Journal of High Speed Networks 13 (2004) 207–222
IOS Press

A practice of a collaborative multipoint medical teleconsultation system on broadband network

Chien-Cheng Lee [a], Pau-Choo Chung [b], Dyi-Rong Duh [c], Yunghsiang S. Han [d] and Chi-Wei Lin [e]

[a] *Department of Communications Engineering, Yuan Ze University, Chungli, Taoyuan 320, Taiwan, ROC*
Fax: +886 3 4554264; E-mail: cclee@saturn.yzu.edu.tw

[b] *Department of Electrical Engineering, National Cheng Kung University, Tainan 70101, Taiwan, ROC*
Fax: +886 6 2345482; E-mail: pcchung@eembox.ncku.edu.tw

[c] *Department of Computer Science and Information Engineering, National Chi Nan University, #1 University Rd. Puli, Nantou Hsien 545, Taiwan, ROC*
E-mail: drduh@csie.ncnu.edu.tw

[d] *Graduate Institute of Communication Engineering, National Taipei University, #151, University Rd, Sanshia, Taipei County, Taiwan, ROC*
E-mail: yshan@mail.ntpu.edu.tw

[e] *Via Technology Company, Shinchu City, Taiwan, ROC*

Abstract. The paper presents and discusses a collaborative teleconsultation system built on next generation network (NGN) transmission considerations. Considering the capability of merging medical images with multimedia data and real-time video conferencing in transmission provided by NGN networks, the system is built with computer-supported cooperative work (CSCW), DICOM standard, security functions, and image processing/analysis tools. The built-in CSCW creates a collaborative consultation environment for synchronous interactive face-to-face discussion. The security functions provide the privacy and integrity in patient data transmission. The DICOM standard enables the medical image access to the PACS connecting with various imaging modalities. The image processing/analysis tools supported by CSCW functions provide useful tools for physicians to examine the images, and short-code messages are defined to transmit the image operation command for maintaining the system consistency between users. These functions are discussed and tested on the NGN network transmission for its characteristics including transmission latency, jitter, data loss rate, and multicast performance. The experiments show that adopting the short-code message drastically reduces the bandwidth requirement and also the user waiting time, under which the basic bandwidth requirement of the system during consultation is about 160 Kbps. The security functions occupy 92 ms and 83 ms for encryption and decryption, respectively, for a 518-Kbytes image file. The multicast transmission technology is adopted to avoid the increase of network traffic when the number of participants expands. The experiments also show that the use of tunneling slightly increases overhead; however, the system can be deployed on the network without supporting IP multicasting via tunneling.

Keywords: Computer-supported cooperative work (CSCW), next generation network (NGN), Digital Imaging and Communications in Medicine (DICOM), security, multicasting, telemedicine

1. Introduction

Next Generation Network (NGN) brings packet-based convergence to the communication environment, allowing voice, video, and data to come together through a single unified broadband network. Driven by the evolving technologies and the enhanced functionality of unifying disparate networks, the NGN makes network communication dramatically more efficient, convenient, and cost-effective in many aspects.

In the last few years, there are many researchers dedicated to developing the telemedicine systems for providing remote healthcare delivery [1–14]. However, the traditional transmission technologies limit the systems functionality like only point-to-point service [2,3], different network infrastructures needed [2,6], poor computer-supported cooperative work (CSCW) supported [4,7,8], and absence of security policy [2,4,5]. The point-to-point architecture limits the number of participants, and therefore hinders its applicability to requiring multiple points connection such as multipoint consultation and tele-education. On the other hand, some systems need different network infrastructures for transmitting different data including voice, video, medical images, and patient data. This means that it needs more facilities and cost to deploy the system, and these may become a major problem for hospitals using the system, which limits the feasibility of the system. As a computer-supported cooperative work (CSCW) module including shared workspace and conferencing system is also prerequisite for providing a cooperative discussion environment for physicians, the existing systems often use the off-the-shelf CSCW solutions (e.g., NetMeeting) to provide the cooperative work. This approach again limits the number of persons joining to conference. Furthermore, the off-the-shelf software usually uses application-share for shared workspace. This enforces the clients to unselectively execute exactly the same function. On one hand, this is impractical in telemedicine system since some functions such as file retrieval should be executed only on one site. On the other hand, this could also cause security issue when one client is accessing patient records from its associated patient information center. Most of the off-the-shelf CSCW software transmits the image of the entire application window to maintain the shared workspace. The bandwidth required is large and depends on the number of the participants and the image resolution of the application Windows. This manner also causes the clients lose the option of adjusting its window to the most preferable size. In addition, the off-the-shelf CSCW software also brings a drawback of the inflexibly bandwidth allocation from the build-in video conferencing system because it is designed for general purpose, the bandwidth allocation is fixed in spite of the priorities of the transmission of application data. This drawback causes the inefficiency of bandwidth and a poor quality of service (QoS), especially in the transmission of the mass quantity of application data (i.e., image data retrieval).

In this paper, we take the advantage of the NGN potential for converging voice, video, and data into a single unified system on a broadband network, and present a bandwidth-effective, low-cost multipoint telemedicine system with computer-supported cooperative work, Digital Imaging and Communications in Medicine (DICOM) based medical image retrieval and processing, data confidentiality and integrity. A relaxed "what you see is what I see" WYSIWIS shared workspace model based on the short command message transmission is built in to provide the cooperative function. All the command execution in the system is encoded to a short code and dispatched into the client sites for execution. One common confronted problem associated with using command execution approach is the "command race" confliction which arises when more than two users try to perform commands in the same time, resulting in that the final result of each client depends upon the order of the command received which cause user confusion and the inconsistent status of the consultation. To solve the "command race" confliction, a message coordination mechanism is employed which uses a waiting-reply queue combined with command-finished signals to maintain the operation consistency. With this approach, all participants can be maintained with a consistent shared workspace through these short-encoded messages transmission. In order to enhance the efficiency of bandwidth and quality of service, different kinds of the application data such as command message, cursor message, images, shape annotation, voice, and video are assigned a different priority, respectively. The bandwidth is dynamically allocated depending on the priority of the transmitted data so that the utilization of bandwidth is promoted, and quality of service is maintained. To show the characteristics of the system performing in practice, we evaluate the computation time of the security functions, the performance of the telepointer transmission, the benefits of using the short-code message in coordination, and test the system on NGN network about its delay, jitter, and data loss rate. Performance influence when the system is deployed via tunneling on a network without supporting IP multicasting is also evaluated.

The remaining of this paper is organized as follows. Section 2 describes the telemedicine system design and architecture, emphasizing on these functions essential and unique to the NGN network environments. The experiments of the system on NGN environments about transmission delay, jitter, and system characteristics when various operations invoked are conducted in Section 3. Discussion of the measured characteristics is also given in this section. Finally, Section 4 summarizes the conclusions of our study.

2. System design

Our teleconsultation system was designed to be client–server model based on Microsoft Windows 2000 Server platform to provide the multipoint services. The system consists of two application software, the client and the server, which are depicted in Figs 2 and 1, respectively.

The client application consists of three major modules, i.e., CSCW (including video/audio conferencing and shared workspace), data security and authorization, and medical image retrieval and processing modules. In the overall, these modules provide the user to login to the server from remote site, retrieve image, exchange data

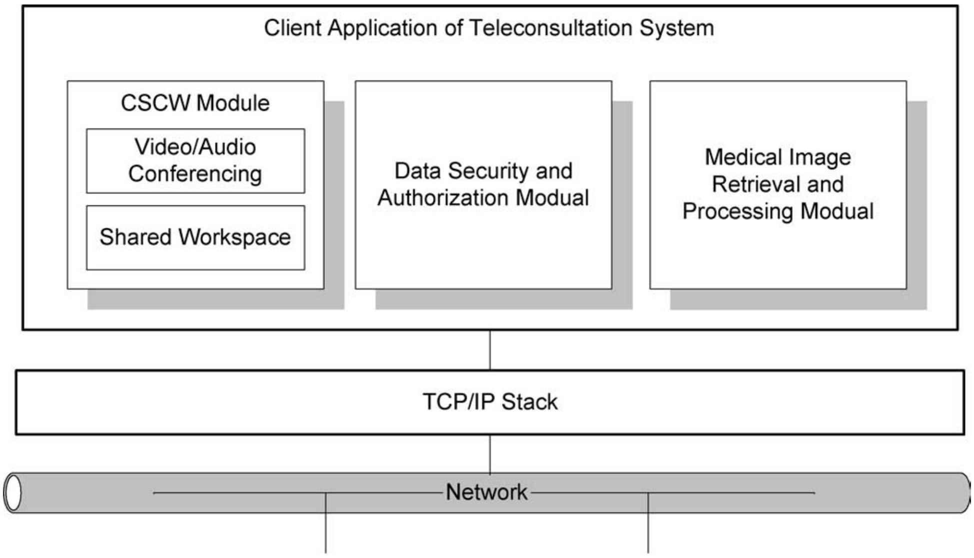

Fig. 1. Client application modules of teleconsultation system.

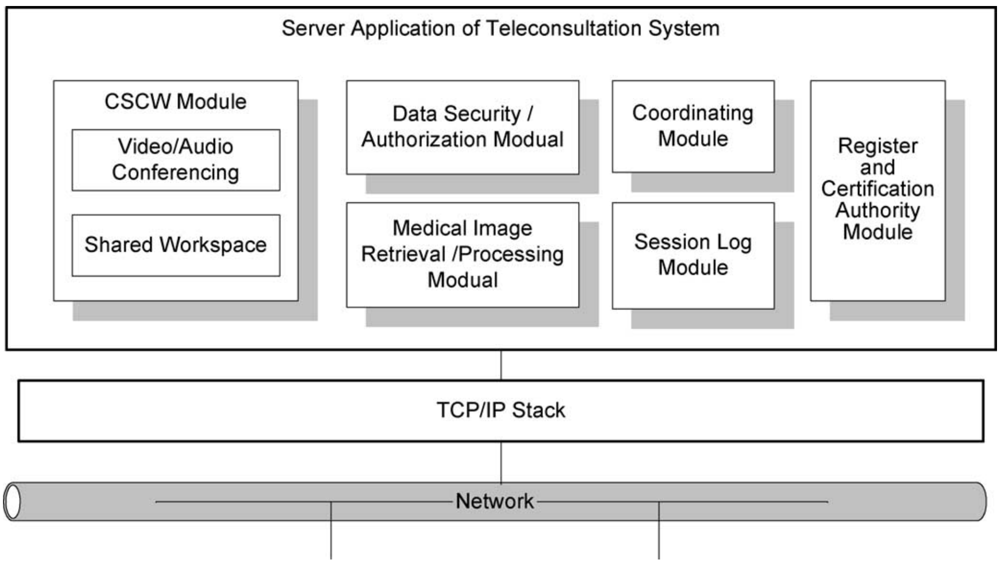

Fig. 2. Server application modules of teleconsultation system.

Table 1
Roles of the users and the corresponding priority and the rights of the operations

Role	Administrator	Session creator	Normal user	Audience
Priority	0 (highest)	1	2	3 (lowest)
System management (account create/delete)	✓			
Session management (invite/kick user)	✓	✓		
Operations (image operations, drawing shape, annotation, etc.)	✓	✓	✓	
Send tele-pointer and audio/video packets	✓	✓	✓	
Receive tele-pointer and audio/video packets	✓	✓	✓	✓

with other users, and process consultation via CSCW. It is worth to note that data transmission between different locations is confidential and privacy through security and authorization services.

In the server side, in addition to the three major modules in client application, session logging procedure, message coordination, and register and certification authority (C.A.) modules are also included. Session logging procedure provides the capability of tracking the events in consultations. Message coordination module maintains the session consistency and handles the data exchanges between all participants. Register and C.A. module takes charge of the user registration, maintaining register database, generating and managing security keys. Besides, the Internet Locator Service (ILS) [20] has to be also initiated to manage conference objects and publish IP multicast conferences on the network.

Four roles of users are defined in the system including system administrators, session creators, normal users, and audiences. Different roles have the different privileges, operation rights, and priorities. System administrator who manages the system such as account create/delete and session management has the highest priority and all of the operation rights. Session creator who manages the session such as inviting participants, kicking roguish participants, changing the roles of the normal and audience users has the second priority and all of the operation rights. Normal user has the third priority and all of the operation rights, but doesn't have rights to manage session and system. Audience has the lowest priority who doesn't have any right to operate the images and must always keeps silence, and is not allowed to send tele-pointer or audio/video packets. Table 1 shows the roles of users and the corresponding priorities and rights of operations.

According to these, the system can avoid roguish users to disrupt the consultation. These considerations are more important in multi-point telemedicine system when applied in the tele-education.

2.1. Computer-supported cooperative work

When the physicians or radiologists are discussing with the other experts between geographic distances, the conversation tools should be built in for bridging the gap of distances. To support cooperative work, synchronous facilities for reflecting the documents and workspace for users' manipulations should also be provided. Therefore, a practical teleconsultation system has to fully support the Computer-Supported Cooperative Work (CSCW) [8–10]. In our implementation, the CSCW module includes video and audio conferencing and shared workspace, described as follows:

2.1.1. Video and audio conferencing

Microsoft Telephony Application Programming Interface (TAPI) version 3.0 was adopted for building our video and audio conferencing module. TAPI 3.0 consists of a set of COM components which are easy to be integrated into any application. It supports industry-accepted H.323 conferencing standard and IP multicast conferencing. To enable multipoint conference, the Site Server ILS service needs to be initiated on at least one server on the

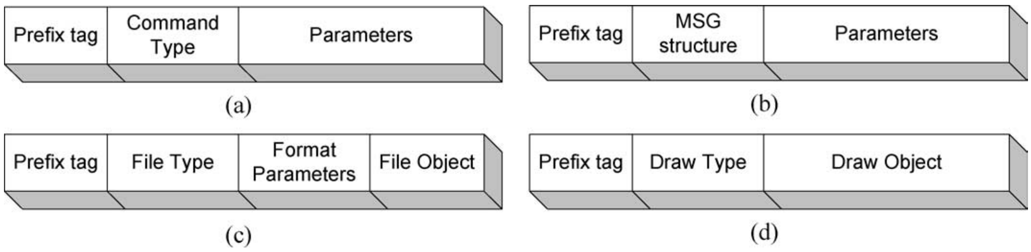

Fig. 3. Data transmission format. (a) System-defined format. (b) M.S. Windows format. (c) File transfer format. (d) Drawing tools format.

network. ILS service manages conference objects, and is used to publish IP multicast conferences on the network. TAPI program has to connect to the ILS server before joining the multicast host group and proceeding a group communication.

In our architecture, ILS service is running on the server side. Client application connects to the server, queries the exist conferences, and decides whether to join or not. The authorized user may also add, delete, and enumerate multicast conferences stored on an ILS Conference Server through the TAPI Rendezvous controls. Since the IP multicast transmission model was employed, users send only one copy of their information to a group IP address that reaches all recipients. It can eliminate the transmission of redundant data, reducing the bandwidth required and achieving the scalability when the number of participants expands.

2.1.2. Shared workspace

Shared workspace provides a remote discussion environment. For keeping the environment consistent, "what you see is what I see" (WYSIWIS) views should be achieved. There are two types of WYSIWS model: strict WYSIWIS and relaxed WYSIWIS [21]. The strict WYSIWIS model, where participants see exactly the same screen, has existed limitations such as display device, display resolution, human usage, etc. For this reason, in our implementation, relaxed WYSIWIS model, which maintains the same window of document rather than keep exactly the same display, was adopted. Users can arrange their windows layout for suiting their display, such as toggling tool bars, moving/resizing windows, and adjusting their resolution. Therefore, the relaxed WYSIWIS model is more flexible and suitable for the human factors.

For maintaining the same document windows of relaxed WYSIWIS model and supporting telepointer, many kinds of messages should be transmitted and exchanged during consultation. Cursor moving messages are used to present the movements of remote cursors; Window control messages are used to maintain the consistency of document windows after resizing, zooming, leveling, and other GUI commands. Drawing tools and annotation text messages are used for ROIs telemarking and text comments embedding. Conference commands messages are used to provide the conferencing control such as user login/logout, join/leave, invite/kick, etc. In addition, image processing commands messages are used to trigger the image processing commands on the remote sites.

In order to transmit these messages appropriately and efficiently, four transmission formats, system-defined, M.S. Windows, file transfer, and drawing tools formats, as shown in Fig. 3, are defined to carry the messages mentioned above. System-defined format is used to transmit the system communication commands such as conferencing commands. M.S. Window format is designed to carry Microsoft Windows Messages, e.g., cursor movement, button click, and menu items of image processing, etc. File transfer and drawing tools formats are used to transmit the files and deliver object-drawing commands, respectively. Based on the definition of formats, maintaining the consistency of the views between different participants is achieved by the transmission of the short-code commands, rather than the image of the entire application window. The bandwidth required is thus significantly reduced due to decreasing the network traffic during consultation.

To farther speedup the network transmission and lower the transmission latency, protocols UDP and TCP are applied in the transmission of different messages according their tolerance capability to packet lost. As cursor moving messages are used to indicate the cursor position of other users, occasional packet loss does not cause vital effect for the system. Therefore, multicast transmission based on UDP is used to transmit the cursor moving messages for improving the transmission efficiency, increasing real-time interactivity, and reducing the bandwidth required. On the contrary, packet loss of other messages would cause system fatal error. Therefore, the transmission of these messages must be reliable, and TCP transmission was adopted. In order to further enhance the efficiency of bandwidth and quality of service, different kinds of the application data such as voice, images, command message, shape annotation, cursor message, and video are assigned a different priority from higher to lower, respectively. The bandwidth is then dynamically allocated depending on the priority of the transmitted data. For instance, when a user wants to retrieve images (the video stream), which has the lowest priority, will be paused to release the bandwidth for accelerating the transmission. By this approach, the utilization of bandwidth is promoted, and quality of service is maintained.

2.2. Messages coordination mechanism

In the system, the server plays the center of network topology by coordinating all the transmission of system messages. Among the messages defined above, conference command messages are used for conferencing control, such as login, logout, join, and leave, etc. These conference command messages are not used for invoking commands or operations on the client site, but for notifying the server about the statuses of the participants in the system. Therefore, when the server receives these messages, it also notifies other clients to adjust to the current consultation status, e.g., user join or leave. On the other hand, all other messages (Windows, file transfer, and drawing tools messages) are to deliver user operations to all the clients. When these messages are received by the server, they are forwarded to all other users who join the same conference, to activate the associated operations on the user sites.

Another issue which should be considered is the “command race” conflictions which result from delivering messages to other clients, especially in image processing command message. As these messages are activated by user’s triggers, it is unavoidable that two users could activate commands simultaneously. This causes the integrity problem where client sites might have different processed results due to the disorder of command arrival. Also, the users will be confused by these conflictions, especially for the users who activate the command. To overcome this problem, a command dispatch mechanism was implemented in our system.

The idea of the command dispatch mechanism is based on that commands are not executed directly by user’s triggering, but coordinated by the server in which a waiting-reply queue is maintained to monitor and control each command’s execution. The command dispatch algorithm flows as follows and is depicted in Fig. 4:

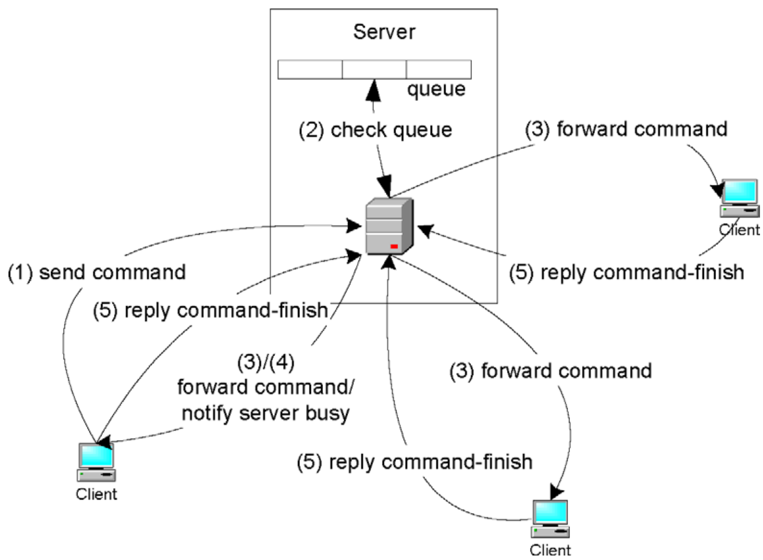

Fig. 4. Command dispatch flow.

(1) When a user activates a command, the command will not be executed immediately in client's computer, but will be sent to the server.
(2) When the server receives the command, it checks the waiting-reply queue to see whether it is empty.
(3) If the queue is empty, the server sends the command to all the client participants, and put a waiting-reply record in the queue for each participant. Otherwise, the server ignores the command, and notifies the sender that the server is waiting for a command to finish.
(4) When a client receives the command sent from the server, it activates its local processing module to perform the command. After the command is finished, the client notifies the server by sending a command-finished message.
(5) When the server receives a command-finished message from a client, the waiting-reply record associated with this client will be removed from the queue.
(6) If the server does not receive the command-finished message of a client for a time interval, it will automatically remove the record from the queue, and try to recover the consistency of all participants by processing the following steps:
    (6.1) Checks the network connection for this client;
    (6.2) If the connection is fine, it will send a signal to terminate the command processing of the client, and send the new image result to the client for replacing the current image.

The mechanism described above not only maintains mutual exclusive of command executions, but also prevent the overlong command execution time for low performance computers.

Embedding a teleconsultation system with the capability of recording the discussion procedures provides add-on advantages for experience learning and retrospective review when argument arises. Teleconsultation usually occurs either when physicians have the difficulty, or at least uncertainty, about the diagnosis decision or when arise cases of worthy special notice. Under this situation, cases under teleconsultation are usually of high complexity, uncommon, and of special to the clinic history, and thus, valuable for education. Therefore, the usability of a teleconsultation system built in with a logging mechanism to record down the consultation process as well as the discussed medical data (images, patient records), physicians' opinions, and image regions which require especial notice, could be extended from opinions exchange to special medical cases collection for learning and analysis.

To record down the consultation procedure, a logging directory is created in the system to store the logging data when the session is started. The directory contains two types of files: medical image files and one event-log file. The event-log file is composed of event records, and is used to keep the events happened in the consultation such as user join/leave, image operations, drawing objects, and cursor movements, etc. When the server receives a command sent from one client, command-received time, the originator, command code, and parameters associated with the command are organized as one event record and saved in the event-log file. Meanwhile, the medical image files accompanying the associated commands (e.g., medical images retrieval commands) are also stored in the logging directory. On the basis of the event logging, the activities happened in the consultation can be reviewed, and the use of the consultation cases for education and training can be achieved.

2.3. Data security and authentication

Data security and authentication are also important issues in the teleconsultation system, since patient data are very personal, and therefore, sensitive and privacy. For the consultation, patient data of medical image, patient record, and diagnosis reports are transmitted through the network. These data are easy to be sniffed and altered. In order to protect the personal privacy and maintain the data integrity, a security and authentication mechanism must be integrated into the teleconsultation system to ensure data confidentiality, integrity, and protected [9,15–17]. In our system, the IDEA [22], of less coding complexity, is adopted for bulk encryption such as images, and RSA [23], an asymmetric coding and of high coding complexity, is adopted for user authentication and secret-key exchange.

In the system security implementation, a Certification Authority (CA) is built in the server. At the first starting of the server, the CA will generate the RSA public and private keys for the server. Before using the system, each user has to sign up the system by registering his/her related information and choosing a login id and passwords. If the registration procedure is successful, the CA will generate the public and private keys for the user, and the user information including the user's public key will be appended in the user information database. Finally, the user will obtain a key disk in which the key pair of the user and the public key of the server are stored. For protecting the private key, a private key password is necessary to retrieve the private key stored on the disk.

On the time of the server creating a consultation, a session secret-key is randomly generated which is used in the IDEA algorithm for transmitting the consultation data such as images. When a user tries to login to the server, he/she has to pass the password authentication. If the authentication is completed successfully, the secret-key exchange procedure proceeds following. For the security reason, the procedures of user authentication and secret-key exchange employ RSA encryption–decryption, digital signature, and verification technology.

3. Experiments and discussions

The system was designed to be able to perform on general multimedia PCs which have Microsoft Windows 2000 platform or later version with ILS service installed. In addition, USB cameras, microphones, and earphones are used for providing the audio/video conferencing. The system can be run in Intranet or Internet environment with TCP/IP protocol, independent from different network medias, such as asynchronous transfer mode (ATM), Ethernet, or Token Ring. In order to fully support the video/audio conferencing and telepointer functions, an IP multicast–enabled network (i.e., Mbone) should be available.

3.1. Cryptography computation evaluation

While the cryptographic mechanisms provide the capabilities of security in the system, they should not affect the system performance too much. For this concern, we measured the time-consuming of the cryptography computation on a Pentium III 450 MHz CPU. The results of the IDEA encryption and decryption tests are shown in Table 2, and the results of the digital signature and verification tests are shown in Table 3. The numbers indicate that the computation time depends on the file size in IDEA and SHA-1 in signature and verification. As for RSA, because its input data in signature and verification is generated from the SHA-1, which is always 160 bits, the computation time is independent from the file size which are 0.17 s for signature and 0.22 s for verification. To understand the influence of IDEA encryption and decryption algorithm for the system performance, we transmitted a medical image file (518 Kbytes) over a network with throughput varying from 64 Kbps to 1 Mbps, and measured the computation time of IDEA and image file transmission time. Figure 5 shows the percentage of IDEA encryption and decryption time over the transmission time. It can be seen that the influence of encryption and decryption is very limited and is less than 6 percent when the available traffic shape is less than 1 Mbps.

Table 2
Computation time of the idea encryption and decryption

	File size			
	4098 Kbytes		518 Kbytes	
Length of the secret-key	16 bytes	8 bytes	16 bytes	8 bytes
Encryption time (sec)	1.172	0.721	0.449	0.092
Decryption time (sec)	1.162	0.693	0.412	0.083

Table 3
Computation time of digital signature and verification

	SHA-1	RSA	SHA-1	RSA
File size	4344 Kbytes		19483 Kbytes	
Signature (sec)	0.270	0.170	1.212	0.171
Verification (sec)	0.271	0.220	1.211	0.220

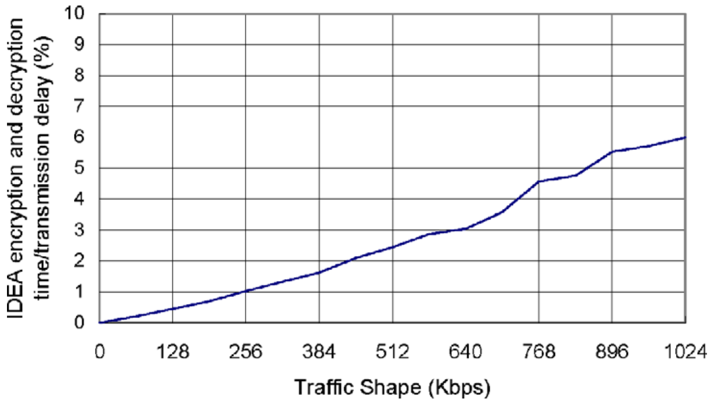

Fig. 5. Percentage of IDEA encryption and decryption time over transmission delay.

3.2. Telepointer measurements over different traffic shape

Telepointer is also an important aided communication tool in teleconsultation system. Supported with the telepointer and audio, a user can indicate the regions of interest in the medical image to other users. To evaluate the performance of telepointer, we measured the transmission latency and the packet loss rate of the cursor movement messages over different traffic shapes. In this experiment, the CISCO 2600 series router with IP multicast enabled is used to simulate the different network traffic and connect the networks. In our experiment, when the consultation is established and the audio/video conferencing is started, the users move their cursors continuously, and the cursor movement messages are sent to the specified multicast group address. Each participant who joins the multicast group would receive these messages and draw the cursor track in their screen. Different traffic shapes are setup by the router to simulate the different network traffic. For evaluating the performance in different bandwidth, 1000 movement messages are sampled for each different traffic shapes. The average and the standard deviation of the transmission latency are obtained and shown in Fig. 6(a) and Fig. 6(b), respectively. According to Fig. 6, it can be seen that the average transmission latency quickly decreases from 2.956 sec to 0.778 sec while the available traffic shape increases from 64 Kbps to 160 Kbps; meanwhile, the standard deviation also decreases from 0.524 sec to 0.005 sec. Both of the average and the standard deviation of the transmission latency are stable while the traffic shape is greater than 160 Kbps. Therefore, we can know that the minimum bandwidth requirement during the consultation is about 160 Kbps including audio/video conferencing and telepointer. On the other observation, packet loss rate also exhibits this feature; when the traffic shape is greater than 160 Kbps, the packet loss rate is reduced to 0, as shown in Fig. 6(c).

3.3. Message coordination design evaluation

For analyzing the benefit of the messages coordination, the system was tested in our laboratory subnet with 100-Mbit/s Ethernet, and performed upon the Pentium III CPU 450 MHz and 128 MB RAM computers. The flow of the data transmission was measured between one client and the server. First, the clients connected to the server, and finished the user authorization procedure. After the user joined a consultation, the video/audio conferencing and telepointer were enabled, beginning the conferencing data transmission. During the consultation, three images of 519 KB, 191 KB, and 519 KB were fetched. Various image analysis operations such as zoom in/out, segmentation, and smoothing filtering were also performed. The flow of the data transmission between the client and the server is shown in Fig. 7(a). From Fig. 7(a), we can see that there are three peaks appearing in the flow. These peaks represent the bulk network transmission in the three image fetching. Except these bulk flows, other flows are very low as a result of the short-code command message transmission. In contrast, another command synchronization via transmitting the whole image result instead of short-code message was designed and tested. The test procedure

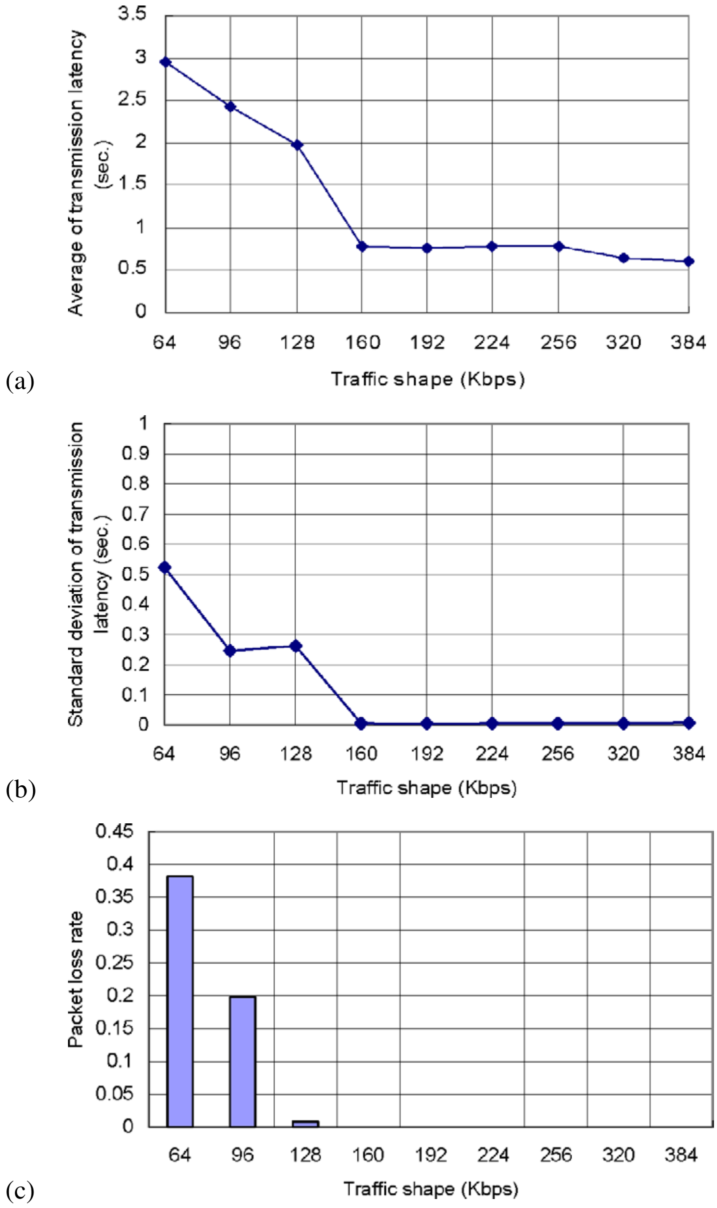

Fig. 6. Performance of the telepoint movement over different traffic shape. (a) Average of the transmission latency. (b) Standard deviation of the transmission latency (c) Packet loss rate during the messages transmission.

is the same as the short-code message synchronization. The flow of the data transmission between the client and the server is shown in Fig. 7(b). From Fig. 7(b), we can see that the peaks not only happen in the image fetching but also appear during the image processing operations. This implies that by adopting the short-code command, the large network bandwidth consumption has been reduced to only when image fetching is performed. Besides of the consumed bandwidth, another benefits obtained in the short-code command synchronization approach is the real-time of user responses. As the session proceeds, image processing operations are often performed for the discussion of subtle findings. Therefore, it is required that these operations should not cause significant physicians' operation delay. Consequently, to maintain an acceptable interaction, the user response time should be short. Figure 8 shows

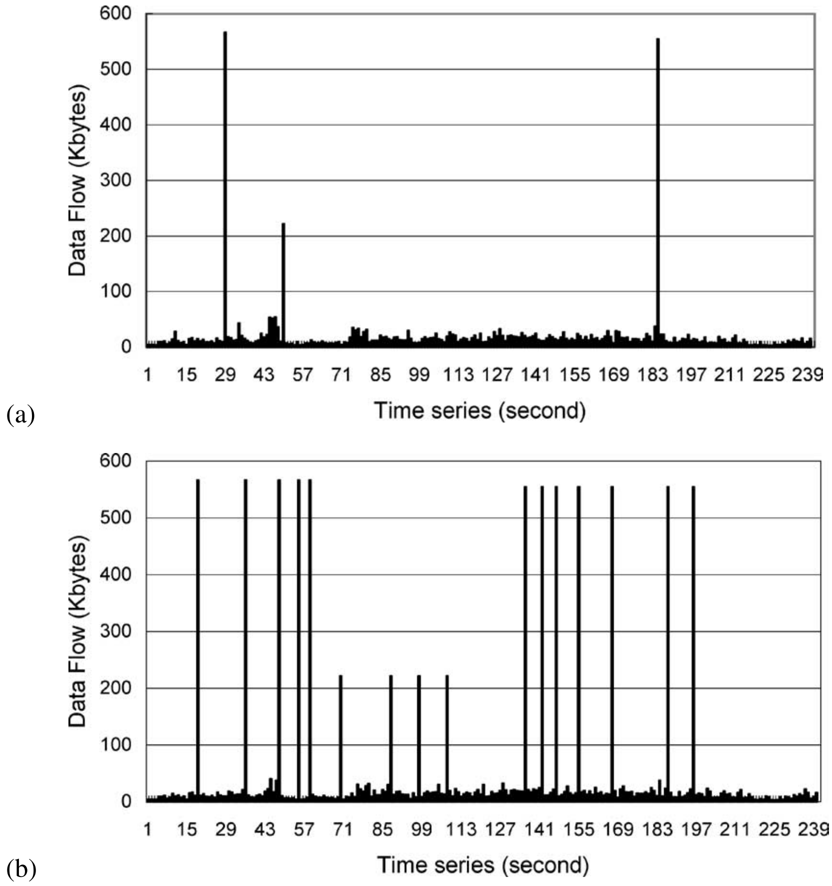

Fig. 7. Distribution of the flow of the data transmission: (a) by sending the operation command message, (b) by sending the operation result image.

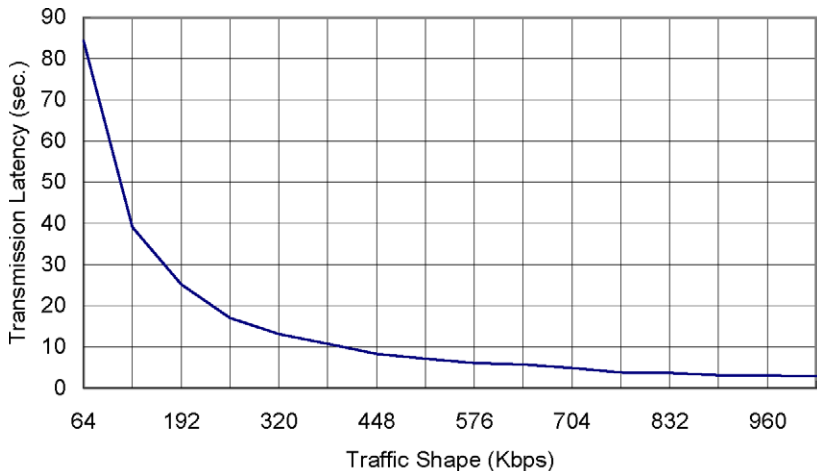

Fig. 8. Transmission latency of an image of 519 Kbytes with different available traffic shapes from 64 Kbps to 1024 Kbps.

the transmission latency of an image of 519 Kbytes with different available traffic shapes from 64 Kbps, 160 Kbps, to 1024 Kbps, where the transmission latency is from 84 seconds, 30 seconds, to 3 seconds, respectively. While it is reasonable to wait 2–3 seconds for an image retrieval, especially that the image retrieval can be performed in a scheduled prefetch, it is unacceptable to wait additional 2–3 seconds for operating every analysis operation in transmission from command synchronization, not to mention that more waiting time could be spent in a network of worse traffic. As discussed in Section VII-B, the basic bandwidth requirement of our CSCW module is about 160 Kbps for providing audio/video conferencing, telepointer, and command messages transmission. Based on this consideration, we know that, without the use of short-code command transmission, either the user would expect 30 seconds of waiting time for each analysis operation, if 160 Kbps applied, or the system would require at least 1024 Kbps bandwidth, if the additional operation waiting time is to be reduced to 2–3 seconds.

3.4. Topologies of network trials

The system has been tested on the three platforms of networks which topologies are shown in Fig. 9. Figure 9(a) shows the trial topology of a newly constructed broadband network in Taiwan, called NBEN (National Broadband Experimental Network) which construction is supported by the National Science and Technology Communication in Taiwan. The NBEN, constructed starting from 1998 and completed in June 1999, is an OC-3 ATM network connecting major universities, research institutes and organizations in Taiwan, as shown in Fig. 10. Following the NBEN construction, several research projects were also initiated. The purpose of these projects is to develop key transmission technologies in the broadband network. At the initial implementation stage of the NBEN, the network protocols including IPv6, RSVP, and IP multicasting were developed for providing the NBEN with guaranteed quality of service transmission to support the applications on it. Our system is also tested on the NBEN platform utilizing its high-speed and multicasting capabilities for transmitting multimedia data. Table 4 shows the test results of the average latency and jitter corresponding to the three types of data: mammogram (4098 Kbytes), CT/MR (512 Kbytes), and system messages (112 bytes). It can be seen that the image file of 4098 Kbytes can be retrieved in about 2 seconds (1845 ms), while the average transmission latency of system messages, each about 112 bytes, is 47 ms with variation 0.012 ms. Therefore, the image operation and the cursor movement of telepointer, which are transmitted through the system messages, can be performed in smooth interaction of small latency delays.

In order to address the system deployment in a network without supporting IP multicasting, we also test the system on the campus network by using the tunneling technologies to achieve the multicasting. Figure 9(b) shows the trial topology of the campus ATM OC-3 network which is not an IP multicast-enable network. In this trial, the tunneling technologies are employed between endpoints over the internetwork to transfer the IP multicast packets from one network to another network. Tunneling is an expedient method for transmitting datagrams between multicast-capable endpoints separated by routers, bridges, or switches that do not support multicast traffic. Tunnels encapsulate each IP multicast packet with an additional IP header. In the new IP header, the source workstation IP address is replaced by the IP address of the tunnel source, and the destination multicast IP address is replaced by the address of the tunnel endpoint. Therefore, tunneling allows the multicast traffic to travel across portions of the Internet that do not support multicast forwarding [24]. For evaluating the performance of tunneled multicast, we simulated multicast traffic at three data rates: 64 Kbps, 384 Kbps, and 512 Kbps for two pairs of multicast groups. The first group consists of two multicast-capable routers, and the second group used two lab routers with tunneling for multicast operation. A sample file of 256 Kbytes was transmitted over the two groups for 5 minutes, and the data streams were analyzed for throughput, packet jitter, and data loss rate as shown in Table 5. It can be seen that when the sending data rate increases, the performance of the group using tunneling is getting worse. In 512 Kbps trials, the throughput of the group using tunneling is at 99.8% of the transmitted data rate. The data loss rate and jitter are also higher than the network with multicast-capable routers. As mentioned above, the performance with the tunneled multicast network is slightly worse than the native multicast network because the use of tunneling requires higher workloads such as encapsulating, transporting, and de-encapsulating multicast streams.

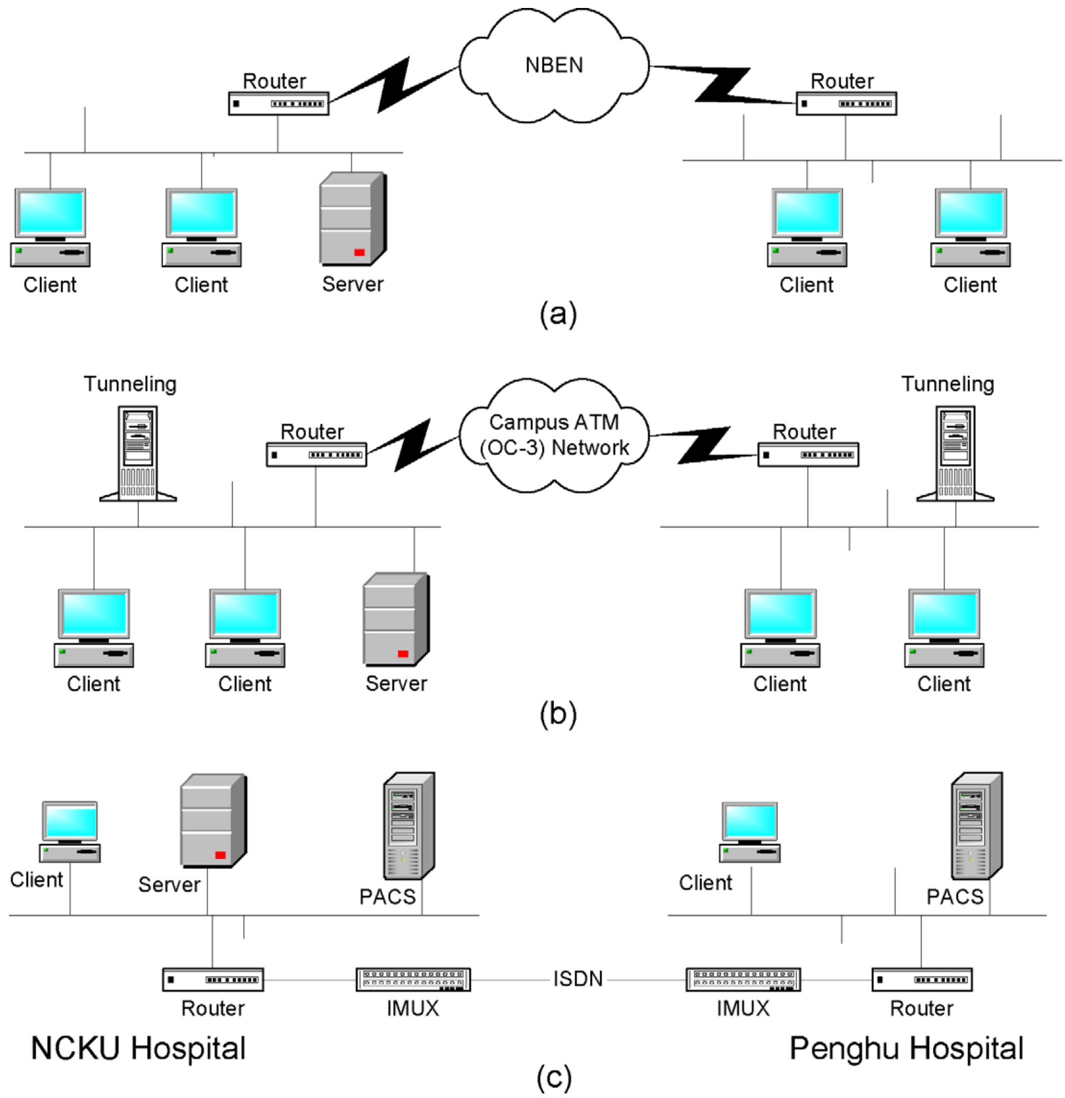

Fig. 9. Topologies of the networks in the trials. (a) An NBEN network with IP multicast-enable. (b) A campus ATM network using tunneling technologies to transfer the IP multicast packets. (c) ISDN network connection between NCKU Hospital and Penghu Hospital.

As the clinical test, the system is installed between the National Cheng Kung University Hospital (NCKUH), one of the medical centers in the southern Taiwan, and the Penghu Hospital (PH), the major hospital in the off-shore island Penghu of Taiwan, through ISDN network connections, as shown in Fig. 9(c). Due to the geographical disadvantage, the manpower and medical services in the outlying Penghu Hospital is very limited. Therefore, a telecommunications medical consultation program was initiated between NCKUH and PH to provide medical services for Penghu areas. The traditional teleconsultation system between NCKUH and PH was established on the UNIX-based workstation platform in 1995. The functionality of the traditional system consists of two independent subsystems: an audio/video conferencing system and a consultation system providing telepointer, medical image transmission, and image zooming/inverting. However, these functions cannot satisfy the requirements of the modern teleconsultation due to the lack of support for DICOM image standard, security, user authorization, and image analysis tools. Besides, the conferencing and consultation subsystems are independent, and therefore, the audio

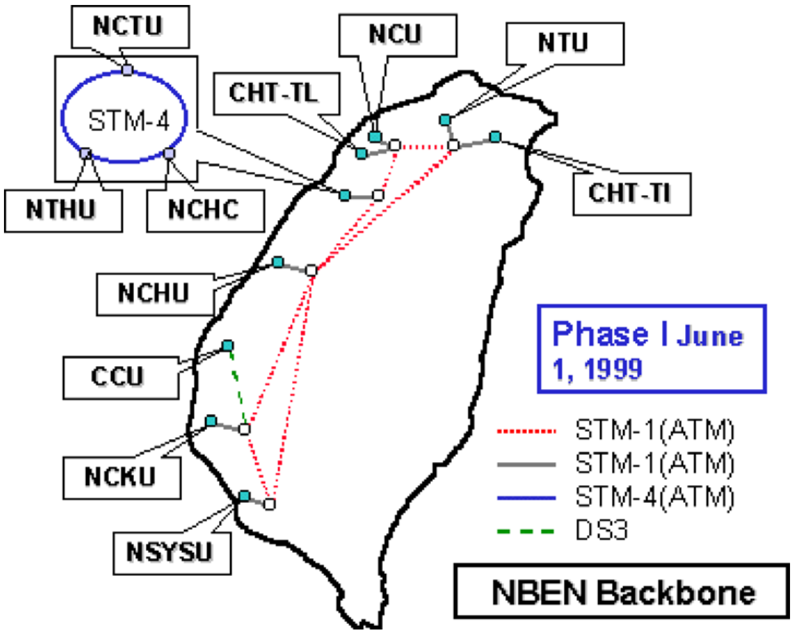

Fig. 10. Topology of NBEN backbone.

Table 4
Data transmission tests on NBEN

Data size	Avg. latency	Avg. jitter
112 bytes	47 ms	0.012 ms
519 Kbytes	313 ms	0.087 ms
4098 Kbytes	1845 ms	0.203 ms

Table 5
Performance comparison with multicast routers and tunneling

	Using multicast router			Using router with tunneling		
Sending data rate (Kbps)	Avg. throughput (Kbps)	Data loss rate (%)	Avg. jitter (ms)	Avg. throughput (Kbps)	Data loss rate (%)	Avg. jitter (ms)
64	64	0	0.006	64	0	0.015
384	384	0	0.011	384	0.013	0.129
512	512	0.017	0.091	511	0.081	0.472

and video data cannot be manipulated such as recorded and captured; it is especially darned inconvenience to visual diagnosis such as dermatosis, etc. Our system is established as a test system on PC Windows-based platform, which provides DICOM image retrieval, security, user authorization, and image analysis tools and audio/video integration. The consultation procedure could also be record in the system to provide review and education purposes.

4. Conclusions

Recently, the next generation network (NGN) has been a new trend as the Internet backbone. The NGN provides a high-speed broadband network environment of a faster data transmission, larger network bandwidth, and more network protocol capabilities including Ipv6, RSVP, and IP multicasting. These results completely revolutionize the traditional healthcare delivery, and make the possibility of the real-time transmission of large-volume medical images in broadband networks. In hospital, particularly Taiwan, the construction of PACS emerges in recent years in the wake of the coming of NGN advanced broadband communications. This imposes the requirement of the DICOM standard in a telemedicine system for communicating to the PACS connecting with several imaging modalities, and the security issues are also raised considering the personal privacy and data integrity for medical data transmission in public networks. This also drives a teleconsultation system to merge medical imaging with multimedia data for extending communication capabilities using the real-time high-quality video conferencing.

Under such situations, this paper combines security functions, DICOM standard, and CSCW in the teleconsultation system using message coordination mechanism for maintaining system consistency. The built-in computer-supported cooperative work (CSCW) creates a collaborative consultation environment for physicians to proceed the consultation, and the video/audio conferencing module for the physicians face-to-face communication. To evaluate the network in providing the CSCW functions in real-time transmission, we measure the bandwidth requirement of the CSCW module and find out that the basic bandwidth requirement of the CSCW module is about 160 Kbps for providing audio/video conferencing, telepointer, and command messages transmission. This can be easily achieved in the NGN network environment going to the last mile of home or remote areas. The encryption for providing user authorization is the function to ensure the privacy and integrity of the patient data in the transmission during consultation. The experiments show that the influence of encryption and decryption on data transmission delay is very limited. The encryption and decryption of IDEA totally take 175 ms for 518 Kbytes medical image file and 8 bytes security key length. This occupies less than 6 percent of the file transmission time when the available traffic shape is less than 1 Mbps. The experiments also show that adopting the short-code message drastically reduces the bandwidth requirement and also the user waiting time during the consultation. A command dispatch algorithm is implemented to prevent the race conflictions from the use of short-code command message in the system. Based on the algorithm, users can perform the operations without collisions occur, and the image status can be maintained consistent among all clients.

The multicasting is one transmission technique adopted to avoid the increase of network traffic when the number of participants expands. This is especially important when many users need to join the consultation, such as tele-education applications. This technique needs an IP multicast-enabled network to support IP multicast routing and forward of IP multicast packets. When this network setting cannot be achieved, fortunately, the tunneling technologies can be employed between endpoints over the network to transfer the IP multicast packets from one network to another network. In the experiments, we test these technologies and successfully deploy the system on the network without supporting IP multicasting. Our experiments also show that the use of tunneling slightly increases jitter and data loss rate because of the workloads such as encapsulating, transporting, and de-encapsulating multicast streams. However, the overall system throughput and scalability are improved, and bandwidth saved, with multicast.

Acknowledgements

The authors would like to thank the National Science Council for supporting this work under the Grant numbers NSC90-2219-E-006-009 and NSC91-2622-E-006-079.

References

[1] H.K. Huang, Teleradiology technologies and some service models, *Computerized Medical Imaging and Graphics* **20** (1996), 59–68.

[2] J. Zhang, J.N. Stahl, H.K. Huang, X. Zhou, S.L. Lou and K.S. Song, Real-time teleconsultation with high-resolution and large-volume medical images for collaborative healthcare, *IEEE Trans. Inform. Technol. Biomed.* **4**(2) (2000), 178–184.

[3] E.J. Gomez, F. del Pozo, E.J. Ortiz, N. Malpica and H. Rahms, A broadband multimedia collaborative system for advanced teleradiology and medical imaging diagnosis, *IEEE Trans. Inform. Technol. Biomed.* **2**(3) (1998), 146–155.

[4] R. Sacile, Telemedicine systems for collaborative diagnosis over the Internet towards virtual collaboratories, in: *Proc. 2000 Academia/Industry Working Conference on Research Challenges*, 2000, pp. 191–196.

[5] M. Akay, I. Marsic, A. Medl and G. Bu, A system for Medical Consultation and Education using Multimodal Human/Machine Communication, *IEEE Trans. Inform. Technol. Biomed.* **2**(4) (1998), 282–291.

[6] J.N. Stahl, J. Zhang, Ch. Zellner, E.V. Pomerantsev, T.M. Chou and H.K. Huang, Teleconferencing with dynamic medical images, *IEEE Trans. Inform. Technol. Biomed.* **4**(2) (2000), 88–96.

[7] E.I. Karavatselou, G.-P.K. Economou, C.A. Chassomeris, V. Danelli-Mylonas and D.K. Lymberopoulos, OTE-TS – a new value-added telematics service for telemedicine applications, *IEEE Trans. Inform. Technol. Biomed.* **5**(3) (2001), 210–224.

[8] Y. Bouillon, F. Wendling and F. Bartolomei, Computer-supported collaborative work (CSCW) in biomedical signal visualization and processing, *IEEE Trans. Inform. Technol. Biomed.* **3**(1) (1999), 28–31.

[9] L. Makris, I. Kamilatos, E.V. Kopsacheilis and M.G. Strintzis, Teleworks: A CSCW application for remote medical diagnosis support and teleconsultation, *IEEE Trans. Inform. Technol. Biomed.* **2**(2) (1998), 62–73.

[10] L. Kleinholtz, R. Virchow and M. Ohly, Supporting cooperative medicine: The Bermed project, *IEEE Multimedia Mag.* (winter, 1995), 44–53.

[11] F. Malamateniou, G. Vassilacopoulos and P. Tsanakas, A workflow-based apporach to virtual patient record security, *IEEE Trans. Inform. Technol. Biomed.* **2**(3) (1998), 139–145.

[12] S. Tachakra, M. Loane and Ch.U. Uche, A follow-up study of remote trauma teleconsultations, *J. Telemed. Telecare* **6**(6) (2000), 330–334.

[13] E.D. Lemaire, Y. Boudrias and G. Greene, Low-bandwidth, Internet-based videoconferencing for physical rehabilitation consultations, *J. Telemed. Telecare* **7**(2) (2001), 82–89.

[14] O. Cuzzani, M. Bromwich, E. Penno and H. Gimbel, The effect of transmission bandwidth on the quality of ophthalmological still and video images, *J. Telemed. Telecare* **6**(4) (2000), 11–13.

[15] M. Miller and M. Copper, Security considerations for present and future medical databases, *Int. J. Bio-Med. Comput.* **41** (1996), 39–46.

[16] S. Bengtsson and B.B. Solheim, Enforcement of data protection privacy and security in medical informatics, in: *Proc. MEDINFO'92*, K.C. Lyn, P. Degoulet, T.E. Piemme and O. Rienhoff, eds, North-Holland, Geneva, Switzerland, 1992, pp. 1561–1565.

[17] L. Makris, N. Argiriou and M.G. Strintzis, Network access and data security design for telemedicine applications, *Med. Informat. J.* **22**(2) (1997), 133–142.

[18] Microsoft Co., *IP Telephony with TAPI 3.0 White Paper*, Microsoft Co., 1999.

[19] Microsoft Co., *Telephony Application Programming Interface*, MSDN Library, Microsoft Co., Oct. 2000.

[20] Microsoft Co., *Inter Locator Service*, MSDN Library, Microsoft Co., Oct. 2000.

[21] S. Greenberg, C. Gutwin and M. Roseman, Semantic telepointers for groupware, in: *Proc. 16th Computer–Human Interaction Conference*, Australian, 1996, pp. 54–61.

[22] NBS, Data encryption standard, Nat. Bureau Standards, U.S. Dept. Commerce, Washington, DC, NBS FIPS PUB 46, 1977.

[23] R.L. Rivest, A. Shamir and L.M. Adleman, A method for obtaining digital signatures and public-key cryptosystems, *Commun. ACM* **21**(2) (1978), 120–126.

[24] L. Allen et al., GBS IP multicast tunneling, in: *Proc. 21st Century Military Communications Conference*, Vol. 2, 2000, pp. 699–703.