2.5 Networked Medical Care

In the future, networks will support expert medical care, including surgery, delivered to patients in remote and mobile locations on line, in real time, and collaboratively in a highly secure, intelligent, dynamic, and reliable environment. Additionally, doctors will access distributed medical records and medical expertise wherever it is located.

2.5.1 Medical Scenario Description

A middle-aged man at home begins to suffer chest pains. He uses a medical sensor to take automated medical readings that are relayed to a medical center that determines he is having a heart attack. In an ambulance dispatched to take him to the hospital, sensors monitor his vital signs and cardiac function. A remote cardiologist monitors these data and accesses the patient's medical records. She orders an angiogram to be taken when the patient reaches the hospital. The angiogram shows a possible anomaly and a remote consultant is shown the angiogram over the Internet. The angiogram displays a warning that the resolution of the image, as delivered by the Internet, does not meet the standard required for angiogram interpretation.

Heart surgery is performed on the patient at the hospital. An anomalous cardiac vasculature found in the patient leads the surgeon to consult an on-line 3-D anatomical library in real time. The library finds a consultant surgeon who, also in real time, assists in the operation, occasionally taking control of the haptic surgical robot.

2.5.2 Networked Medical Care Research Needs

Ubiquity

Multimegabit-per-second effective wireless bandwidth from multiple sources is needed. Bandwidth available during the ambulance ride may occasionally be degraded so the network should be able to identify networking alternatives, choose the best alternative for the application, and reconfigure the network.

Trustworthiness

Trustworthiness has many components that collectively assure the end users of the quality, timeliness, security, and reliability of the services provided by the network:

- Security and data integrity: First and foremost, the network must meet legal standards for medical data privacy and security as currently documented in the Health Insurance Portability and Accountability Act (HIPAA). This requires the networks to support authentication of the patient and the end user, authorization for end users, encryption to support privacy requirements, and traffic diversity to prevent identification of restricted information through traffic analysis. Authorization and access should be logged to provide an historical security record. Data security is required for restricted data and to assure data accuracy and integrity.

- Quality of Service: QoS is required to support the strict demands of distributed medical care delivery and collaboration. To support the cardiologist at a remote site, the wireless channel must provide real-time video and real-time data indicating the quality of the video display. Although this scenario may tolerate a fair amount of latency, it will not tolerate jitter and the video, audio, and data channels must be synchronized. Medical service must be provided across network service boundaries in a dynamic and sometimes mobile environment. All devices need to support QoS, and the system must be able to adapt in real time to networking or data content changes.

Sensors and end user devices

Networks must support dynamic sensors and end user devices that must be identifiable and locatable. Sessions may migrate from one device to another – for example, migrating from a fixed end station in a patient's home to PDAs in an ambulance requires networking services that support significantly different access interfaces.

Collaboration environments

The networks must support ad hoc establishment of collaboration sessions for specific access modes, locations, service needs, and networking capabilities. For example, one participant may need voice-only capability while others may need varying degrees of video, voice, and whiteboarding. The networks also need to support access to on-line resources such as distributed computing and database access to support the collaboration. Security, discussed above, is critical to collaboration environments.

Intelligent networking, end-to-end performance

The medical scenario angiogram procedure illustrates the need for end-to-end knowledge of the network data path including the end user display devices to assure that angiogram interpretation standards are met. Thus, an intelligent, scalable network needs to be able to reconfigure itself and automatically resolve any QoS problem to meet medical standards. The network must report any unresolvable problem to the participants.

Assured real-time service

For the bypass surgery scenario, the surgeon needs to retrieve 3-D image data sets, each of which may be several gigabytes in size. The consultant must be able to view the surgery in real time and accurately guide the surgical robot using its haptic controls. This requires a network operating at high bandwidth with minimal latency and minimal jitter while maintaining the security and integrity of the transmissions and the privacy of the patient data.