Developing next-generation Telehealth tools and technologies

Insup Lee
PREICSE Center
Department of Computer and Information Science
University of Pennsylvania

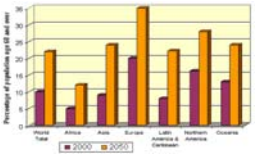
NIH Future of Telehealth Workshop
June 25, 2009

An Aging World

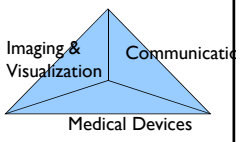
- Department of Health projects by 2050 over 20% of the population in U.S. will be above 65.

Consequences
- Acute **shortage** of trained medical professionals.
- **Reduced** healthcare delivery **coverage** .
- **Increase** in the medical **costs**.

Possible Solution
- Extend traditional delivery model, with:
  - Communication infrastructure
  - Devices facilitating remote checkup, surgery
  - Visualization and imaging tools
- Result: **Remote Monitoring models**
  - Telemedicine model
  - Centralized monitoring model



Source: *World Population Prospects, The 1998 Revision*, United Nations Secretariat



Telemedicine Today

Goals
- To **enhance** health care **delivery** to medically-underserved populations using telecommunication technology
- To **increase access** to **medical specialty** services while **decreasing** health care **costs**
- To provide ongoing **training** for preceptors, medical **students**, and residents.

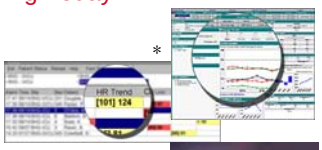
Features
- Medical facility based care.
- Connect participating medical facilities across large areas through high speed back-bone.
- Provide facilities for remote:
  - Patient checkup
  - Videoconferencing
  - Transfer of technology

AZ Telemedicine Initiative
Source: *AZ Telemedicine Initiative*

Centralized Monitoring Today

Applications
- Hospital based monitoring
- Secondary monitoring infrastructure

Features
- Patient Care Tools*
  - Patient Profile
  - Treatment Plan
  - Event Log
  - Physician note-writing capability
- Remote Health Management Tools*
  - Video-assessment
  - Remote Bedside Monitoring



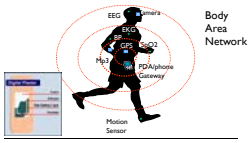
- Alerts*
  - Types
    - Patient Status Alerts
    - Care Issue Alerts
    - Process Reminder Alerts
    - Daily Management Reports
  - Patient Parameters monitored inclu
    - Heart rate (value, trend)
    - Mean Arterial Pressure (value, trend)
    - Inter-beat Interval (EKG)
    - O2 Saturation


Penn E-lert eICU*

* Source: Visicu Inc.'s eICU system (http://www.visicu.com/products/index.html)

Pervasive Health Management

Use ***Pervasive Computing*** for day-to-day healthcare management to enable ***real-time***, ***continuous*** patient monitoring



Body Area Network

Applications


Home-based Care


Sports Health Management


Disaster Relief Management


Medical Facility Management

Features
- ❖ **Extends remote monitoring model** by enabling:
  - ❖ Physical presence of caregivers required only during emergencies
  - ❖ Improved coverage and ease of monitoring
- ❖ Utilize in-vivo and in-vitro **medical sensors**
- ❖ ***Mobile*** patients. **No time & space restrictions** for health monitoring
- ❖ Better **quality of care** and reduced medical errors
- ❖ **Early detection** of ailments and actuation through automated health data analysis

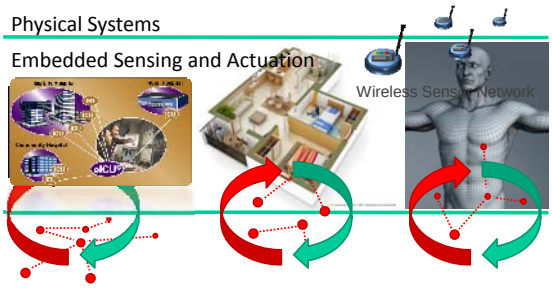
Key Trends in Telehealth Systems

- System Complexity
  - Increasing functionality
  - Increasing integration and networking interoperability
  - Growing importance and reliance on software
  - QoS is no less important than functionality
- Nature of tomorrow's systems
  - Dynamic, ever-changing, dependable, high-confidence
  - System of systems – scale & interoperability
  - Self-*(aware, adapting, repairing, sustaining)
- Cyber Physical Systems

Interacting With Physical World

Physical Systems

Embedded Sensing and Actuation



Cyber-Physical Systems (CPS)

Software, the Great Enabler

- Good news: anything is possible in software!
- Bad news: anything is possible in software!

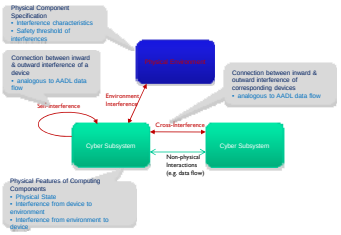
- It is the software that affects system complexity and also cost.
  - Software development stands for 70-80 % of the overall development cost for some embedded systems
- Need software development methods that keep complexity under control
  - Model-driven approaches
  - Compositionality

Interaction Complexity

- Telehealth systems are systems of systems.
- Composition of systems are about the interactions of systems.
  - Some interactions are unintended and unanticipated
    - Interoperability
    - Emerging behaviors
  - Mixed criticality
- "Normal Accidents", an influential book by Charles Perrow (1984)
  - One of the Three Mile Island investigators
  - And a member of recent NRC Study "Software for Dependable Systems: Sufficient Evidence?"
  - A sociologist, not a computer scientist
- Posits that sufficiently complex systems can produce accidents without a simple cause due to
  - interactive complexity and tight coupling

Interference

- Telehealth systems have implanted or worn sensors/devices on the human body.
- Sensor activity causes heating in the tissue.
  - Heating caused by RF inductive powering
  - Radiation from wireless communication
  - Power dissipation of circuitry
- Needs:
  - Interference awareness in BSN design and deployment
  - Safety analysis akin to cyber-physical system
  - Model based approach



Need for formal safety analysis methods for future Telehealth systems

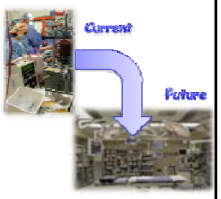
Needs for telehealth systems

- Integration techniques for systems of systems
  - Interoperation of medical devices, EHR systems, ...
  - High-confidence systems
- Secure, dependable, real-time communication networks
  - QoS guaranteed Internet service
  - Interference-resilient wireless networks
- Validation and Evidence-based certification
  - Incremental certification
  - Model-based development
  - COTS (Commercial-off-the-shelf) components

Interoperability

Characteristics

- Over the years medical devices gaining communication capabilities
- Devices still operate independently
- Standardized interaction between devices non existent
- Full benefit of communication capabilities not being realize



Advantages

- Improve Patient safety
- Complete, accurate medical records
- Reduce errors
- Context awareness
- Rapid deployment
- Safety interlocks

Interoperable medical devices based on plug-n-play!

Vender neutrality based on virtualization (virtual medical device interfaces)

Security, Privacy & Trust

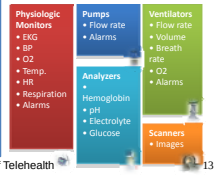
Security is essential for Telehealth Technologies

Current State

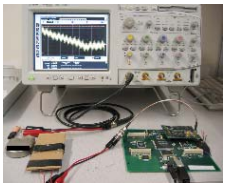
- Sensors and devices storing more personal/sensitive health information
- Sensors and devices are wireless with increasing access range
- Increasing complexity of sensors and devices leading to bugs (software/hardware)
- Substantial increase in deployment - greater incentive for attack
- Connecting to existing IT infrastructure (Internet) for easy access
- Use of COTS software, Improper configurations
- HIPAA requirement if personally identifiable information

Medical devices today, either do not have any inbuilt security features or have proprietary features which are not disclosed.

sensitive information collected



Pacemaker Hacking Example



Researchers working with an implantable cardiac defibrillator were able to remotely read telemetry data and reprogram the device.

These devices currently have no safeguards beyond an unpublished, proprietary interface.

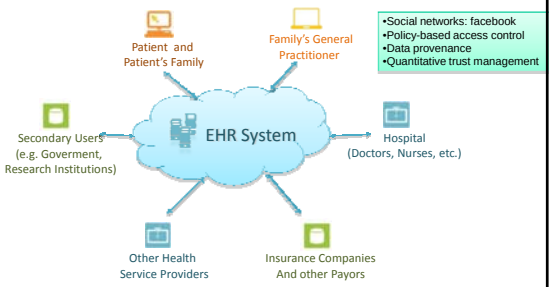
Besides the obvious physical hazards, there are also privacy implications.

- "To our knowledge there has not been a single reported incident of such an event in more than 30 years of device telemetry use, which includes millions of implants worldwide," a Medtronic spokesman, Robert Clark, said.
- St. Jude Medical, the third major defibrillator company, said it used "proprietary techniques" to protect the security of its implants and had not heard of any unauthorized or illegal manipulation of them.
  http://www.nytimes.com/2008/03/12/business/12heart-web.html?ref=business

Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses

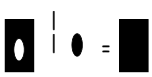
Daniel Halperin, Thomas S. Heydt-Benjamin, Benjamin Ransford, Shane S. Clark, Benessa Defend, Will Morgan, Kevin Fu, Tadayoshi Kohno, and William H. Maisel
IEEE Symposium on Security and Privacy, May 2008

Security, Privacy & Trust



Assurance and Certification

- How do we provide assurance that we've done so?
  - All assurance is based on arguments that purport to justify certain claims, based on documented evidence
- There are two approaches to assurance: implicit (standards based), and explicit (goal-based)
- Science of Certification
  - Certification is ultimately a judgment that a system is adequately safe/secure/whatever for a given application in a given environment
  - But the judgment should be based on as much explicit and credible evidence as possible
  - Incremental Certification
  - A Science of Certification would be about ways to develop that evidence



Challenges in telehealth systems

- Interoperability, Heterogeneity, Scale
- Validation and certification
- Security & privacy, Trust management
- Usability – physical, logical
- Open
- Costs

Recommendations

- R&D in Interoperability of Telehealth Systems
  - Interface technologies and tools based on formal methods
  - Open requirements, device interfaces, prototypes
  - Platform independent telehealth systems
    - Interface standards
    - Virtualization
- R&D for Security, Privacy and Trust Management of Telehealth Systems
  - Must be considered from the beginning
- Open testbeds to facilitate collaborations among stakeholders
  - caregivers, biomedical engineers, computer scientists, developers, regulatory agency,…

Acknowledgements

- Some slides are based on materials from
  - Sandeep Gupta, PhD (ASU)
  - Jack Stankovic, PhD (UVA)
  - Bill Hanson, MD (UPHS)
  - Margaret Fortino-Mullen, MSN,RN (UPHS)

END.