Privacy and Security Considerations in Real-Time Remote Healthcare Delivery

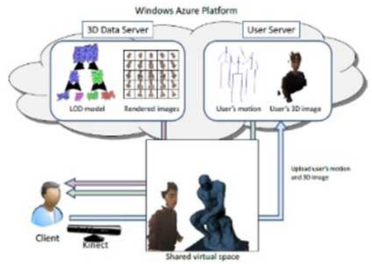
Dr. Gregorij Kurillo

Teleimmersion Lab
University of California, Berkeley

gregorij@eecs.berkeley.edu

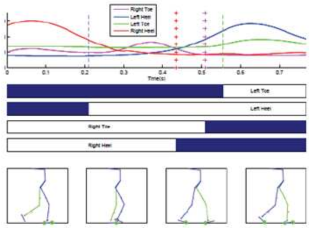
UC Berkeley - Teleimmersion Lab

- Exploring Teleimmersion technology for **collaborative work** of geographically distributed users through **virtual presence**
- Real-time observations and modeling of human movement dynamics
- Our research combines **3D computer vision**, **collaborative virtual reality** and **networking**

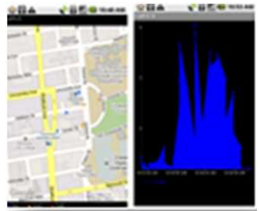


Access of Large Data
(UCB, Uni. of Tokyo)

Automotive Safety
(UCB, UCB ME)



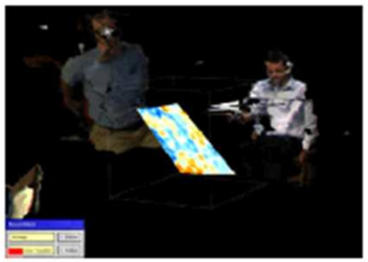
Modeling of Walking
(UCB, UT)



Mobile Technologies
(UCB, USB SPH)

Immersive Tai Chi
(UCB, Stanford Univ.)

Remote Dancing
(UCB, UIUC)



Virtual Geology
(UCB, UC Davis)

Virtual Archaeology
(UCB, UC Merced)

Tele-Medicine
(UCB, UC Davis)

Outline

- Motivation
- Remote Healthcare delivery
- Sensor technology
- Our Tele-healthcare projects
- Proposed solutions
- Conclusion

Motivation

- We are witnessing conjunction between **Information Technology**, **Communication** and **Healthcare**
- Use of **wireless personal computing** (i.e. smart phones) and **health-monitoring** devices is increasing

BASIS Watch
https://mybasis.com/

Fitbit Ultra
http://www.fitbit.com/

BioHarness BT
http://www.zephyr-technology.com

Nike FuelBand
http://www.nike.com/fuelband/

BodyMedia Link Armband
http://www.bodymedia.com

Motivation

- Devices are becoming increasingly **connected**
- There are security and privacy issues in **remote healthcare delivery** with respect to:
  - Data collection
  - Communication protocols
  - Data storage
  - Data analysis
  - Data sharing…
- What and how much do you share with whom?
  - Family, Parents, Children, Physician, Insurance…

Introduction

- Majority of research in healthcare privacy and security is in data encryption and access control of already stored data
- We are interested in privacy & security issues pertaining to **human observations in real time**
- In tele-health delivery, there are **heterogeneous sensor networks**. Challenge is how to ensure calibration, synchronization, validity of data, and privacy controls within the same framework.

Remote Healthcare Delivery through Heterogeneous Sensors

- Tele-healthcare:
  - Real-time interaction between patient & doctor
    - Video & audio … teleconference, consultation, remote office visit
    - Therapy & exercise … tele-rehabilitation
  - Real-time monitoring of patient's activity (with data analysis and storage):
    - EKG/ECG, EMG, heart-rate … body function
    - GPS … location (e.g. are you walking uphill, are you on busy street)
    - Accelerometry … activity levels
    - Questioners … can be triggered by other sensors to request patient's input

Sensor Technologies

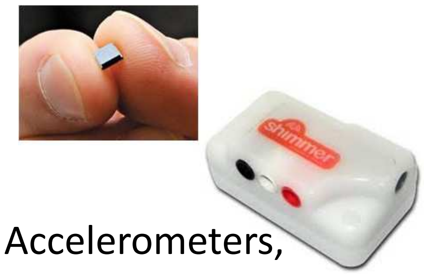
Video

Cameras
(wireless, wired,
Security, mobile…)

Audio

Microphones

Movement

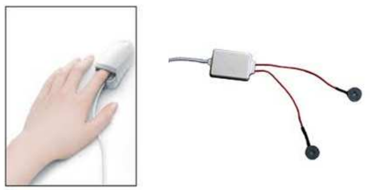


Accelerometers,
Gyroscopes,
GPS…

Multimedia Devices

Video, audio, 3D,
GPS, accelerometers,
Gyroscopes…

Body Functions



EKG/ECG, EMG,
Skin conductivity…

Other Sensors

Motion, pressure...

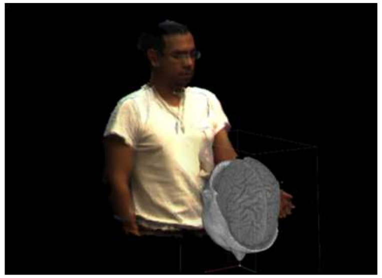
Privacy Considerations in Heterogeneous Sensor Systems

- If the user does not feel privacy is respected, they will less likely embrace the technology
- Users should be involved in the design phase to understand the privacy needs
- Tele-healthcare development should:
  - Include visibility and transparency of the processes
  - Provide education of users on how the system operates
  - Maximize both privacy and functionality

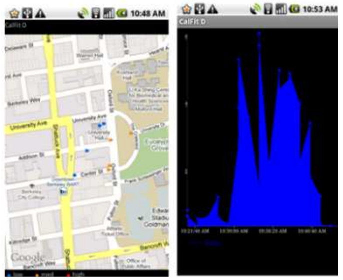
Privacy Considerations in Heterogeneous Sensor Systems

- Video and audio data is considered most revealing
- Computer vision algorithms can extract even mode from the data (e.g. person detection, face recognition, accurate tracking, activity recognition)
- Combination of sensors – **data fusion**, can reveal even more information that is by itself out of context (e.g. human daily activity recognition – time synchronized and geo-referenced)

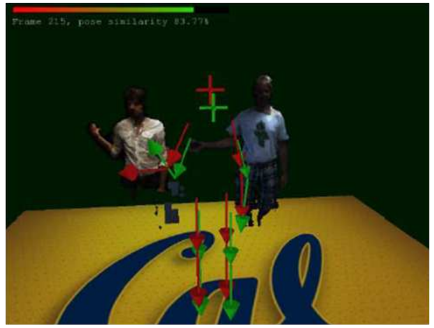
Teleimmersion Lab Healthcare Projects



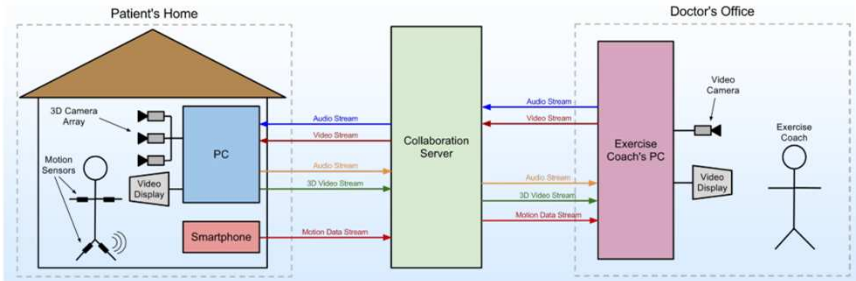
Remote Consultation & Medical Data Visualization
(Collaboration with IDAV, UC Davis)



Wireless/Mobile Sensor Monitoring of Activity



Remote delivery of physical therapy
(Collaboration with UC Davis Medical Center, CITRIS grant)



TeleHealth Network Architecture

Consensus from multiple specialists
(Collaboration with Kaiser Permanente)

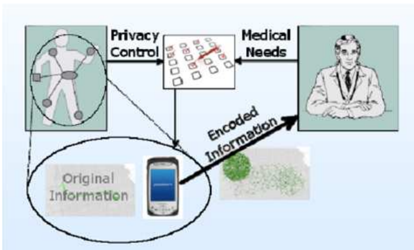
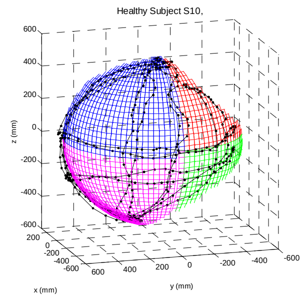


Figure 2: The Problem: Encoding the information

Data Privacy & Security



Upper Extremity Evaluation
(Collaboration with UC Davis Medical Center)

Motion Capture & Exercise Evaluation
(Collaboration with Oregon Health & Science University, NSF #1111965)

DexterNet

- An **open platform** for heterogeneous body sensor networks
- Project between UC Berkeley, Cornell University, Telecom Italia, UT Dallas, Tampere University of Technology- Finland
- Features **three-layer architecture** to control heterogeneous body sensors:
  - Body sensor layer (BSL) …
    design of sensors on the body
  - Personal network layer (PNL) …
    sensors on single subject communication
  - Global network layer (GNL) …
    multiple PNLs communication with
    remote Internet server

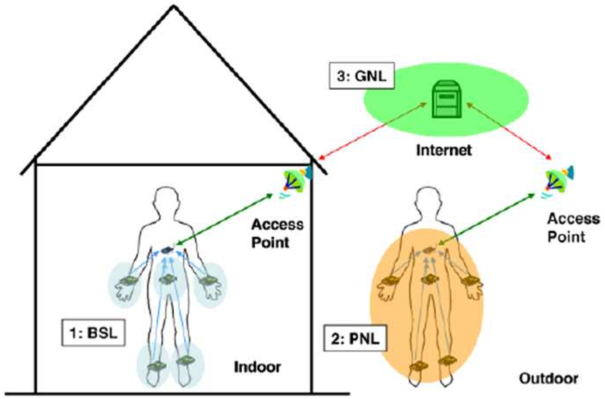
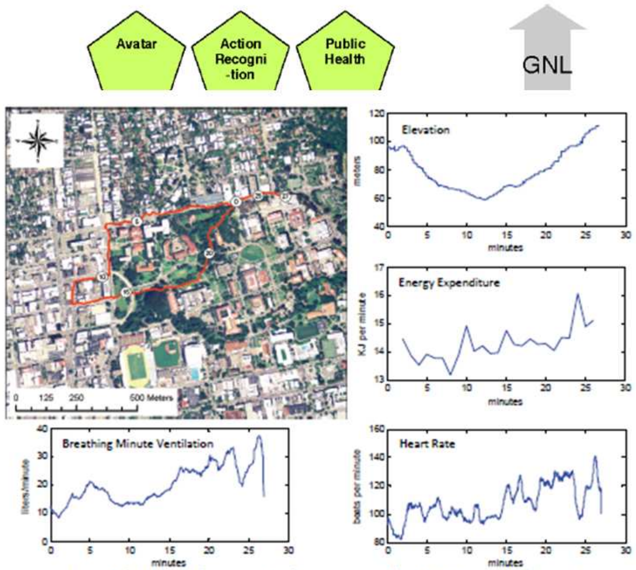


Figure 1. The three-layer hierarchy of the DexterNet system: 1. Body sensor layer (BSL). 2. Personal network layer (PNL). 3. Global network layer (GNL).

Kuryloski, P.; Giani, A.; Giannantonio, R.; Gilani, K.; Gravina, R.; Seppa, V.-P.; Seto, E.; Shia, V.; Wang, C.; Yan, P.; Yang, A.Y.; Hyttinen, J.; Sastry, S.; Wicker, S.; Bajcsy, R.; , "DexterNet: An Open Platform for Heterogeneous Body Sensor Networks and its Applications," Wearable and Implantable Body Sensor Networks, 2009. BSN 2009. Sixth International Workshop on , vol., no., pp.92-97, 3-5 June 2009

DexterNet

- DexterNet presents a competitive framework to support a variety of applications in healthcare, military, and consumer electronics.
- Architecture implemented **higher-level algorithms**:
  - Fall detection
  - Breathing volume
  - Energy expenditure
  - Recognition of 13 action categories
    (e.g. stand, sit, lie down, walk,
    go upstairs, jump, push wheelchair…)
- Geo-referenced multi-sensor data

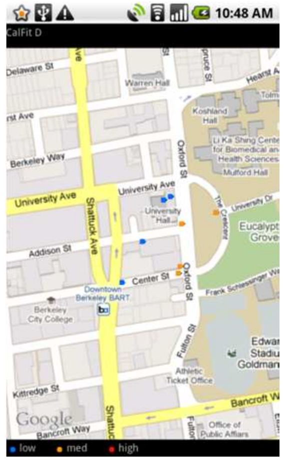


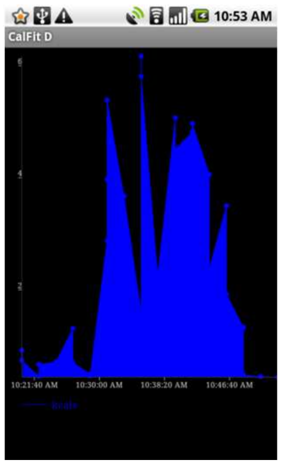
less tablet) and associated sensors. The GNL includes our applications built with the DexterNet system.

Kuryloski, P.; Giani, A.; Giannantonio, R.; Gilani, K.; Gravina, R.; Seppa, V.-P.; Seto, E.; Shia, V.; Wang, C.; Yan, P.; Yang, A.Y.; Hyttinen, J.; Sastry, S.; Wicker, S.; Bajcsy, R.; , "DexterNet: An Open Platform for Heterogeneous Body Sensor Networks and its Applications," Wearable and Implantable Body Sensor Networks, 2009. BSN 2009. Sixth International Workshop on , vol., no., pp.92-97, 3-5 June 2009

CalFit (BerkeleyFit)

- CalFit, a **multi-user mobile application**
- Monitors physical activity and encourages exercise through social interaction and competition.
- Collaboration between UC Berkeley Engineering and the School of Public Health
- CalFit aims to fulfill two goals:
  - to promote healthier and more active lifestyles
  - to provide data on social and physical environments (important for future health policies and planning)





Yan, P.; Lin, I.; Roy, M.; Seto, E.; Wang, C.; Bajcsy, R.; , "WAVE and CalFit — Towards social interaction in mobile body sensor networks," Wireless Internet Conference (WICON), 2010 The 5th Annual ICST , vol., no., pp.1-2, 1-3 March 2010

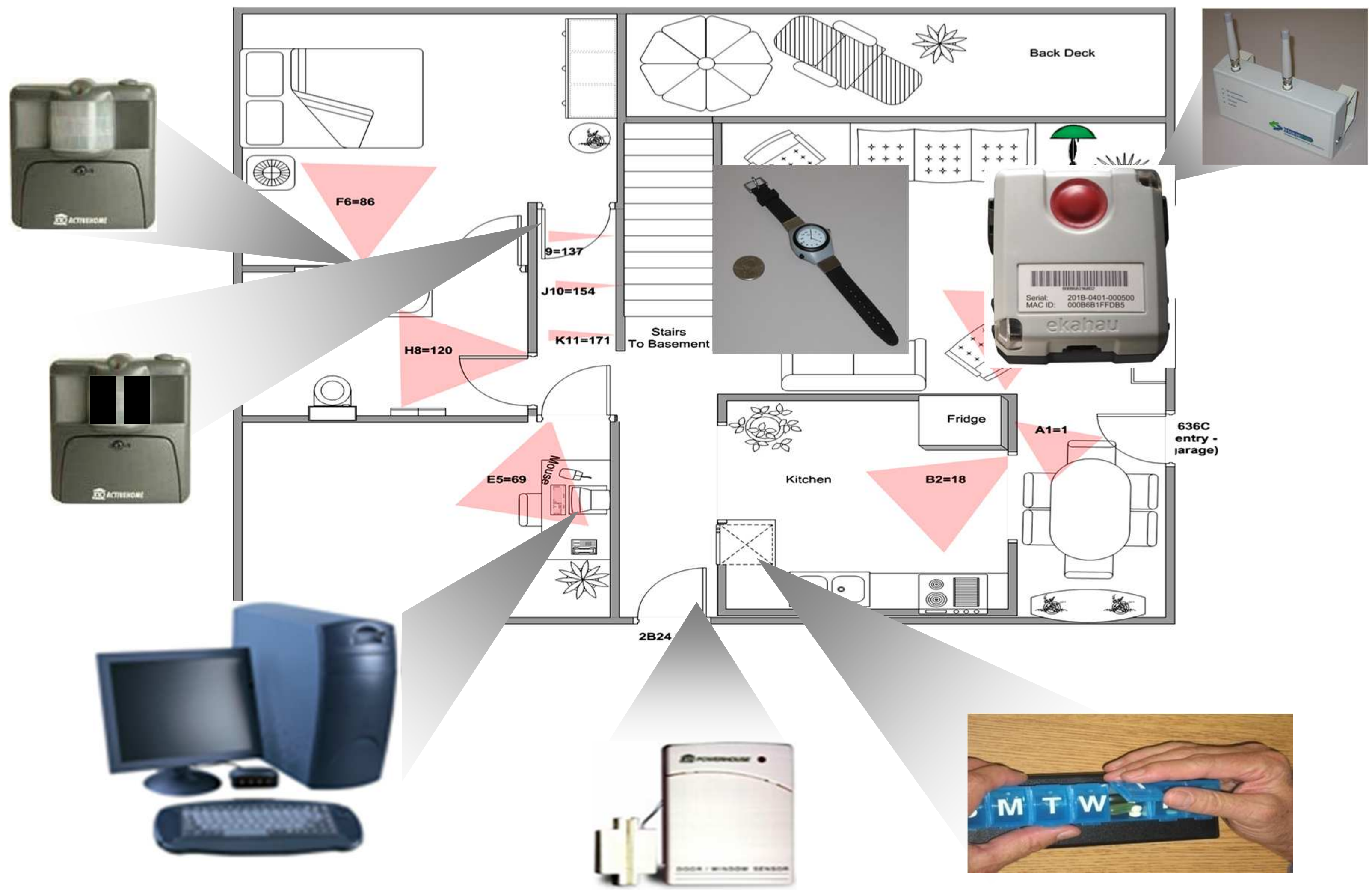
DexterNet & CalFit

- **Privacy & Security considerations:**
  - Location information is collected with relatively high accuracy
  - Several action categories are detected from the smartphone data in your pocket
  - Data is geo-referenced and time synchronized
  - Activity and location data is shared with others as in a social network

Smart Healthcare for Older Adults

Integrated Communications and Inference Systems for Continuous Coordinated Care of Older Adults in the Home

- Millions of **elderly people** live alone and do not take proper care of their physical health.
- **Wireless and other sensors** in home can be used to **observe** cognitive behavior and physical activity.
- National Science Foundation (NSF) sponsored project to **investigate and model cognitive and physical performance** in elderly.
- Partner: **Oregon Health Science University: Center for Health & Healing.**
- Privacy models for the sharing of home monitoring data



Holly Jimison, OHSU

Smart Healthcare for Older Adults

- **Privacy & Security considerations**:
  - Patients are monitored by various sensors 24/7
  - Information is being collected on computer usage, phone, Skype etc.
  - Data is used to provide semi-automated cognitive and physical health coaching
  - A lot of information is sensitive.
  - The goal is to understand what data subjects are willing to share and with whom

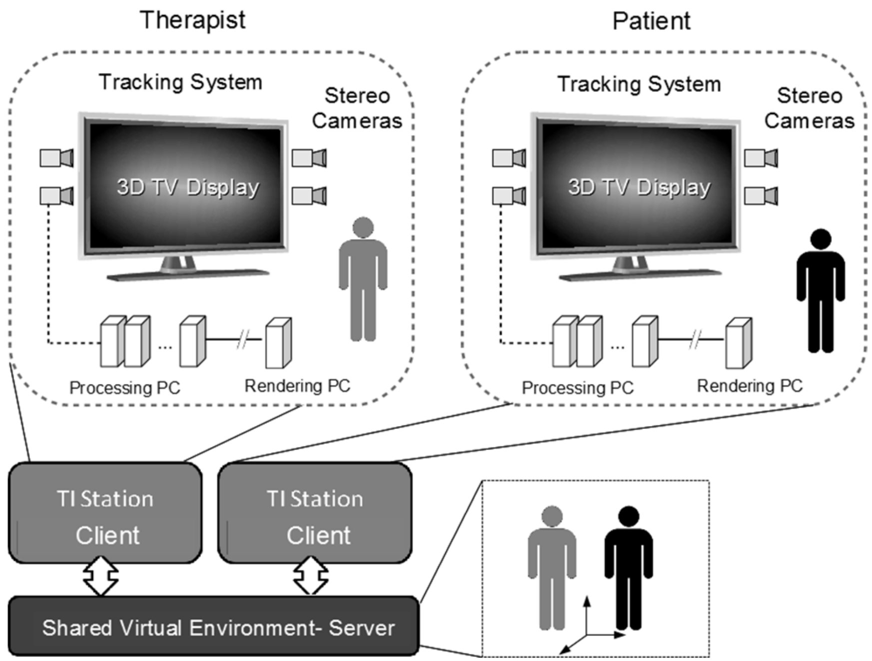
Smart Healthcare for Older Adults

Physical Health Coaching

- Technology assisted interactive exercise with Microsoft Kinect camera
- Movement data is collected and analyzed in real-time
- Real-time interaction between subject and coach on daily basis

Delivery of Remote Healthcare through Teleimmersion

- Tele-immersion connects remote users through a shared 3D virtual environment
- Communication through 3D video
- Use of real-time 3D imaging for observing, recognizing and measuring human movement
- Implementation of security and privacy measures to protect patient and ensure robust delivery



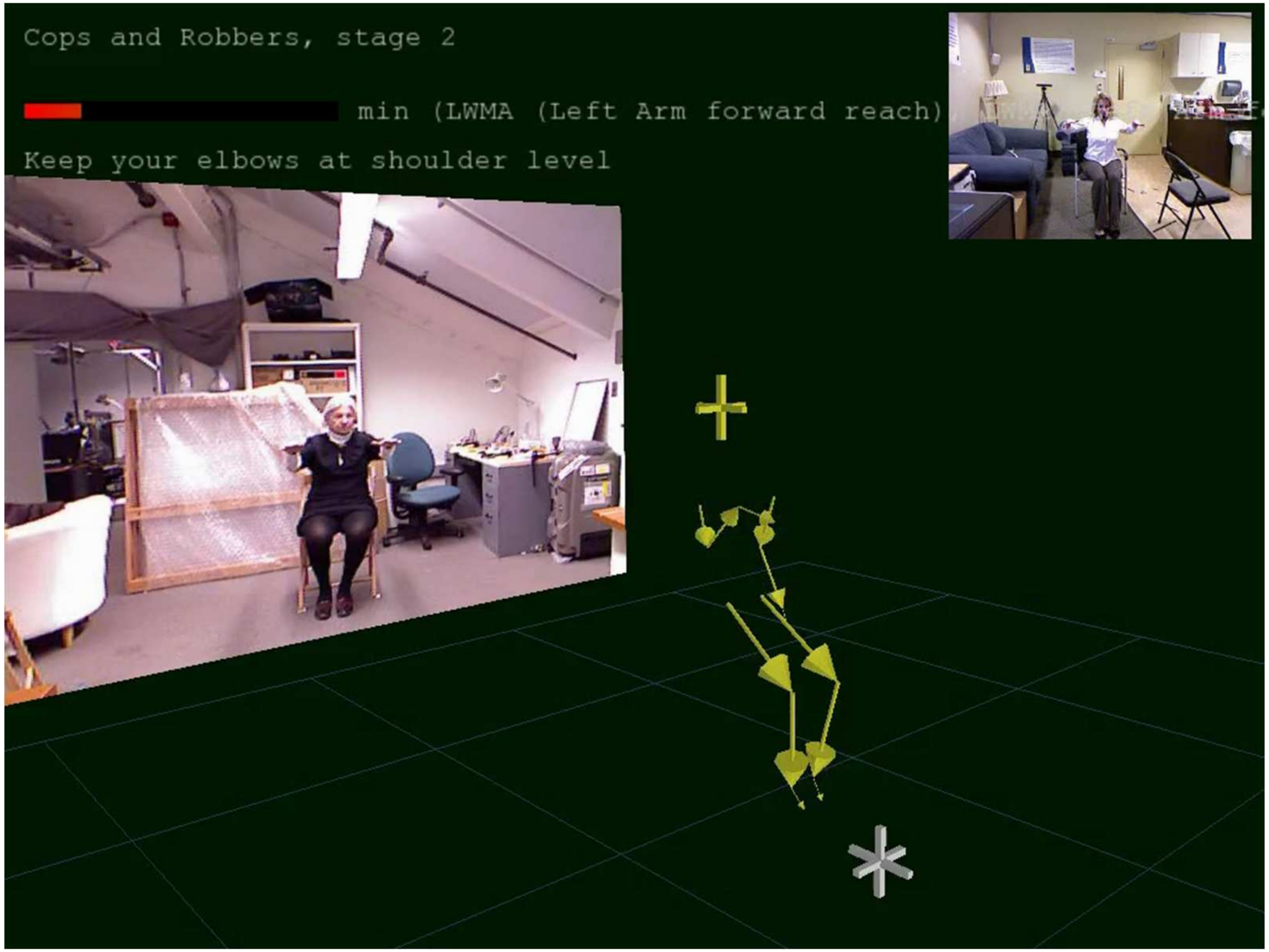
Smart Healthcare for Older Adults

Physical Health Coaching

- Kinect is used to provide tracking information on individual’s exercises from 3D image
- Higher-level features (based on joint angles and positions) are extracted in real-time based on predefined exercise routine
- These features provide performance measures, describing individual’s levels of endurance, strength, balance and flexibility.

Smart Healthcare for Older Adults

Physical Health Coaching



Smart Healthcare for Older Adults

Physical Health Coaching

- **Privacy & Security considerations:**
  - Elderly are considered vulnerable population, especially with respect to new technology
  - Video & audio is captured in person's home
  - 3D data is collected (e.g. body geometry, weight)
  - Body tracking data is being collected (e.g. action recognition, style
  - Objective information on subjects physical state is available.

TeleHealth: Remote Office Visit

- Collaboration with Kaiser Permanente Oakland
- In this scenario patient connects via a multimedia link to talk to doctor from home
- From technological point of view, this is trivial
- Privacy and security of data are crucial
- Can we use off-the-shelf technologies?

Remote consultation

Consensus from multiple specialists

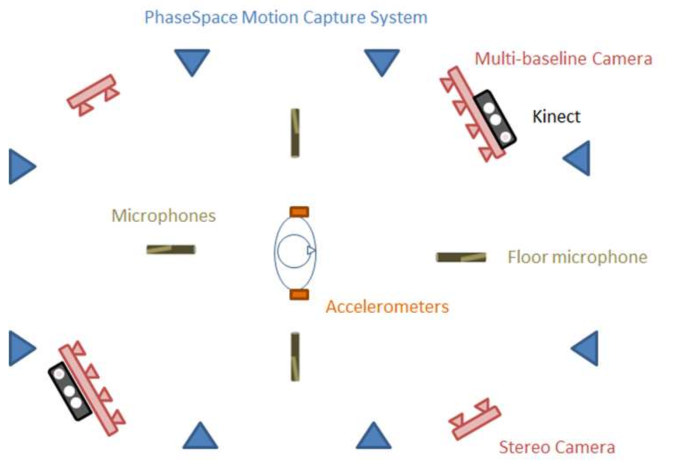
Remote office visit

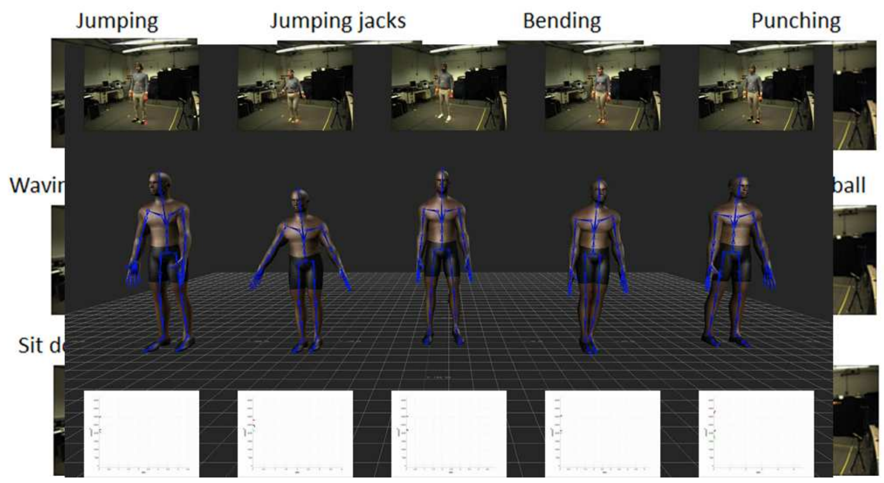
TeleHealth: Remote office visit & consensus from multiple specialists

- Remote office visit allows patient to be "seen" without travel, e.g. orthopedics
- Physician may need to perform remote visual assessment (e.g. ask patient to move limbs)
- Video quality (resolution, frame rate), camera positioning are important
- Technology would allow multiple geographically distributed physicians to observe/evaluate patient at the same time

Multimodal Human Activity Database

- Multimodal data collection facility:
  - Motion capture
  - Multi-view stereo
  - Accelerometers
  - Sound
- 12 actions, 11 subjects, 5 repetitions
- Large amount of data for motion analysis, segmentation, recognition etc.
- Exploring activity recognition from various modalities





Patient-Controlled Privacy of Real-Time Data

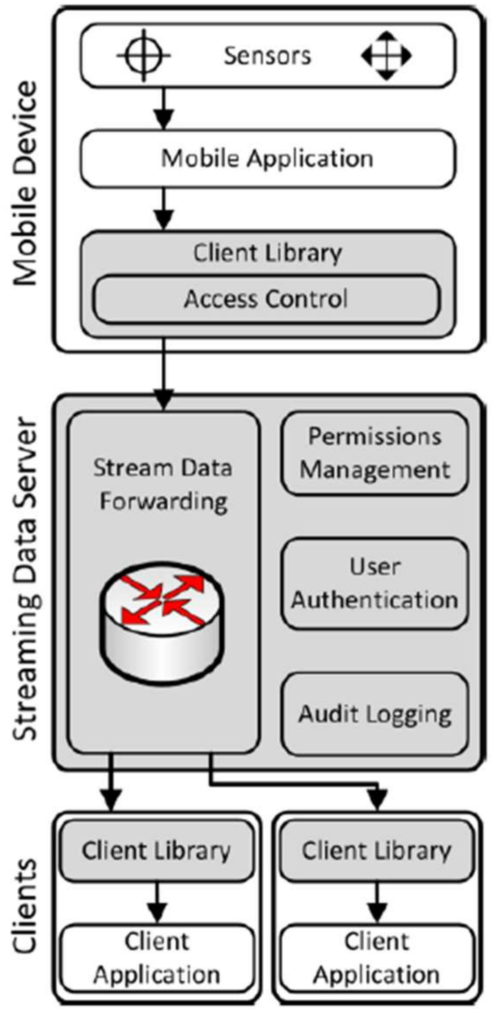
- **Challenges in real-time data collection**:
  - Multiple heterogeneous sensors streams (e.g. video, audio and other data)
  - Data access requires low latency for real-time interaction (e.g. in home monitoring, tele-rehabilitation)
  - Access control model for static data repository does not work.
  - Should raw data be stored on third-party system?
  - Who is the owner of the data?

Architecture for Patient-Controlled Privacy of Real-Time Data

- **Privacy Principles**:
  - User should have ultimate control of their data
  - The control should be at the device level
  - The resolution of the data is set by user
  - Framework should allow generating data at different granularities to each recipient
  - Data, which user choose not to share, is discarded
  - Authentication of users and devices
  - Audit logging of data access and permission settings

Architecture for Patient-Controlled Privacy of Real-Time Data

- Client-server architecture:
  - Client Library: facilitates r/w access to data streams
  - Streaming Data Server: provides interconnection point for clients
- Data streams are forwarded to each recipient in real time
- Access control is applied on the client side (device level)



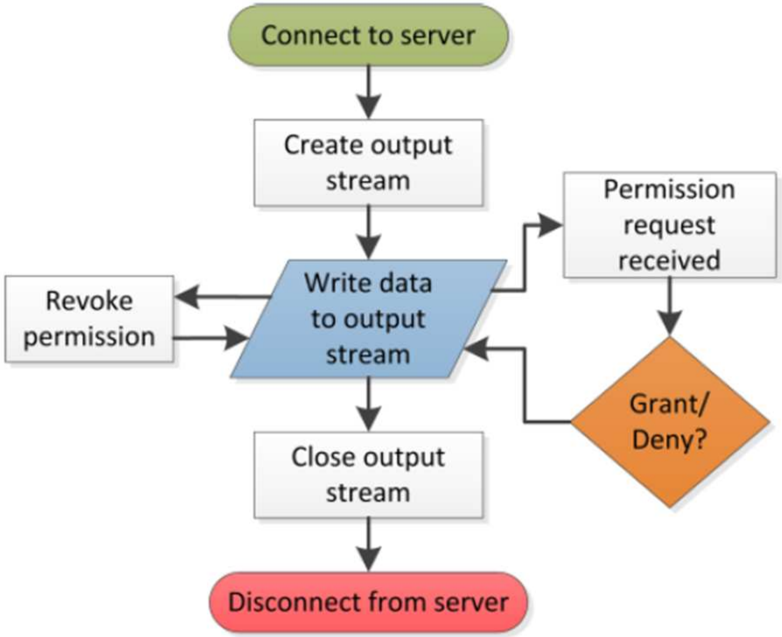
Client Library

- Provides simple API for device to access network:
  - Opening/closing sockets
  - Managing IP addresses
  - Sending/receiving control and data packets
- Telehealth applications interact with a simple abstraction of the network
- Client can accept, deny or revoke requests for data streams
- Implementation in Java and Python on PC and Android device, C++ to follow

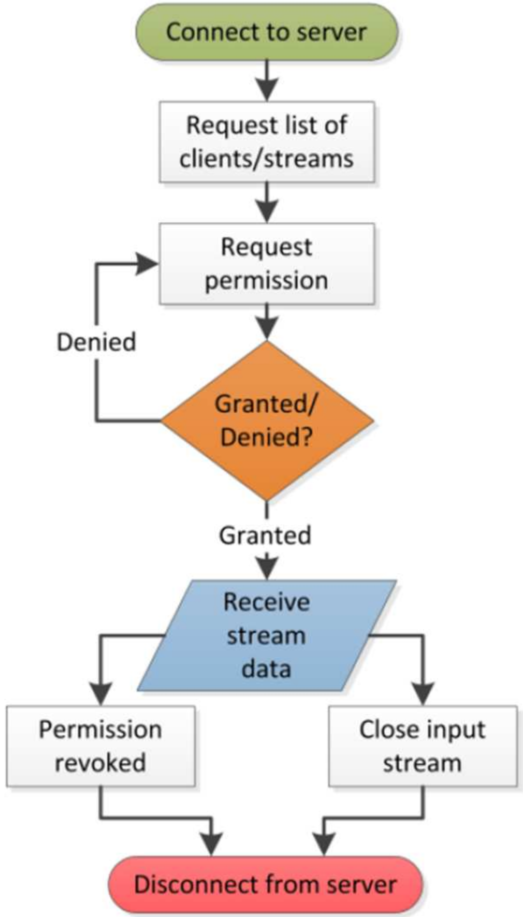
Streaming Data Server

- Provides a common point of contact for networked clients with authentication and logging mechanisms
- Key functions:
  - Receiving and forwarding of data streams based on permissions controls
  - Maintains list of valid user credentials
  - Maintains a log of connected clients and streams for audit
- Standardized and descriptive XML header describing sensor parameters (type, settings, resolution) for abstraction
- Implementation in Java

Architecture Protocol

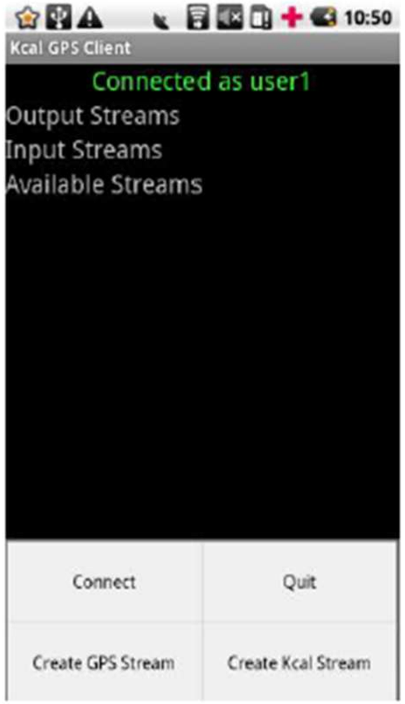


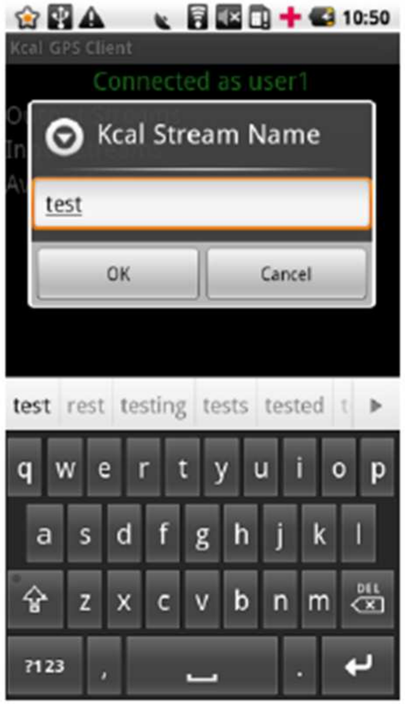
Flow diagram for sending client



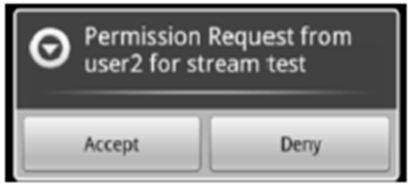
Flow diagram for receiving client

Test Application – kcal Streaming

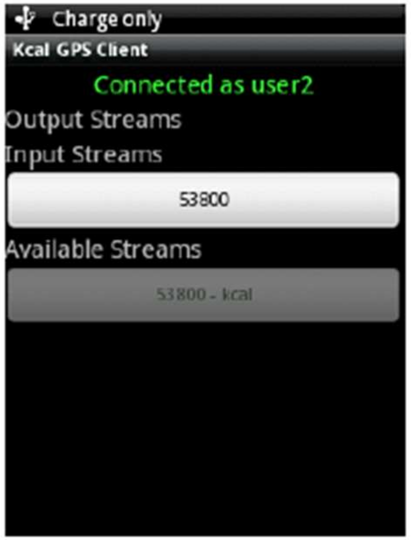


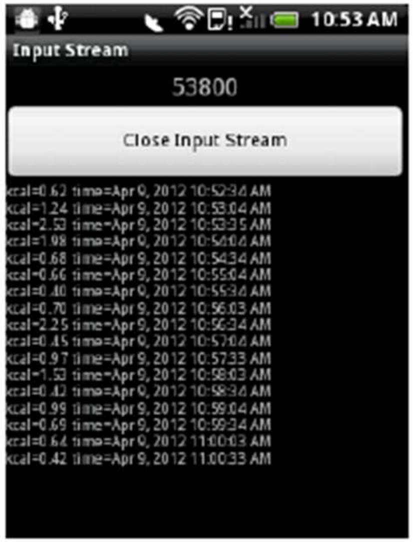


Test Application – kcal Streaming

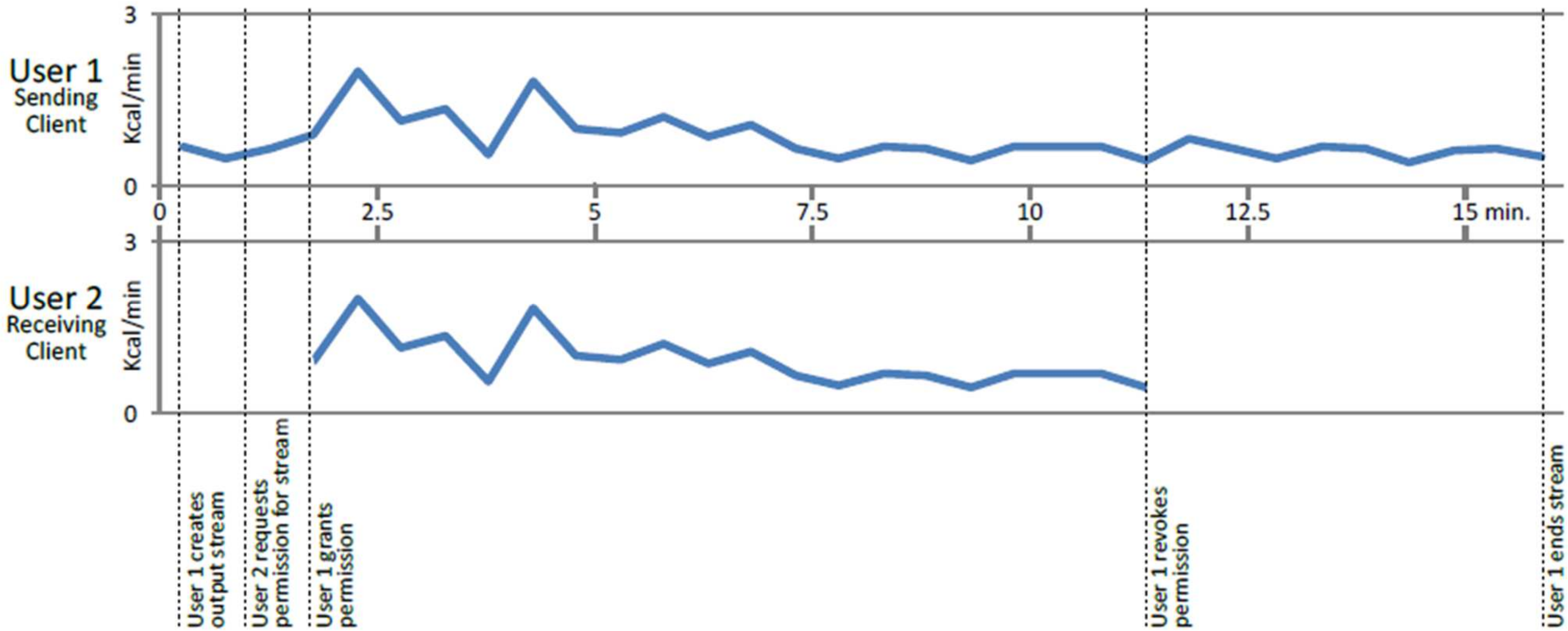


Test Application – kcal Streaming





Test Application – kcal Streaming



Framework - Summary

- Framework creates permission model for real-time data streaming across multiple platforms (PC, Android)
- Data flow is controlled close to the source (sensor)
- Users are able to control granularity of data received by different clients
- Abstraction of device output streams (application requests type of stream, does not care about sensor)
- The framework allows reliable, secure connectivity in a variety of network environments

A Game Theoretic Approach to TeleHealthcare

- Patients have **sensors** attached to their bodies/in their environment gathering measurements and **sending data** to a doctor/hospital
- We need to make sure that the data being sent complies with the patients' **privacy preferences** but is enough for doctors to **provide healthcare**
- Defining a **game** in which we have the three players: The **P**atient, The **H**ospital and The **D**evice. Each player has one move which represents their decisions/preferences.

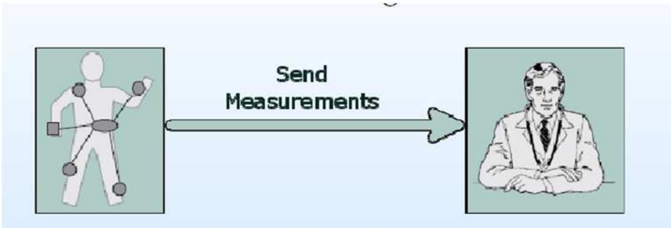


Figure 1: The Setting

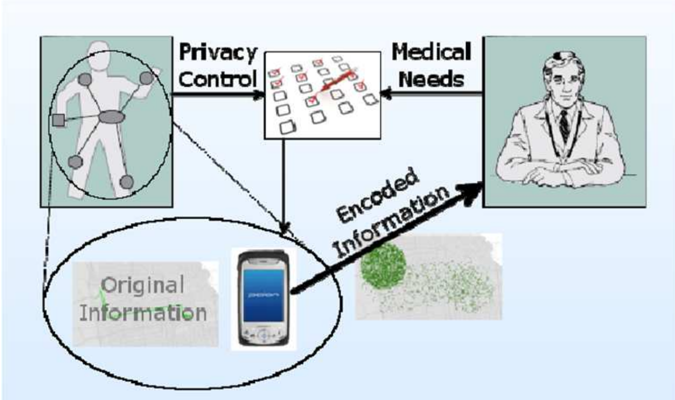


Figure 2: The Problem: Encoding the information

Daniel Aranki, UCB

Information bargaining

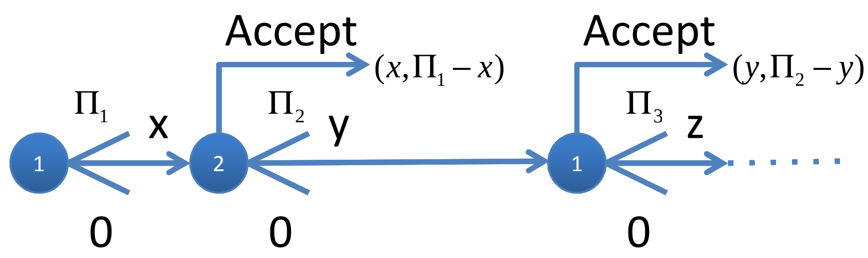
- Model the Doctor-Patient dynamics in the process of bargaining for information
  - Patients and doctors have mutual payoff but individual costs for each information partition x
    - **Mutual payoff**: good treatment
    - Patients may not want to share all their medical information with doctors because of potential cost in case the information gets compromised
    - Doctors may have a cost for receiving information: liability, misleading irrelevant information, etc…

The Problem

- The goal is to find the policy of sending measurements/information that produces minimal level of dissatisfaction
- Encoding information includes:
  - sending partial data
  - adding noise to the data
  - sending peaks or average …

Approach

- In the Rubinstein bargaining model:
  - Starts with player 1 making an offer
  - Alternating offers until a player accepts the other's offer
- **Assumption 1** [Rubinstein [1] (A-1)]: At any given round of the game
  - If x>y then Player 1 will prefer the partition x over the partition y
  - If x<y then Player 2 will prefer the partition x over the partition y
- In our medical setting, this assumption usually doesn't hold.
  - Relax the assumption

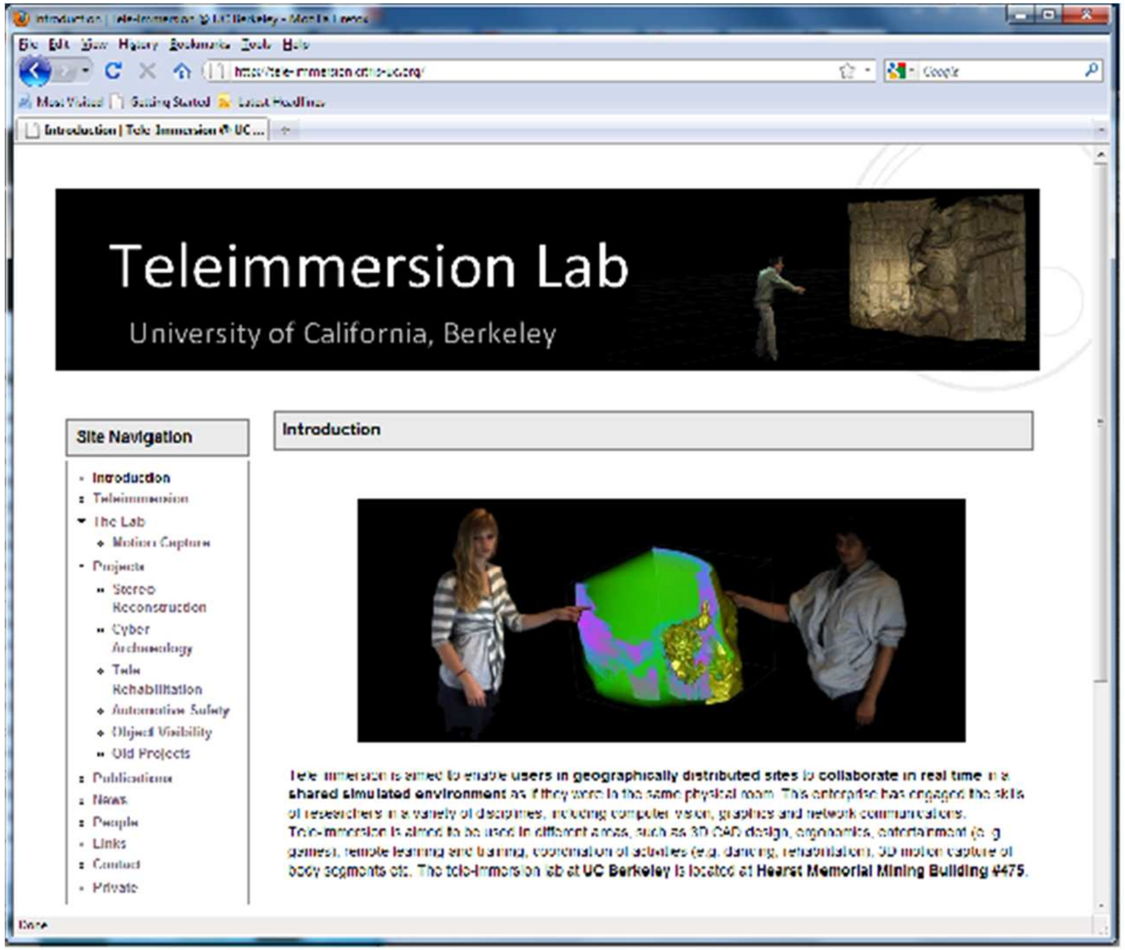


Conclusion

- Use of wearable and environmental sensors in healthcare can:
  - Reduce cost through prevention
  - Improve clinical outcomes
  - Facilitate independence of living
- Continuous data collection is required for the above -> significant privacy risks
- In real-time data collection users should have control over what data is collected, when and who is the reciever

Acknowledgements

- This work was partially supported by grants:
  - SHARPS Grant, HHS 90TR0003/01
  - National Science Foundation (NSF) Grant #1111965
  - TRUST
  - Center for Information Technology Research in Interest of Society (CITRIS), Seed Grant



http://tele-immersion.citris-uc.org
gregorij@eecs.berkeley.edu