Body Area Network Security: Robust Secret Sharing

Sang-Yoon Chang, Yih-Chun Hu,
Hans Anderson, Ting Fu, Evelyn Huang

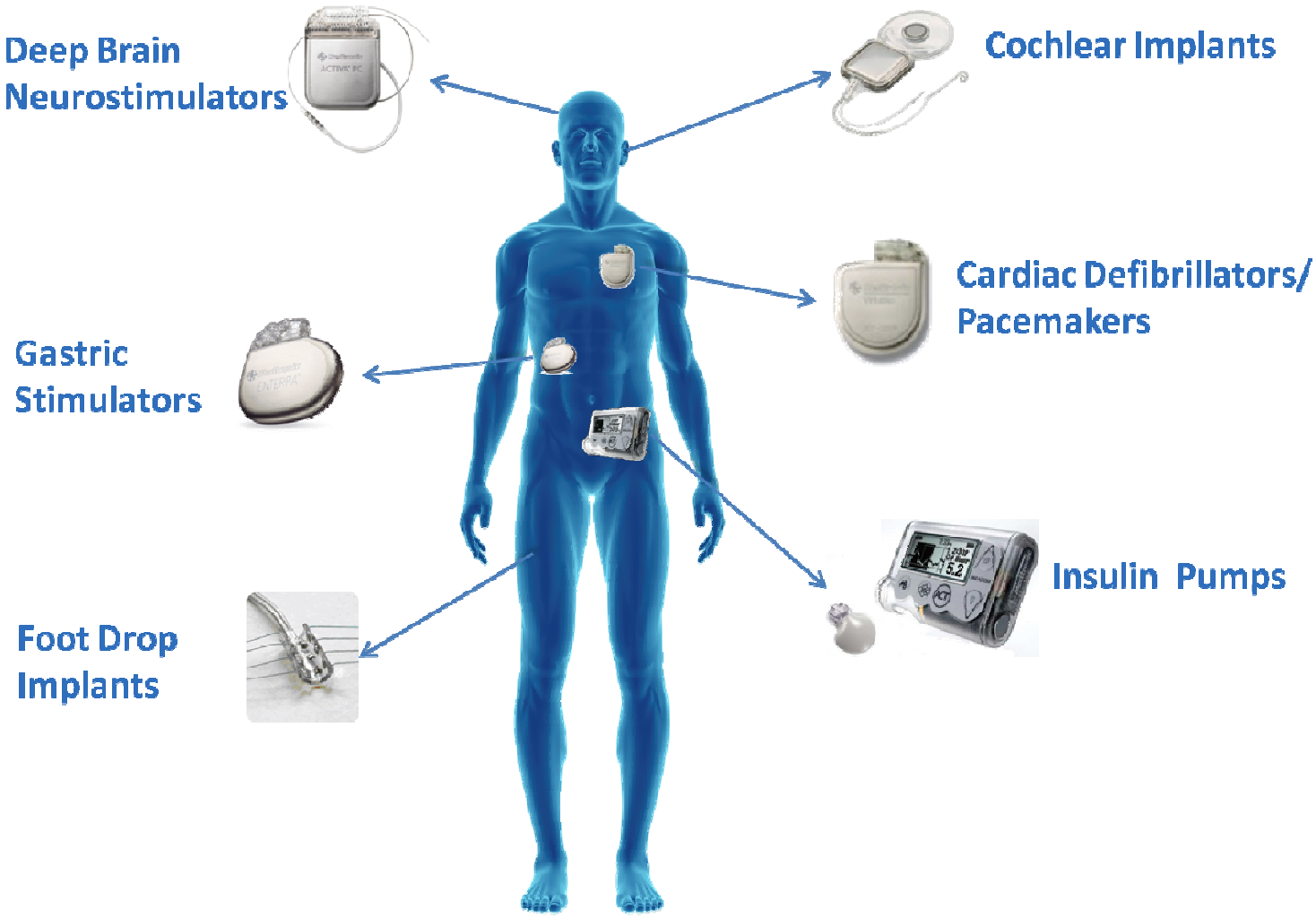
University of Illinois



Body Area Network Background

- Body area network (BAN) consists of nodes *physically touching* the human body (either worn or implanted)
- Sensor nodes monitor the state of the human body, usually for health reasons
- Nodes want to talk to each other

WIRELESS IMPLANTABLE MEDICAL DEVICES



From: http://groups.csail.mit.edu/netmit/IMDShield/

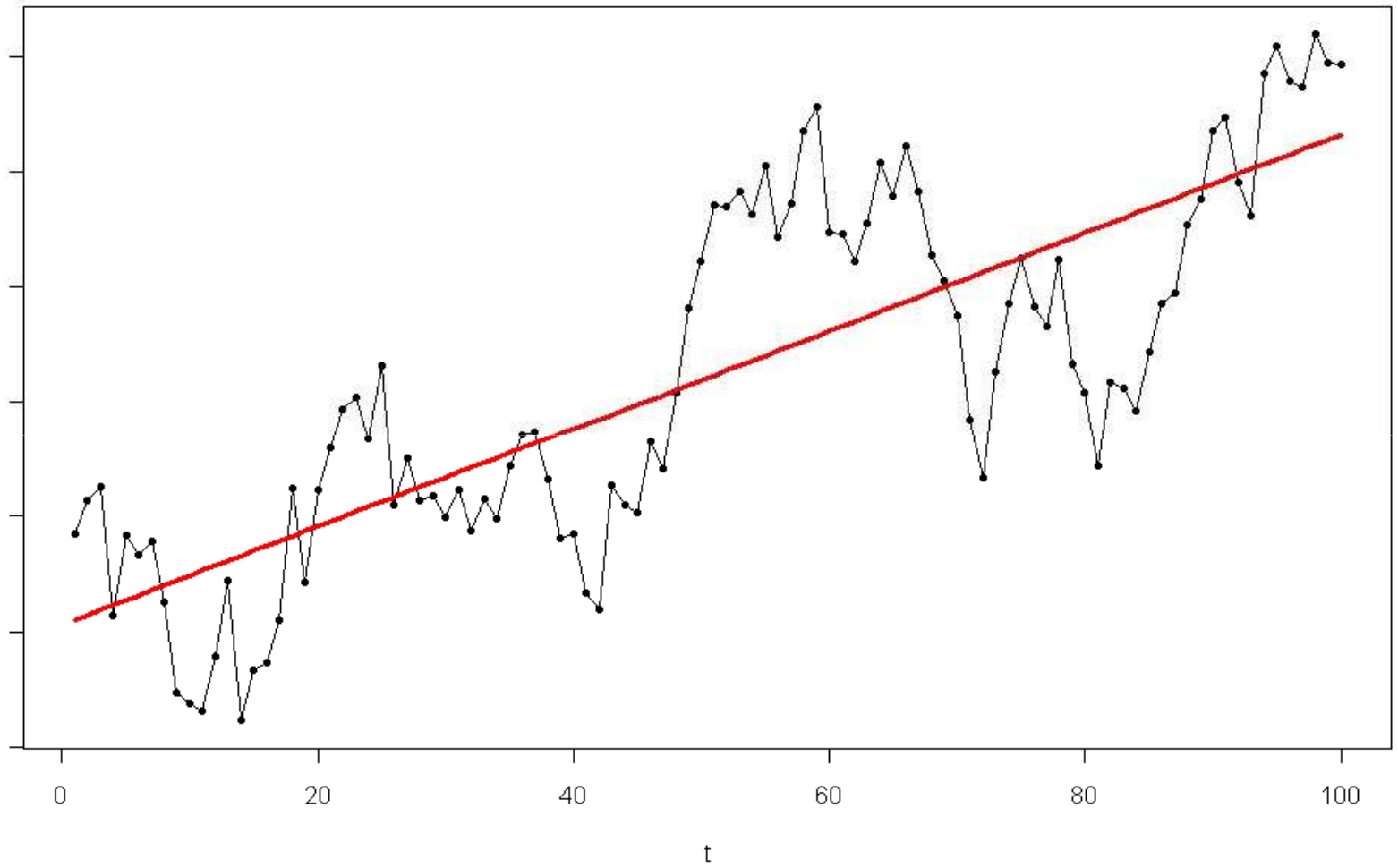
Motivation for Our Work

- Wireless connectivity introduces vulnerabilities
- Halperin et al.* demonstrate successful eavesdropping and impersonation attacks
- We achieve security against outsiders
- A network must share a *secret* to give the network an advantage over outsiders

* Halperin, Heydt-Benjamin, Ransford, Clark, Defend, Morgan, Fu, Kohno, Maisel, "Pacemakers and implantable cardiac defibrillators: software radio attacks and zero-power defenses", IEEE S&P 2008

State-of-the-Art

- Secret sharing using body physiological value
  - Use the randomness of physiological value to share secret
- Physiological state can be modeled as a time-varying signal generated by a random process
  - The history of such states derive secret (Attacker may know the statistics of the random process but not the exact history)


0
20
40
60
80
100
t

Related Work

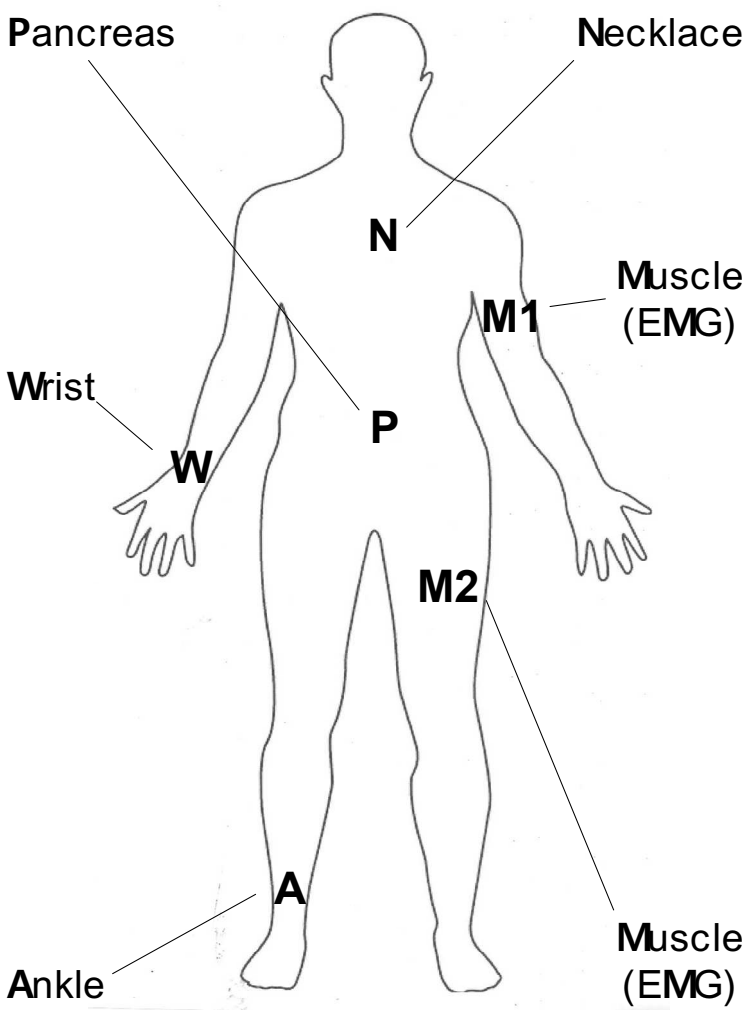
- Prior researchers propose using electrocardiogram (ECG) to share a secret
  - Bao, et al., “Using the timing information of heartbeats as an entity identifier to secure body sensor network,” IEEE Transactions on Information Tehcnology in Biomedicine, 2008
  - Venkatasubramanian, et al., “EKG-based key agreement in body sensor networks,” IEEE Infocom 2008
  - Poon, et al., “A Novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health,” IEEE Communications Magazine, 2006
  - Xu, et al., “IMDGuard: securing implantable medical devices with the external wearable guardian, ” IEEE Infocom, 2011
  - Etc.
- They generally assume ideal ECG measurement, using hospital-provided data

Our Contribution

- We investigate the feasibility of the current literature, propose a novel scheme, study human body channel, and demonstrate the practicality of our scheme
- We conduct four experiments:
  - *ECG Experiment*: to investigate the practicality of current literature by studying the physiological value measurements
  - *Mouse Experiment*: to build our scheme and derive preliminary results about human body channel
  - *Homogeneous Tissue Experiment*: to devise a channel amplitude model using empirical data
  - *Noise Measurement*: to study channel noise on living human body

ECG Experiment

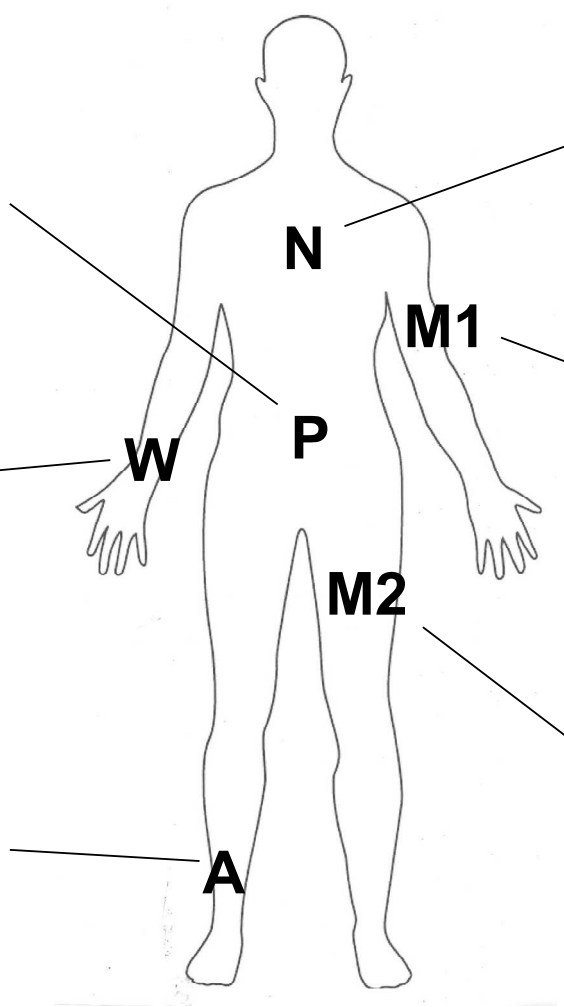
- Correlation coefficient (ρ) for a quantitative measurement of similarity between ideal (I) and other locations
- The measurements are sensitive to electrode orientation; we only show the maximum correlation (the minimum is 0)
- Time synchronization is crucial; readings not aligned in time but otherwise identical yield low correlation (ρ=0.0394)
- Designated target sensor locations that emulate popular BAN use (see diagram on the right)



ECG Experiment Result

Distance	ρ
15	0.9139
5	0.8473
1	0.7709

Distance	ρ
5	0.7436
1	0.6677



Distance	ρ
5	0.1328
1	0.0972

Distance	ρ
7	0.3442
5	0.3047
1	0.1003

Distance	ρ
8	0.0992
5	0.0371
1	0.0155

Distance	ρ
20	0.0782
5	0.0362
1	0.0123

(Distance in cm)

Threat

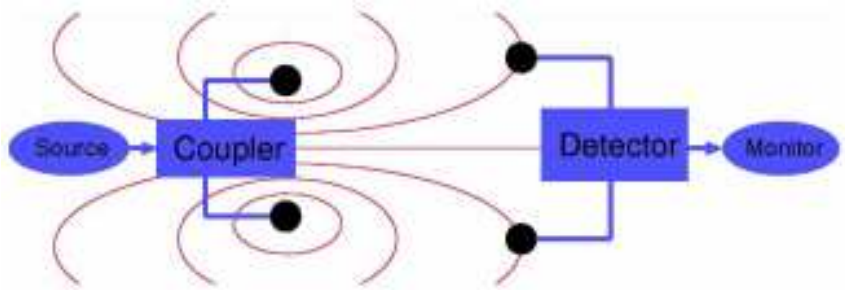
- Physiological value measurements are not robust to the sensor deployment location
- Outsiders can use other technology to remotely measure ECG and compromise physiological value-based secret sharing

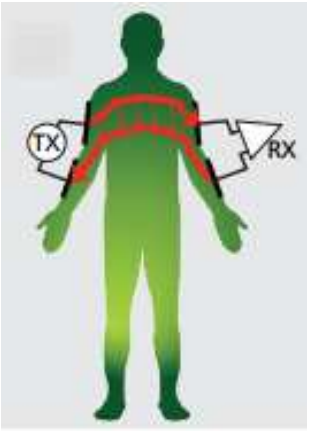




Our Countermeasure

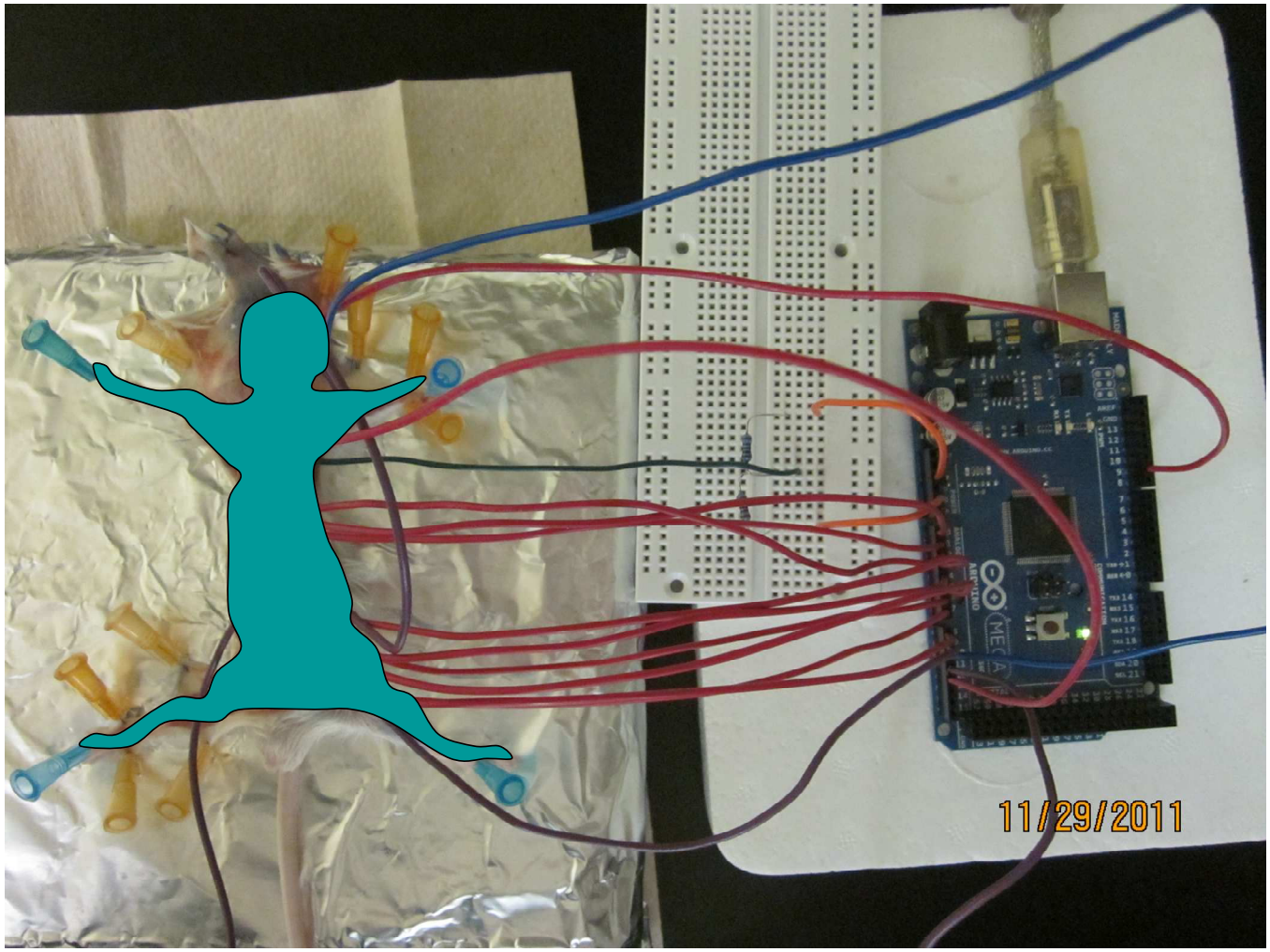
- Our scheme replaces the body physiological values with an artificial electrical signal
- Our electrical signal operates below the action potential level of human body (and thus does not cause change in body physiological state)
- Our scheme is based on body-coupled communication with galvanic coupling





< Images from Wegmueller et al., 2006 (left) and Baldus et al., 2009 (right) >

Mouse Experiment



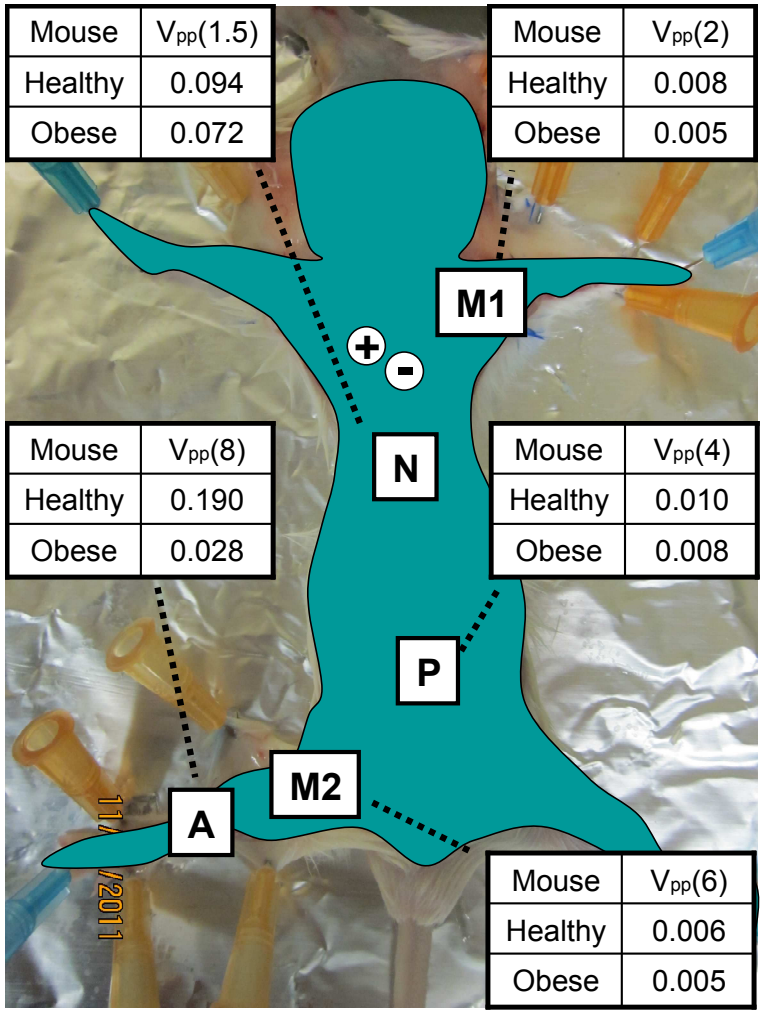
Building Our Scheme

- Source transmits 2Hz rectangular pulse amplitude modulated signal with non-return-to-zero, and receiver uses maximum-likelihood threshold-based decision
- Successful bit transfer
  - 0% at every region except for Ankle (A) region
  - A region showed mean error rate of 0.16%

The mouse is dead (noise is much less than living medium)

Heterogeneous Tissue Channel

- Tissue channel phase measurement
  - Transient state lasts up to 200ms
  - Data rate/bandwidth is limited to 5Hz
- Tissue channel amplitude measurement on the right picture
- However, human is bigger than mouse



Normalized peak-to-peak received voltage magnitude

Human Body Channel Model

- Additive noise channel model

$$S' = h \bullet S + n$$

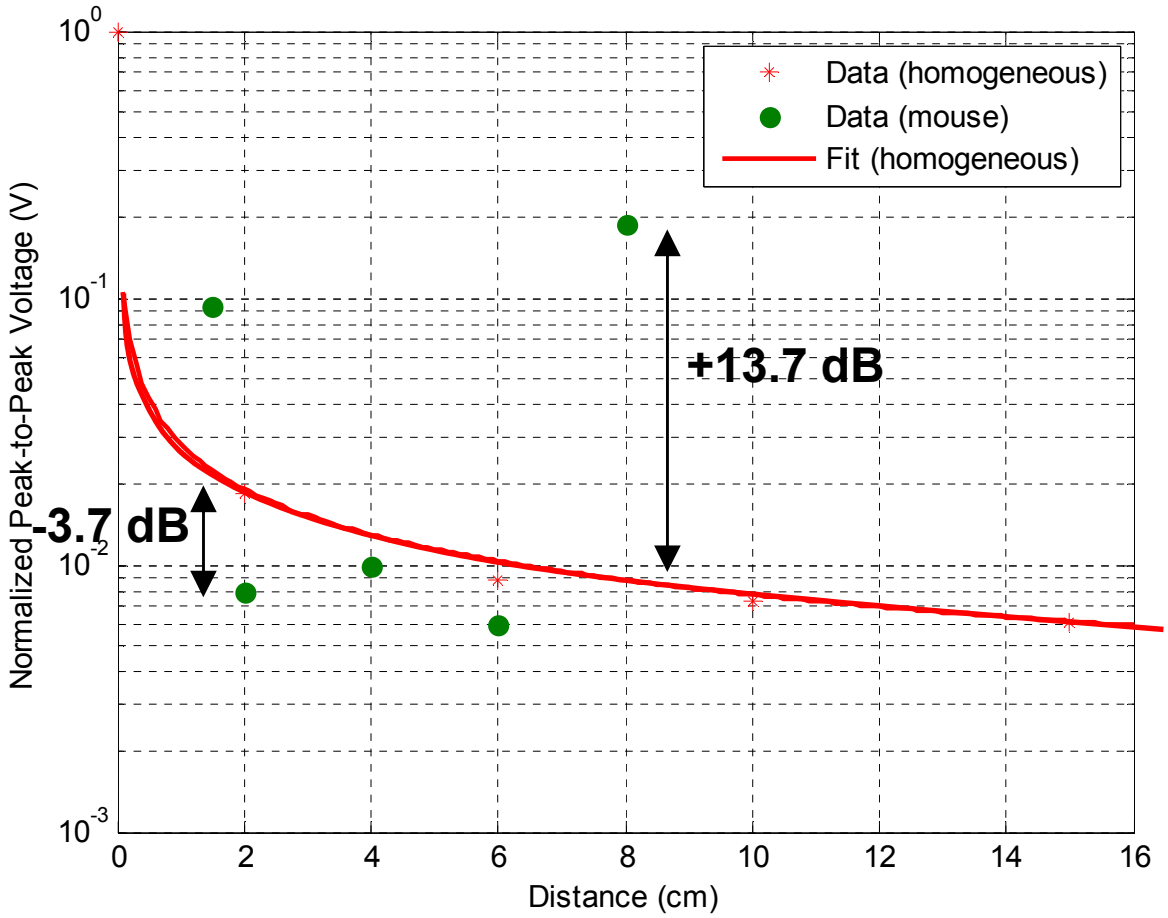
S is the transmitted signal,
S' is the distorted and received signal,
h is channel amplitude,
n is noise

Path loss model for channel amplitude

$$h(d) = \alpha \bullet d^{-\gamma},$$

where d is distance and α, γ some constants

Body Channel Amplitude



h

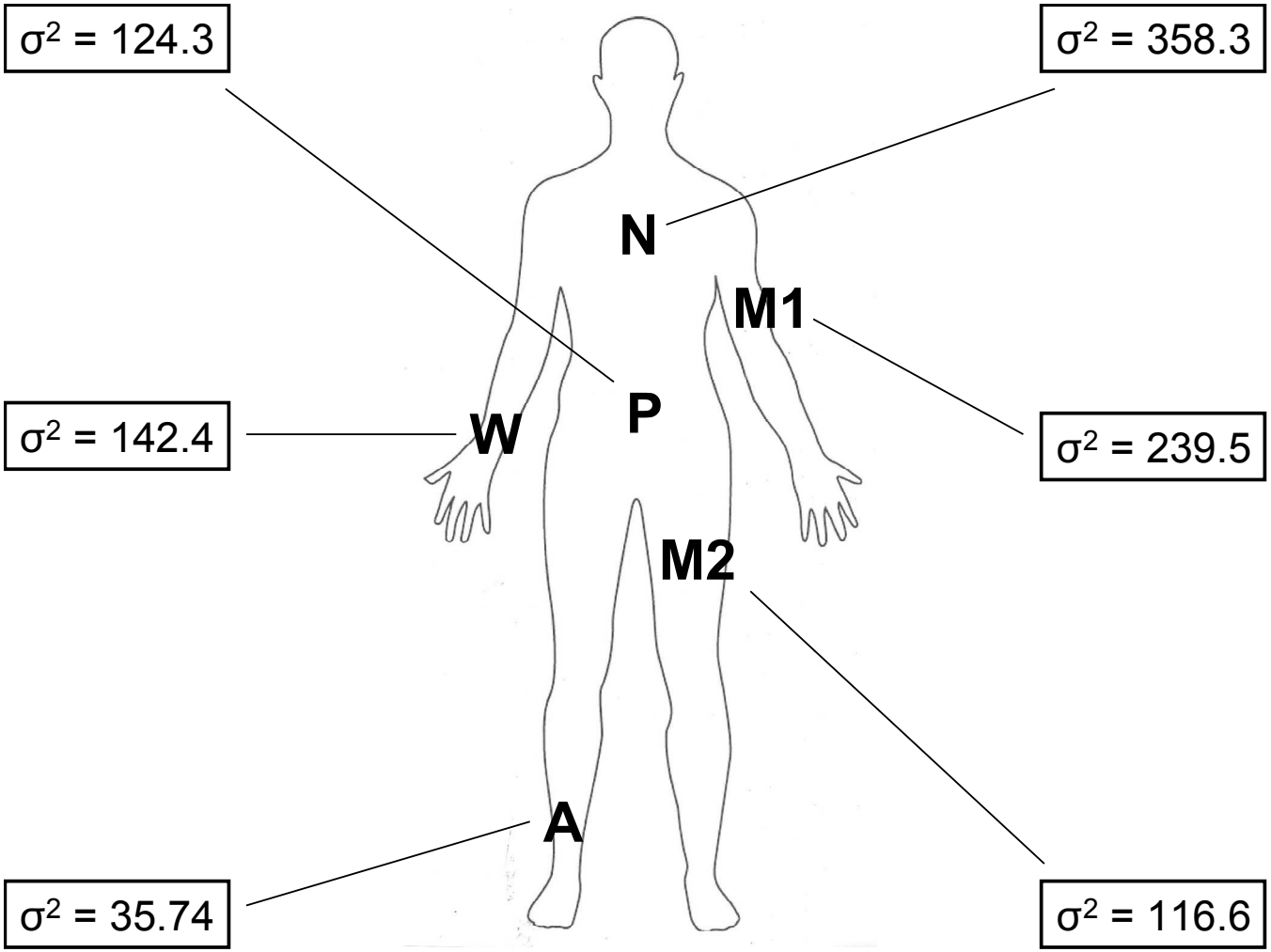
$h_{lower\ bound}$

Using dry pork loin meat

Channel Amplitude Response *h*

- We validate our path loss model from *homogeneous meat experiment* with data acquired from mouse experiment
- $h = 2.1 \bullet 10^{-4}\ d^{-0.5562}$
- $h_{lower\ bound} = 8.9582 \bullet 10^{-4}\ d^{-0.5562}$
- Conservative amplitude response because signals travel through a longer path in human than mouse (and by law of large numbers)

Noise Variance (σ^2) Measurement

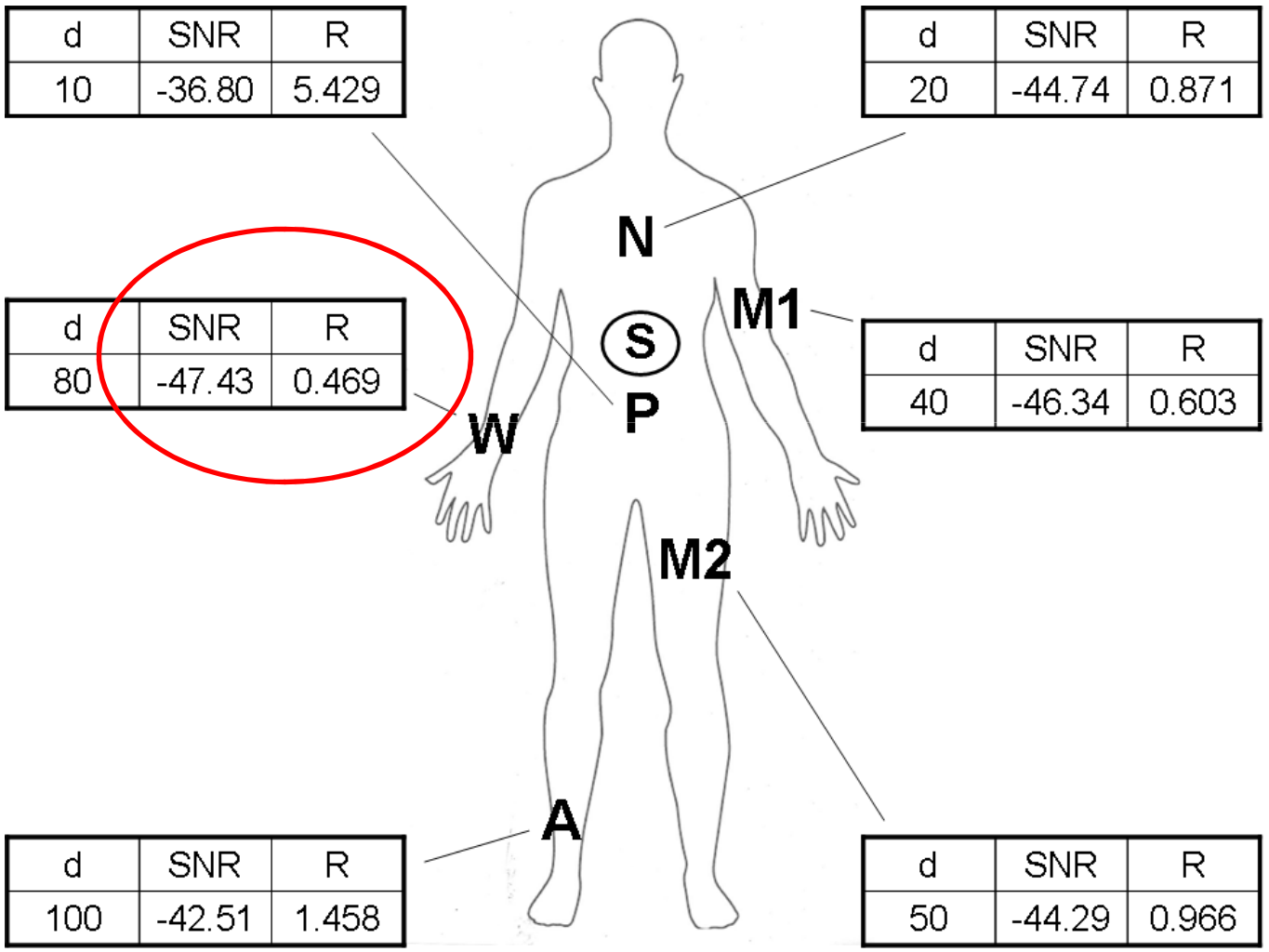


(σ^2 in μV^2)

Analysis of Our Scheme

- Our channel model (not the dead mouse) is used to analyze the performance of our scheme
- To provide a simple numerical value, we use Shannon capacity while assuming Gaussian noise
- Source transmitter is located on the torso region above the belly button, effectively giving maximum distance of 100 cm to reach *anywhere* in *most* human body
- Worst-case capacity because we use $h_{lower\ bound}$

Capacity of Our Scheme



(d in cm, SNR in dB, R in bits per hour)

Application to Body Area Network

- Shannon capacity over 11 bits per day
- BAN applications being characterized by high-risk, low-occurrence events make the very low performance tolerable
- Secret updates are necessary when there is a change in infrastructure, e.g., node misbehaving and needs replacement
- Our scheme requires minimal hardware and is power-efficient, making it suitable for BAN applications

Conclusion

- Investigated state-of-the-art technology for secret sharing
- Realized the necessity to have more understanding about the human body channel
- Measured that channel using empirical data
- Proposed our scheme that does not leak information, demonstrated its feasibility, and analyzed the performance on a practical setting

Thank you

Questions ?