Mobile / Sensor Networks an Integrated System for Healthcare: Potential and Challenges

Ramanna S Havina¹, Girish V Attimarad, M N Giriprasad
Associate Professor, M.B.E Society’s College of Engg., Ambajogai (e-mail: rshavina@rediffmail.com)
Professor Electronics and Communication Engg Dept, Dayanand Sagar College of Engineering Bangalore
Head Electronics and Communication Engg Dept, Dayanand Sagar College of Engineering Bangalore

Abstract - The mobility and flexibility of wireless networks provide convenience and increased productivity. The health care enterprise is faced with some difficult decisions about whether, when, and how to implement wireless solutions. Sensor devices integrating embedded processors, low-power, low bandwidth radios, and a modest amount of storage have the potential to enhance emergency medical care. Wearable vital sign sensors can track patient status and location. The needs to provide medical services in remote areas have motivated researchers to develop telemedicine systems. Telemedicine system operating in such areas must have advanced wireless technology supporting it. Approach is on MANET combined with Mobile IP and MIPv6, is the basis of infrastructure for the mobile telemedicine system.

I. INTRODUCTION

The health-care working environment is ‘highly mobile’, with clinicians constantly moving around from patient to patient while performing their duties. This constrains the shape and performance of computing devices that can be used in such an environment. The clinicians make decisions at the ‘point of care’ i.e., the patients bedside, and they do not have the time to leave and potentially queue up to refer to a desktop based application. Hence, the ideal platform for use in such an environment is the PDA or tablet PC platform, which the clinician can carry around and use wherever necessary. The most obvious issues are those of patient confidentiality and doctor-patient relationship. It is vital that medical data is kept confidential via the use of potentially several vertical layers of security. One of the notable consequences of working in the mobile environment is the different trade offs that have to be made. Data could be stored locally on the client device giving the advantage of fast access. However, this is going to impact on the limited memory available on mobile devices. Alternatively the data could be store remotely at the server and downloaded as required, however this would incur a time over head as the data is downloaded to the device. Thus there is a trade-off here between memory consumption and communication overhead, and the decision depends on the semantics of data in relation to the application. Another trade-off comes as a result of the weak processing power on the mobile device. The healthcare community is showing a strong trend in the adoption of mobile technology, particularly in the use of mobile device such as PDAs.

Dr. Girish V Attimarad is and Dr M N Giriprasad Professor and Head Electronics and Communication Engg Dept, J N Tu college of Engineering Anantapur Communication among healthcare workers in different areas often takes place via fixed telephones, because most hospital regulations prohibit the use of cell phones in many areas of the facility. Immediate access to patient data from anywhere in the facility can significantly reduce potentially life-threatening errors while increasing healthcare workers’ productivity. This, in turn, improves the quality of patient care and reduces costs.

II. TECHNOLOGY FOR THE HEALTHCARE

Mobile computing in a healthcare setting requires more than a notebook computer. Such infrastructure includes the data capture technologies (such as bar-code scanning) to improve the efficiency and accuracy of the user when entering information; the mobile computers (such as PDAs) that can be used to access patient data at the point-of-care, the wireless networks to securely connect the users to the servers, and the software to manage and monitor it all. The network should be highly scalable, with high availability for maximum up-time, and it should support functions such as locationing, voice over IP (VoIP), used in nurse call and other communication applications. Obviously, it needs to support HIPAA security standards. Even so, regulations around patient privacy and safety can make implementing such technical solutions difficult. We need a technology that liberating doctors and nurses from desks, paper and PCs, and giving them fast, secure, mobile access to lifesaving information – where and when it’s needed. The result is increased productivity and a reduction in errors. This technology help medical personnel:

- Match patients with medications
- Track samples from bedside to lab
- Track blood from donation to transfusion
- Download appointment schedules
- Order lab tests and view results
- Communicate, both with patients and other personnel
- Quickly locate critical equipment

Mobility is critical in a healthcare environment but not at the cost of security. Wireless net working products provide security per HIPAA standards. The wireless intrusion protection system alerts system administrators to security breaches such as attempts to hack into the network, and risks such as rogue networks, as well as providing reports to support HIPAA compliance.

2.1 Mobile Healthcare Solutions

Mr. Ramanna S Havinal is
Some healthcare quality studies have shown that adverse events in hospitals are related to information management. By speeding up the flow of information and increasing accuracy, we can eliminate the errors, delays and double handling that can occur when information is not readily available. By giving doctors, nurses and other caregivers access to correct, up-to-the-minute information wirelessly, hospitals can work more efficiently and virtually eliminate potential mistakes like administering the wrong treatment to patients. The aim of introducing new communication technologies into the hospital is to give health professionals immediate access to patient information regardless of physical location. For this to work, the device needs to be completely reliable and able to withstand the sometimes harsh hospital environment. The devices are tough enough to withstand multiple drops to concrete floors, extreme temperature variances and are water- and dust resistant. They include both wireless and barcode scanning functionality, so they'll be able to scale to suit our needs as the solution evolves. This technology should allow the hospital to run more efficiently, enabling us to treat more patients and provide a better level of care. Instead of spending hours waiting to access information, hospital staff will be able to treat and discharge patients quickly and accurately. By making a more comprehensive array of information more readily accessible where it is most needed, we can improve the quality of service for each application.

2.2 Building A Business Case For Mobility
Factors to consider in a wireless solution are:
- Network security and standards compliance
- Support for emerging technologies
- Positioning requirements
- Roaming capabilities
- Required bandwidth
- Quality of service
- Outdoor applications
- Scalability
- Ease of monitoring, troubleshooting
- Minimal disruption in the surrounding area

Wireless network can also deliver significant ROI, in three main areas:
- Improved productivity
- Reduced capital expenditures
- Improved process efficiency/error reduction

A healthcare enterprise should implement wireless only after a careful examination of the potential risks. Based on these results, patient safety, and enterprise security are key factors to consider when making these decisions. Risk analysis involves the examination of the following three factors:

1. Assets — including confidential and private patient and business information, life-critical data and information services, and business critical data and information services.
2. Threats — including competitors, disgruntled employees, dissatisfied patients, and amateur and professional wireless “sports enthusiasts”.
3. Vulnerabilities — Exposed Access Points, SSIDs Used for Authorization

2.3 Understanding Security To Ensure Compliance With Hipaa
With a large mobile population of doctors, nurses, physician’s assistants and other caregivers, wireless technology bring the ability to access the latest patient charts, medical records and clinical decision support data at all times, anywhere in the healthcare organization. And as caregivers travel among different facilities, wireless allows for easy connectivity at each site. Unless specifically configured for security, most wireless equipment is an ‘open’ network, or able to be attached to by any wireless client. This obviously could lead to serious security risks if unauthorized personnel were to gain access to the healthcare network. While security vulnerabilities endanger the integrity of any corporate network, the risks are magnified in healthcare due to HIPAA legislative requirements. HIPAA, or the Healthcare Information Portability and Accountability Act, is a law that aims to simplify the processing and distribution of medical information, improve the portability of health insurance, give patients access to medical information and protect patient data that is stored, transmitted or accessed across networks. To meet HIPAA guidelines, Wireless system delivers the following security features:

Support For Multiple VLANS With Independent Security:
Many types of users may need to access the healthcare wireless network. Doctors, nurses and other caregivers need access to patient records, charts and test results. Other staff such as dieticians and medical billing staff don’t need access to sensitive patient data. Virtual LANS allow each authorized wireless LAN user to gain access to only the network resources they need to see.

Addressing Security Management, Configuration And Incident Reporting Procedures:
Beyond protecting the wireless LAN itself against vulnerabilities by using WPA for strong encryption and authentication, the HIPAA standard also requires that certain administrative and procedural controls be in place to protect the security and integrity of the data. To address these issues, the Wireless system should provide the following capabilities:

Defense Against Rogue Access Points:
With the ready availability of inexpensive consumer-grade access points, a new threat has emerged to enterprise security. Employees with a desire to have wireless connectivity, may bring access points into the enterprise and plug them into the corporate network, without any security mechanism enabled. Once behind the firewall, anyone within range of the signal can connect and access the network or do malicious hacking. Proactive rogue access point detection ensures that the enterprise is protected from this threat. The Wireless System proactively searches out rogue access points, can identify unknown and non-authorized access points, alerting IT administrators. Clients attempting to associate with a rogue access point can be automatically blocked, preventing all access to the Enterprise network unless through an authorized access point.

Notification Of Configuration Changes:
Mis-configured access points can lead to unauthorized users accessing the network, or private healthcare information being broadcast in the open for others to eavesdrop. The Wireless System should provide the ability to constantly monitor the
access points and ensure that all authorized access point security policies remain in place. If the access point configuration changes, immediate notification is provided to the IT administrator and all client connections to the mis-configured access point are prevented.

**Prevention Of Additional Internal Security Violations:**
Beyond rogue access points, the most common threat to the corporate network security is formation of ad hoc networks, or authorized wireless clients connecting to neighboring wired networks. In both cases, this can leave the healthcare institution open to security violations as confidential healthcare information may be accessed on the client device through these insecure and unauthorized connections. The system continually monitors the airwaves throughout the enterprise for internal security violations such as these, and automatically prevents them before confidential information can be transmitted.

### III. AN AD HOC SENSOR NETWORK FOR MEDICAL CARE

Wireless sensor networks are an emerging technology consisting of small, low-power, and low-cost devices that integrate limited computation, sensing, and communication capabilities. This technology has the potential to have enormous impact on many aspects of emergency medical care. Sensor devices can be used to capture continuous, real-time vital signs from a large number of patients, relaying the data to handheld computers carried by emergency medical technicians (EMTs), physicians, and nurses. Wearable sensor nodes can store patient data such as identification, history, and treatments, supplementing the use of back-end storage systems and paper charts. In a mass casualty event (MCE), sensor networks can greatly improve the ability of first responders to triage and treat multiple patients equipped with wearable wireless monitors. Such an approach has clear benefits for patient care but raises challenges in terms of reliability and complexity.

**CodeBlue**, a wireless infrastructure intended for deployment in emergency medical care, integrating low-power, wireless vital sign sensors, PDAs, and PC-class systems. This will enhance first responders’ ability to assess patients on scene, ensure seamless transfer of data among caregivers, and facilitate efficient allocation of hospital resources. Intended to scale to very dense networks with thousands of devices and extremely volatile network conditions, this infrastructure will support reliable, ad hoc data delivery, a flexible naming and discovery scheme, and a decentralized security model. **CodeBlue** offers an efficient wireless communication substrate for medical devices that addresses ad hoc network formation, naming and discovery, security and authentication, as well as filtration and aggregation of vital sign data. **Code-Blue** is designed to operate across a wide range of devices, including low-power “motes,” PDAs, and PCs, and addresses the special robustness and security requirements of medical care settings.

#### 3.1 Potential For Impact

Wireless sensing and communication have the potential for broad applications in medicine. Sensor networks provide the technology to bridge the gap between patient load and available resources.

When faced with a large number of casualties, the goal is to first care for those patients who will benefit the most from trauma care and rapid surgical intervention. To accomplish this, EMTs can deploy wireless, low-power vital sign sensors to monitor severely injured patients. Using sensors, triage in the field and triage at the hospital can be made interactive by continuously feeding patient capacity information from a sensor network to a decision support system. Such an infrastructure would allow efficient matching of out-of-hospital caseload to critical, hospital-based trauma facilities and resources. The devices are capable of operating as active tags, storing information on a patient’s identity, status, history, and interventions, thereby obviating the need for back-end storage systems or paper charts. Moreover, the devices are significantly smaller than existing portable monitors, operate for months on a single pair of alkaline batteries, and completely eliminate wires. In addition, it is possible to track the location of these devices down to meter-level accuracy using ultrasound ranging or RF-localization strategies.

#### 3.2 CodeBlue: A Wireless Infrastructure For Emergency Response

Integration of low-power wireless devices into medical settings raises a number of novel challenges. Current demonstration systems operate with a small number of devices under fairly static conditions. Scaling up to handle a mass casualty scenario and ensuring robust operation with a high degree of mobility and minimal packet loss poses a number of open problems. We need to develop a wireless communications infrastructure for critical care environments. Wireless device is designed to provide routing, naming, discovery, and security for wireless medical sensors, PDAs, PCs, and other devices that may be used to monitor and treat patients in a range of medical settings. Also it should be designed to scale across a wide range of network densities, ranging from sparse clinic and hospital deployments to very dense, ad hoc deployments at a mass casualty site. It must also operate on a range of wireless devices, from resource-constrained motes to more powerful PDA and PC-class systems. **CodeBlue** offers a scalable, robust “information plane” for communication and across wireless medical devices. **CodeBlue** provides protocols and services for node naming, discovery, any-to-any ad hoc routing, authentication, and encryption. **CodeBlue** is based on a publish/subscribe model for data delivery, allowing sensing nodes to publish streams of vital signs, locations, and identities to which PDAs or PCs accessed by physicians and nurses can subscribe. To avoid network congestion and information overload, **CodeBlue** will support filtration and aggregation of events as they flow through the network. For example, physicians may specify that they should receive a full stream of data from a particular patient, but only critical changes in status for other patients on their watch. The use of ad hoc networking will allow the “mesh” of connectivity to extend across an entire building or between multiple, adjacent facilities. Additional coverage, if necessary, will be possible with placement of fixed nodes in hallways, rooms, or other areas. No matter the topology, the network will be self-organizing: loss of a given node or network link can be rapidly detected and data re-
routed accordingly. CodeBlue will also provide for reliable transmission of critical data through content-specific prioritization and dynamic scaling of transmission power.

IV. MANET FOR TELEMEDICINE SYSTEM

Telemedicine is defined as the delivery of medical health care and medical expertise using a combination of telecommunications technologies. Telemedicine systems can support applications ranging from video conferencing to providing diagnostics, high quality image and still-image, and medical database record. The system is based on three technologies viz., MIPv6, MANET, and WLAN. The integration of the technologies will produce a highly capable system with the ability to be rapidly deployed to support medical services. The requirements of the Tele-Emergency are:

1. Capable to work in remote areas, which has limited communications infrastructure
2. Capable of being deployed in emergency condition
3. Capable of managing electronic patient records,
4. Support by real-time multimedia communication and geographical information system (GIS).
5. Low operating cost.

V. MEDICAL APPLICATIONS OF THE FUTURE

Advances in wireless sensor networking have opened up new opportunities in healthcare systems. The future will see the integration of the abundance of existing specialized medical technology with pervasive, wireless networks. They will co-exist with the installed infrastructure, augmenting data collection and real-time response. Examples of areas in which future medical systems can benefit the most from wireless sensor networks are in-home assistance, smart nursing homes, and clinical trial and research augmentation. In home pervasive networks may assist residents by providing memory enhancement, control of home appliances, medical data lookup, and emergency communication. Unobtrusive, wearable sensors will allow vast amounts of data to be collected and mined for next generation clinical trials. Data will be collected and reported automatically, reducing the cost and inconvenience of regular visits to the physician.

5.1 CRITICAL DEVELOPMENT AREAS

5.1.1 Enabling Technologies For Future Medical Devices:
- Interoperability: As a result of the heterogeneity present in the system, communication between devices may occupy multiple bands and use different protocols. For example, motes use unlicensed bands for general telemetry or ISM equipment. Implanted medical devices may use a licensed band allocated for that purpose by the FCC. In order to avoid interference in the increasingly crowded unlicensed ISM band, biomedical devices may use the WMTS band. The homecare network must provide middleware interoperability between disparate devices, and support unique relationships among devices, such as implants and their outside controllers.
- Real-time data acquisition and analysis: The rate of collection of data is higher in this type of network than in many environmental studies. Efficient communication and processing

will be essential. Event ordering, time-stamping, synchronization, and quick response in emergency situations will all be required.
- Reliability and robustness: Sensors and other devices must operate with enough reliability to yield high-confidence data suitable for medical diagnosis and treatment.
- New node architectures: The integration of different types of sensors, RFID tags, and back-channel long-haul networks may necessitate new and modular node architectures.

5.1.2 Embedded, Real-Time, Networked System Infrastructures For Mdis:
- Patient and object tracking: Tracking can be considered at three levels: symbolic (e.g., Room No or X-Ray Lab); geographical (GPS coordinates of a patient on an assisted living campus); relational/associational. It is complicated by the presence of multiple patients, non-patient family members, and leaving the range of the home network.
- Communication amid obstructions and interference: In-building operation has more multi-path interference due to walls and other obstructions, breaking down the correlation between distance and connectivity even further. Unwanted emissions and glitching are likely to be rigorously restricted and even monitored due to safety concerns, particularly around traditional life-critical medical equipment.

- Multi-modal collaboration and energy conservation: Limited computational and radio communication capabilities require collaborative algorithms with energy-aware communication. Richly varied data will need to be correlated, mined, and altered. Heterogeneous devices will be on very different duty-cycles, from always-on wired-power units to tiny, stealthy, wearable units, making rendezvous for communication more difficult.
- Multi-tiered data management: Data may be aggregated and mined at multiple levels, from simple on-body filtering to cross-correlation and history compression in network storage nodes. Embedded real-time databases store data of interest and allow providers to query them.

5.1.3 Medical Practice-Driven Models And Requirements:
- Records and data privacy and security: Data collected by the network is sensitive, and ownership issues are not always clear. It is likely that the healthcare provider owns the sensor and network devices, yet the data pertain to the patient. Data must be available during emergencies, but access should leave a non-repudiable “trail,” so abuses can be detected. Any priority-override mechanisms must be carefully designed. One may want to filter out “privacy-contaminated” data, for example, a patient walks into the wrong room. The system should not “leak” this information through sensors being monitored in the room.
- Role-based access control and delegation in real-time: Doctors may delegate access privileges to other doctors and nurses; family members may monitor quality-of-care for nursing home residents. The system may have DRM-like issues: “read but not copy,” “view but not save,” etc. Also, patients may have read but...
not write privileges for the collected sensor data, in order to avoid fraud.

5.2 Next Generation Smart Homecare
We need a wireless sensor network architecture for smart homecare that possesses the essential elements of each of the future medical applications, namely:
- Integration with existing medical practices and technology.
- Real-time, long-term, remote monitoring.
- Miniature, wearable sensors, and
- Assistance to the elderly and chronic patients.
It extends healthcare from the traditional clinic or hospital setting to the patient’s home, enabling telecare without the prohibitive costs of retrofitting existing dwellings. Currently, patients visit doctors at regular intervals, self-reporting experienced symptoms, problems, and conditions. Doctors conduct various tests to arrive at a diagnosis and then must monitor patient progress throughout treatment. In smart homecare, the WSN collects data according to a physician’s specifications, removing some of the cognitive burden from the patient and providing a continuous record to assist diagnosis. In-home tasks are also made easier, for example, remote device control, medicine reminders, object location, and emergency communication. The architecture is multitiered, with both lightweight mobile components and more powerful stationary devices. Sensors are heterogeneous, and all integrate into the home network. Multiple patients and their resident family members are differentiated for sensing tasks and access privileges. Smart homecare benefits both the healthcare providers and their patients. Wearable sensor devices can sense even small changes in vital signals that humans might overlook, for example, heart rate and blood oxygen levels. Quickly notifying doctors of these changes may save human lives. The data collected from the wireless sensor network can be stored and integrated into a comprehensive health record of each patient, which helps physicians make more informed diagnoses. Eventually, the analyzing, diagnosis, treatment process may also be semi-automated. So a human physician can be assisted by an "electronic physician." Healthcare patients benefit from improved health as a result of faster diagnosis and treatment of diseases. Other quality-of-life issues, such as privacy, dignity, and convenience, are supported and enhanced by the ability to provide services in the patient’s own home. Family members and the smart homecare network itself become part of the healthcare team. Examples of envisioned missions where the WSNs can quickly make an impact are the following:

- **Sleep apnea.** Every night, monitor blood oxygenation, breathing, heart rate, EEG, and EOG using onbody sensors to assess severity and pattern of obstructive sleep apnea. Home network monitors agitation (movement) and stores and reports sensor data. Network alerts provider and patient if oxygenation falls below a threshold. Monitoring can continue while treatment efficacy is assessed.
- **Journaling support.** Journaling is a technique recommended for patients to help their physicians diagnose ailments like rheumatic diseases. Patients record changes in body functions (range of motion, pain, fatigue, sleep, headache, irritability, etc), and attempt to correlate them with environmental, behavioral, or pharmaceutical changes. The homecare network can aid patients by: providing a time synchronized channel for recording and transmitting the journal (PC, PDA, "dizziness" button); recording environmental data or external stimuli (temperature, barometric pressure, sunlight exposure, medication schedule); and quantitatively measuring changes in symptoms (pain, heart-rate, sleep disruption).
- **Cardiac health.** Cardiac arrhythmia is any change from the normal beating of the heart. Abnormal heart rhythms can cause the heart to be less efficient, and can cause symptoms such as dizziness, fainting, or fatigue. Since they are sometimes very brief, it can be difficult to properly characterize them. Cardiac stress tests attempt to induce the event while the patient is wearing sensors in a laboratory. In a homecare setting, wearable EKG sensors can monitor for the condition continuously, over days or weeks, until the event occurs. The recorded data is promptly sent to the physician for analysis. If the event is serious enough, the emergency communication channel may be used to call for help, or it may be dispatched automatically. Other sensors in the home may be able to record environmental data to help identify the cause (side-effect of medicine, little sleep, etc.). The dynamicity and variability of context and conditions make health-care environment very suitable for the use of mobile and wearable computing techniques. The use of small and portable devices can be very beneficial in terms of efficiency and vital support to patients. However, the many challenges that this environment presents need to be addressed, possibly by a general mobile computing framework that could be used in different mobile settings.

5.3 An Eye To The Future
The dynamicity and variability of context and conditions make health-care environment very suitable for the use of mobile and wearable computing techniques. The use of small and portable devices can be very beneficial in terms of efficiency and vital support to patients. To improve enterprise mobility we need an architecture, which should make healthcare deployments even more robust than before. It should optimizes voice performance and enables seamless campus-wide roaming across subnets without the need to re-authenticate. Highly scalable, Technology should offer enhanced security, including advanced intrusion detection tools, making it ideal for even the largest healthcare applications. In the future emerging technologies such as RFID will be supported on the same wireless switch that supports Wi-Fi today. RFID will enable applications such as location-based services and asset tracking, leading to improvements in customer services and supply chain management. Because each healthcare facility is unique, each wireless solution is a little different. But should best-of-breed clinical and administrative applications and comprehensive mobility solutions to meet the unique requirements of the healthcare industry, and your situation. Healthcare technology can help doctors and nurses improve the quality and efficiency of patient care, helping to reduce risk and save lives. Whether connecting patients to doctors on the move, scanning patient information bedside, making test results available immediately, reducing the risk of human error in the lab, pharmacy or donor center and ultimately, help elevate the quality of patient care to the highest standard.
VI. RESEARCH CHALLENGES

To achieve the level of robustness required for medical telemetry, significant research must be undertaken to design communication protocols, energy management schemes, and encryption algorithms appropriate to this domain.

Communication challenges: The first challenge is secure, reliable, ad hoc communication among groups of sensors and mobile, handheld devices. Unlike 802.11 networks, sensor networks are entirely self-organizing and operate with extremely limited energy and computational resources. To limit energy consumption it is desirable for nodes to minimize their transmit power to achieve acceptable connectivity without inducing network interference. In addition, the network must prioritize the transmission of critical data, such as a sudden change in patient status.

Computational challenges: Sensor nodes have very limited computational power, and traditional security and encryption techniques are not well-suited to this domain. System must allow physicians, nurses, and others to assign quickly access rights to patient data and to determine handoff credentials when a patient is transferred to another unit or hospital. Existing authentication systems are extremely rigid in this regard.

Programming challenges: Finally, coordination of a diverse array of sensors, active tags, handheld computers, and fixed terminals requires a cohesive communication and programming model to underlie the system’s operation. Existing software for sensor nodes is very low-level and does not provide higher-level services such as discovery, naming, security, and data delivery within a common framework. The goal is to develop a flexible protocol suite for integrating a range of wireless devices in a critical care setting.

VII. CONCLUSION

Wireless networking is an attractive and promising technology for health care. Wireless technology conceivably could become the essential enabler for the healthcare industry. However, wireless technology was not designed to support life-critical functions or to protect the confidentiality of individuals’ most personal and private information. So architectural and functional features necessary to protect confidentiality and patient safety are lacking. Healthcare providers today must carefully weigh the potential benefits against the most certain risks before implementing wireless networks.

REFERENCES