman V J; Watson, A : "Lip Synchronisation for use over the Internet: Analysis and Implementation", Proc IEEE Globecom'96, London, November 1996.

[13] Jacobson, V : Whiteboard (WB), README file, Lawrence Berkeley Labs (LBL), August, 1993.

[14] Handley, M J : Network Text Editor (NTE), manual pages, University College London (UCL), 1995. ftp://cs.ucl.ac.uk/mice/videoconference/nte/

[15] Rozek, A : TeleDraw, a platform-independent multicast-capable shared whiteboard application, Stuttgart University Computer Center (RUS), 1997. http://www.uni-stuttgart.de/Rus/Projekte/MERCI/MERCI/TeleDraw/Info.html

[16] Floyd, S; Jacobson, V; McCanne, S; Liu, C-G; Zhang,L : “A Reliable Multicast Framework for Lightweight Sessions and Application Level Framing”, Proc ACM SIGCOMM 1995.

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

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

[19] Handley, M J : "Session Description Rendez-vous", README file, University College London (UCL), 1996. ftp://cs.ucl.ac.uk/mice/videoconference/sdr/

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

[21] The RAT (Robust-Audio Tool) Home Page http://www-mice.cs.ucl.ac.uk/mice/rat/

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

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

[24] Jacobson, V : Session Directory (SD), README file, Lawrence Berkeley Labs (LBL), March, 1993.

[25] Schulzrinne, H : "Simple Conference Invitation Protocol", draft-ietf-mmusic-scip-00.txt, February 1996.

[26] Bormann, C; Ott, J; Reichert, C : "Simple Conference Control Protocol", draft-ietf-mmusic-sccp-00.txt, June 1996.

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

[28] Atkins, D; Stallings, W; Zimmermann, P : “PGP Message Exchange Formats”, RFC 1991, August 1996

[29] 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.

[30] The ICETEL Project : http://www.darmstadt.gmd.de/ice-tel/

[31] Bahr, K; Braun, S; Hinsch, E; Kirstein, P T : “Security Architecture for MERCI”, MERCI project deliverable D10.1, August 1996.

[32] Hinsch, E; Jaegemann, A; Roper I C; Wang, L : "The Secure Conferencing User Agent: A Tool to Provide Secure Conferencing with Mbone Multimedia Conferencing Applications", Proc IDMS’96, Berlin, March 1996.

[33] Draft ITU-T Recommendation H.323: Visual Telephone Systems and Terminal Equipment for Local Area Networks which provide a Non-Guaranteed Quality of Service, May 1996.

[34] MERCI Project Annual Review Report 1996, pp 46-52, September 1996 http://www-mice.cs.ucl.ac.uk/merci/reports/ ar1.html

[35] 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

[36] Deering, S; Hinden, R : “Internet Protocol, Version 6 (IPv6) Specification”, draft-ietf-ipngwg-ipv6-spec-02.txt, June 1995.

[37] Ascend FAQ http://www1.shore.net/%7Edreaming/ascend-faq/

[38] MERCI Project Annual Review Report 1996, page 19, September 1996 http://www-mice.cs.ucl.ac.uk/merci/reports/ ar1.html

[39] Rowe, L; Smith, B C : “A Continuous Media Player”, Computer Science Division, University of California Berkeley, 1992

[40] Rao, A; Lanphier, R : “Real Time Streaming Protocol (RTSP)”, draft-ietf-mmusic-rtsp-00.txt, November 1996.

[41] Buckett, J; Campbell, I; Watson, T; Sasse M A; Hardman, V J; Watson, A : ReLaTe: Remote Language Teaching over SuperJANET, Proc. NetWorkshop23, pp 209-214, March 1995.

Author Information

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 National Support Centre for England.