Body Area Network Security: Robust Key Establishment Using Human Body Channel

Sang-Yoon Chang[†], *Yih-Chun Hu*[†], *Hans Anderson*[†], *Ting Fu*[*], *Evelyn Y. L. Huang*[+]
[†]*Electrical and Computer Engineering* [*]*Molecular and Integrative Physiology* [+]*Medicine*
[†*]*University of Illinois at Urbana-Champaign* [+]*University of Illinois at Chicago*
Email: {chang6, yihchun, hcander2, tingfu1, ehuang3}@illinois.edu

Abstract

In order for two sensors within a body area network to determine they are on the same body, e.g., for security purposes, extensive prior work considers the use of physiological values. We study the practicality of using body physiological values for securely exchanging messages for sharing keys. Due to its popularity in the literature, we use electrocardiography (ECG) signals, and show that cardiac physiology is incompatible with such schemes, due to the sensitivity to a node's deployment location on the body and the outsiders' capability to remotely sense the physiological value.

As a solution for key sharing, we inject an artificial voltage signal to build a communication channel secure against an outsider. By implementing our scheme on a dead mouse and analyzing the human body channel characteristic with empirical data, we demonstrate the practicality of our scheme for body area network applications.

1 Introduction

A growing application of wireless sensor network is in body area networks (BAN). Each BAN device is attached to a human body and monitors the state of that body. In health care applications, BAN provides continuous monitoring of the patient's vital signs, allowing for faster medical response without the inconvenience of having to physically stay in the hospital with wired monitoring devices and in-person supervision. BAN can also facilitate a better exercise experience by providing measurements and feedback about how the body is reacting to physical activity.

BAN sensor devices have more stringent set of requirements (which we call *BAN requirements*) than a traditional sensor network. The requirements (in addition to those in sensor networks) have a unifying goal: BAN devices should be convenient and user-friendly since they directly interface with the user. First, the devices and their processing should be highly *power efficient* since charging or replacing battery can be inconvenient and difficult, especially for implanted medical devices, which require surgery to access the devices. Second, the hardware should be *small in size* to minimize the intrusiveness on body mechanics. Third, the network should be *universal*; a network action should affect all nodes, for ease of configuration. Fourth, *wireless connectivity* is essential since it not only provides convenience in mobility (and thus usability) but also aids in controlling and maintaining devices, especially for implanted devices. Wireless connectivity, however, introduces security vulnerabilities (many of which stem from the inherent nature of shared medium in wireless communication) that can be exploited by the threats described in Section 2.1.

We focus on the security of a BAN against an outsider. Since a BAN consists of all entities touching the body, our goal is to secure the communication of these devices against outsider devices that do not touch the body. Our goal is to create a shared secret key among BAN members to ensure confidentiality and integrity (using cryptography) and to resist jamming attacks (using spread spectrum [14, 17]). This paper focuses on key establishment and not on the applications of that key.

Prior work on BAN security has proposed schemes based on establishing a shared secret key using the body's *physiological values*, such as heart rate and temperature. Much prior work relies on the electrocardiogram (ECG) signal, which is a voltage signal that is easily measured by the electronic sensor devices and requires relatively light processing; we review this work in Section 2.2. In this paper, we study the feasibility of using human physiological measurements to establish secret key among network nodes. Our experiment shows that such measurements are highly sensitive to the sensor deployment locations and device size limitations. Moreover, an outsider could potentially compromise key by remotely sensing the pulse, as described in Section 4.

Our scheme securely exchanges a secret among BAN

nodes by building a side channel hidden from outsiders. We inject an artificial electrical signal below the action potential, so that it has no physiological effect on the body. Our scheme is practical in a BAN environment, because it does not require separate frontend hardware to transmit or receive signal. We demonstrate the scheme's effectiveness with empirical data acquired from series of experiments (each using dead mouse, homogeneous meat, and living human body).

The rest of the paper is organized as follows. We begin with the background of our research and related work in Section 2. Then, we investigate the feasibility of the state-of-the-art schemes in Section 3 using experiments on a human body. Threats to current schemes and our countermeasure are presented in Section 4. In Section 5, we build our scheme on heterogeneous tissue and successfully transfer bits. We further study the channel characteristics of human body, the actual platform for BAN applications, in Section 6 and analyze our scheme performance in an application-realistic setting in Section 7.

2 Background & Our Contribution

We consider a *Body Area Network* to be the set of nodes that are physically touching the human body. Our goal is to establish a key among the nodes in the BAN.

2.1 Threat Model

We focus on attacks on confidentiality and integrity. When BAN nodes do not share keys, an attacker can perform passive attacks, such as eavesdropping, and active attacks, such as controlling BAN devices. Though currently deployed BAN medical devices send their transmissions without any cryptographic coding protection, and are vulnerable to both attacks [9], we assume that future devices will include cryptographic protection. Our paper focuses on establishing a key among the BAN users that is known only to BAN devices and cannot be determined by an outside attacker (an attacker without direct access to the human body, however, may be able to observe certain physiological values from outside of the body).

2.2 Related Work on BAN Key Sharing

Currently deployed BAN devices exchange their packets in plaintext and are susceptible to eavesdropping and impersonation attacks, as Halperin et al. demonstrated with an off-the-shelf software radio [9]. In order to counter attacks on confidentiality and integrity, prior work proposes to use a physiological value measurable on the human body to establish cryptographic keys, focusing on electrocardiogram (ECG) [3, 4, 15, 19, 20, 23]. Other authors propose using accelerometer data, either to aid key generation using ECG [18] or to generate keys by themselves [6, 11]. However, such approaches using accelerometer data require specialized accelerometer hardware for motion sensing and are vulnerable to threats described in Section 4.

Proposed key sharing schemes use the random nature of body physiological values either to share a secret or to establish that two sensors are connected to the same body. For example, vital signs, such as heart rate and blood pressure, can be modeled as a time-varying signal generated by a random process. The sequence of physiological values and the holding times can be used to derive a shared secret or to verify that two nodes are connected to the same body. Previous researchers used the variation on the heart beat frequency, (or its inverse, the period of ECG heart pulse) to share information among BAN users.

2.3 Related Work on Body-centric Communication

Existing literature on key establishment for BAN security uses the electrical voltage signal of the ECG. In such schemes, the human body represents a propagation medium for the ECG signal, which originates at the heart. However, the physical-layer characteristics of the ECG signal are yet to be well understood in the security community. In a non-security context, previous researchers have studied the human body channel characteristics for radio frequency (RF) waves [10, 16], which are the predominant form of wireless communications. However, RF technology uses electromagnetic waves for signal propagation and do not apply to electrical voltage signals such as ECG signals or our work. In *body-coupled communications*, electrical signals are sent across the body; these can be divided into two approaches: *capacitive coupling* and *galvanic coupling*. The capacitive coupling approach [2, 5, 8, 12, 24] couples one electrode to the body and the other to a ground shared with all nodes; here, the body acts as a signal conductor and communications medium. This technology, however, is for personal area networks [24] and extends the network to nodes that are not in direct contact with the body, such as cell phones, credit cards, and identification badges. In contrast, the galvanic coupling approach [21, 22] requires the nodes to have direct physical access to the body by having both of the transceiver's electrodes on or within the body (the body acts as a transmission line). Our scheme is based on galvanic coupling.

2.4 Our Contribution

Previous work on the security of physiological-value based key establishment schemes, which has been tested mostly in simulation [3, 4, 15, 19, 20, 23]. However, the measurements used in such simulations were based on data measured in a hospital, taken from the ideal locations on the body using sophisticated hardware devices. We use more realistic hardware and human body placements to determine the reliability of such approaches. In other words, we study the human body as a communication channel. Our measurements indicate that the physiological value measurements are not robust to sensor deployment locations; the measurements are very noisy and distorted, and it seems possible that an adversary can remotely measure the physiological values at least as well as a legitimate node that is placed badly.

Our solution to these shortcomings is to develop a novel scheme that constructs a secure side channel against an outside eavesdropper. We conduct four experiments to better understand the human body channel and to demonstrate the practicality of our scheme and analyze its performance. In addition to studying the physiological value measurements in our *ECG experiment* (to investigate the other proposed schemes), we demonstrate the practicality of our scheme by building it on heterogeneous tissue (the *mouse experiment*, performed on a dead mouse). To devise a conservative channel model that considers the complex and highly-varying nature of human body, we study the signal wavefront propagation and attenuation by experimenting with *homogeneous tissue*. We also take *noise measurements on human body* to complement our channel model and derive the capacity of our scheme. Using these experiments and our channel model (based on empirical data that we acquired from living human body), we analyze our scheme and demonstrate its practicality.

3 ECG Experiment

Because the heart produces electrical signals, called electrocardiography (ECG) signals, that are both easily measurable by sensor nodes and greater in magnitude than most other electrophysiological signals, much previous research uses the randomness of ECG for key establishment as detailed in Section 2.2. We determine the extent to which ECG information is reliably shared between two sensors attached on the same body.

3.1 ECG Background

In this section, we provide a brief overview on electrocardiography, which is the study of electrical activity of heart, focusing on the notions most relevant to our work.

The human heart is a muscular organ that is responsible for blood circulatory system; the heart periodically contracts to push blood through the arteries. Each of two upper chambers is called an atrium, and each of two bottom chambers is called a ventricle. The right atrium and ventricle receives oxygen-deprived blood from most of the body and pump it into the lungs; the left atrium and ventricle receive oxygen-rich blood from the lung and pump it through the rest of the body.

The heart is controlled through the flow of electrical current, which causes muscle to contract. When electrical current reaches the outside of cardiac muscle, the electrical charges disturb the muscle cell's electrical balance, which causes positively charged ions to flow into the muscle cell, resulting in an increase in the cell charge potential. This process, called *depolarization* promotes the contraction of the muscle cell. The natural pacemaker, called the *sinoatrial node*, is located at the top of the atrium, and initializes depolarization and thus the contraction of the atria. The depolarization current then reaches the *atrioventricular node*, at the junction between atrium and ventricles, that delays the current flow to delay contraction, so that the atrial blood has adequate time to flow into the ventricle, after which the current flows downward through a track of conducting fibers to reach the ventricles, inducing ventricular contraction. Ventricles, which have thicker muscle walls and thus are capable of exerting higher pressure than atria, pump the blood out of the heart to the rest of the body.

The depolarization travels downward and leftward in the human body, making the heart a cardiac dipole with the positive end pointing downward and leftward. We can visualize lines around that dipole that have equal electrical potential; such lines are called *equipotential lines*. Ideally, measurements are made with electrodes as orthogonal to those equipotential lines as possible. Therefore, we measure ECG with the negative electrode on the upper right chest (close to right arm) and the positive electrode on the upper left abdomen (close to left foot), giving a consistently positive ECG measurement. We refer to this deployment location as the *ideal location* and denote it as I; this location is one of the leads used in the first practical ECG machine [7]. When leads are placed in the ideal location, we can clearly measure the heart's cyclic depolarization and repolarization. We use this signal as our reference signal to compare with other suboptimal electrode placements, as described in Section 3.2.

3.2 ECG Experiment Setup

We developed a platform around the Arduino Mega 2560 microprocessor to digitize the ECG signal. Our circuit includes amplifiers and filters and samples at a rate

Variable	Simulated Scenario	Positive Electrode	Negative Electrode
I	Ideal (ECG)	Left (upper) abdomen	Right (upper) chest
I^-	Ideal (ECG)	Right (upper) chest	Left (upper) abdomen
I'	Ideal (ECG)	L. abdomen (different body)	R. chest (different body)
I''	Ideal (ECG)	L. abdomen (different time)	R. chest (different time)
DC	DC voltage	Power supply (+5V)	Power supply (GND)
P	Artificial pancreas	Left abdomen	Right abdomen
$M1$	EMG (muscle)	(Left) arm	(Left) arm
$M2$	EMG (muscle)	(Left) thigh	(Left) thigh
A	Inertial sensor	(Right) ankle	(Right) ankle
W	Watch	(Right) wrist	(Right) wrist
N	Necklace	(Center) chest	(Center) chest

Table 1: ECG sensor deployment locations

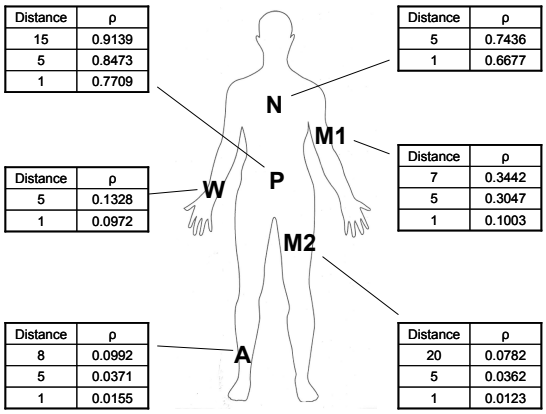

Figure 1: ECG sensor deployment locations and their correlation values with ideal orientation (distance in cm)

around 1kHz. The voltage potential at each lead is measured using a single microprocessor to ensure close synchrony between samples.

Since our goal is to determine the extent to which two sensors in a BAN can share a value, we compare ECG signals from different electrode locations. We measure the correlation coefficient ρ to provide a quantitative measurement of the similarity of two signals.

We built two ECG circuits with identical specifications. Table 1 lists the locations of the positive and negative electrodes on the human body, the variables we use to denote them, and their simulated medical application scenarios. Since human heart acts like a cardiac dipole with positive end pointing downward and leftward, we use the ideal location I as our reference signal to compare with other electrode locations. These locations are also illustrated in Figure 1. Each signal is a physiological, with the exception of the *DC* signal, and each was measured simultaneously with the exception of I''. Because the measured correlation varies with orientation, we tried at least three orientations for each location, and indicate the *highest* correlation value found at each location (the lowest correlation was negligible because two electrodes on an equipotential line measures no signal).

3.3 Correlated and Independent Signals

To verify the correctness of our implementation, we compare ECG measurements in four scenarios: electrodes located at the same location ($\rho_{I,I}$), electrodes located at the same location with opposite polarity (ρ_{I,I^-}), ideal electrodes compared to a DC power supply ($\rho_{I,DC}$), and ideal electrodes on different human bodies ($\rho_{I,I'}$). We observe that $\rho_{I,I} = 0.9990 \approx +1$; and $\rho_{I,I^-} = -0.9992 \approx -1$; these results are within 0.1% of their theoretical values; the discrepancy between the measured values and the theoretical values come from imperfections in the analog hardware. We also observe that $\rho_{I,DC} = 0.0003 \approx 0$ and $\rho_{I,I'} = 0.0013 \approx 0$ and verify that physically independent values yield no correlation.

3.4 Simultaneous Measurement

This section demonstrates another challenge of using ECG measurements in BAN: when two readings are not time synchronized, the resulting correlation is much lower. In this section, we take ECG measurements of the same body, at the ideal location, but at different non-overlapping time intervals. To ensure that I and I'' are drawn from the same distribution, we measured I'' immediately after I. The correlation between the two values, however, is $\rho_{I,I''} = 0.0394$. This very small correlation value shows that BAN nodes can generate randomness both from time-average statistics as well as the variation in those statistics, though the variation is likely to be more secure, since most people exhibit normal (non-pathological) time-average statistics.

3.5 Common Body Locations for BAN Use

We tested body locations that are commonly considered for BAN use. An artificial pancreas sensor (P) is used to monitor the blood glucose level and pump insulin accordingly for people who suffer from diabetes. Electromyogram (EMG) measurement systems ($M1, M2$) estimate the electrical potential generated by muscle cells to detect medical abnormalities in skeletal muscle or study biomechanics of movement. Inertial sensors (A), typically located on ankles, keeps track of location and movement. A watch (W) and necklace (N) are commonly examples of a human interface to the BAN network.

Electrodes placed on the torso generally yield a high correlation. For example, near the pancreas (P), $\rho_{I,P} \geq 0.77$, and the necklace (N) has $\rho_{I,N} \geq 0.66$. However, the other locations show low correlations since they are either dense in large muscle (and thus experience more noise), e.g., $M1, M2$, or adjacent to skeletal bone (and lose conductivity), e.g., A, W. As can be seen in Figure 1, the ECG signals measured at these four locations yield negligible correlation to ECG signals produced by the

heart. In particular, the thigh region, which simulates EMG sensor devices ($M2$), yields the lowest correlation of $\rho_{I,M2} \leq 0.05$.

3.6 Correlation Dependance on Distance

The size and the number of sensor devices directly affect their usability. Since the sensor's size determines the maximum distance between the two electrodes with which the sensor measures the electrical potential, we also study the effect of distance between the electrodes on ECG measurements. For each body location, Figure 1 shows the correlation as the electrode distance decreases. We start with the largest distance compatible with that sensor location, and in addition evaluate a distance of 5 cm to simulate a wearable medical devices and of 1 cm to simulate the size of implanted medical devices.. In each case, the correlation is monotone increasing in electrode distance, because we choose the ideal orientation for each location, and when the orientation is orthogonal to equipotential lines, greater distance results in a stronger signal.

3.7 ECG Experiment Summary

Our study on the measurement of the ECG signal shows that it is difficult for devices located at arbitrary positions to measure the ECG. In particular, the physiological values' measurements are not robust to where the sensor is deployed on the body (especially, yielding very noisy measurements on body regions that are muscular and adjacent to skeletal bone), calling into question their ability to provide a shared value.

4 Threat and Our Countermeasure

A substantial threat to systems based on body physiological values is that such values may be remotely monitored. In the case of ECG signals, there are a number of well-developed technologies for remotely monitoring heart activity. For example, pulse oximetry uses light emitting diodes to measure the oxygen saturation of the blood, which can also determine the heart beat times (which previously proposed schemes typically use for key establishment). Pulse oximetry works by shining light at two wavelengths through a blood vessel; one wavelength is better absorbed by deoxygenated blood, and the other wavelength is better absorbed by oxygenated blood. Commercial smartphone apps such as Instant Heart Rate can also measure heart rate. Another technology is the electronic stethoscope, which can measure pulse through sound waves. These techniques do not directly measure ECG signals, but they measure a signal highly correlated to ECG. Therefore, ECG-based key establishment approaches are susceptible to attacks from an outsider, and can become especially problematic when some sensor nodes are deployed in suboptimal locations where the ECG signal is overwhelmed by noise.

Though the ECG values are not robust to sensor deployment locations, since the best correlation values in some regions are as low as 1%, as described in Section 3, a non-zero correlation value shows that ECG reaches everywhere in the body. Theoretically, the network can use correlated information even from highly distorted data and still establish a key hidden from a limited adversary, as long as the electrical signal is not known to the attacker.

Our solution is to use a different electrical signal for key sharing. Instead of using ECG information, which might be compromised as described above, we construct a communication channel that is not based on the physiological state of the body. Rather, we inject an artificial electrical signal below the *action potential* level of human body (which is the required voltage magnitude that triggers the activity of body cells); the action potential is 50 millivolt. In other words, the magnitude of the injecting signal is too low to trigger a physiological change in body. A source node generates an electrical voltage signal, and like the ECG signal from the heart, the voltage travels across the body and reaches the receiver node. While radio frequency (RF) technology relies on the propagation of electromagnetic wave in free space, our scheme uses electrical field propagation within the human body for communication (such technology is called body-coupled communication with galvanic coupling, described in Section 2.3).

In order to validate the practicality of our scheme, we need to understand the communication channel medium. Since human body channel is heterogeneous and complicated to model, much more so than air (the typical medium used for radio communication), we take empirical measurements and construct a conservative channel model in Section 6. Then, we analyze the lower bound on the capacity of our scheme in real life applications to human beings in Section 7.

5 Mouse Experiment

To determine the effectiveness of our proposed scheme, we use the heterogeneous tissue of mice, which is often used to simulate human body for dielectric (electromagnetic) properties [1, 13]. We study the capacitive nature of the heterogeneous tissue medium and find the bandwidth limit (Section 5.2); we measure the in-body wavefront propagation and see how the signal attenuates (Section 5.3); and we successfully build our scheme on dead mice (Section 5.4).

5.1 Experimental Setup

We run the experiment with a dead mouse. The mouse, originally used for obesity studies, was killed within one hour of our experiment time. Our mouse torso was about 7cm long and weighed about 30 milligram, and was obese, since it ate a mixture of 40% chow (healthy food) and 60% lard (pure fat) and lacked exercise throughout its lifetime.

We use an Arduino microprocessor to generate the source signal and read the voltages at the various receiver electrode locations. We took our readings tightly spaced in time, as described in Section 3.4, and emulated the ECG experiment for sensor locations, as shown in Table 1, with electrodes at a distance of 5 mm. In our measurements, the source and receiver readings do not share a common ground. We used multiple electrodes at each location to find the best orientation.

We use a zero-order hold rectangular pulse signal for our experiment. That is, we sent a "1" bit by maintaining α between the transmission electrodes, and a "0" bit by maintaining $-\alpha$ between the transmission electrodes, where α is the voltage level we chose for that experiment. Subject to frequency limitations imposed by tissue capacitance, other modulations are also possible, though we chose this signal for our evaluation because it yields the highest effective signal-to-noise ratio given a power constraint and without knowing the receiver strategy. The receiver, in turn, decodes the signal using a threshold-based maximum likelihood (ML) decision rule.

5.2 Bandwidth

Since we use rectangular signal, we only require one sample per symbol. Our experiments showed that it takes less than 200 ms to approach steady-state after source changes its voltage level in the heterogeneous tissue of mice; the transient state, generally lasting between 150 ms and 200 ms, is due to the capacitance of the tissue. We therefore wait for 200 ms before we sample, limiting our data rate to 5Hz.

5.3 Channel Amplitude Response

In this section, we study the channel amplitude response, or the signal propagation attenuation along the channel. Figure 2 depicts the average received peak-to-peak voltage amplitude normalized to the source voltage sampled across more than 100 periods of the source signal, which was injected at 2 Hz. Region *N*, being the closest to the source, showed high received voltage amplitude, as did region *A*, showing that skeletal muscle (muscle along the skeletal bone) is a good channel medium. We also found, as in our previous experiments, that these values are highly sensitive to the sensor deployment locations and their orientations (Figure 2 only displays the largest channel amplitude response). To cope with the complex nature of the mammalian body channel, we construct a channel path loss model and develop a lower bound on the channel amplitude response in Section 6.2.

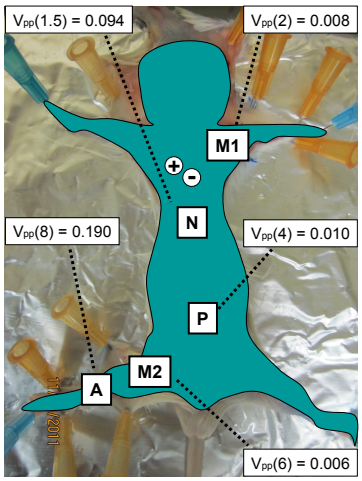

Figure 2: Signal propagation attenuation on mouse with distance (cm) from the source in parenthesis

5.4 Mouse Experiment Results

We ran our system on the dead mouse as described above and confirmed that bits are reliably transferred as long as the transmission bandwidth is less than 5Hz. For example, we sent 200 bits at a rate of 2 Hz and found no error inside of the body network, except at the ankle area, which had an average error probability of 0.15%.

5.5 Mouse Experiment Limitations

Although we were to successfully transfer messages across a mouse using our scheme, these results do not directly prove applicability to a *living* human body, because the noise in a dead body is substantially lower than in a live one. Unlike our ECG experiment, our mouse experiment does not consider the effect of noise; for example, the *P* region in the ECG experiment performed better than the *P* region in the mouse experiment, because the significant attenuation in the human body is accompanied by a significant reduction in noise. Our use of $\alpha = 0.625$ volt (which greatly exceeds the action potential) boosts the signal-to-noise ratio in a manner unreasonable for living bodies. A mouse is also smaller than human; the signal travels through a much longer path in

human body. In Section 6, we extend the study of heterogeneous tissue channel and overcome these limitations by studying a living human body.

6 Human Body Channel Model

Though the mouse experiment yielded some useful information about the heterogeneous body channel such as capacitance-induced bandwidth limits, it lacked noise and used signal levels impractical in live bodies. In this section, we extend our study of the body channel.

6.1 Channel Model

A signal is attenuated as it travels through a medium (for example, in a BAN, the medium is a human body). We model these channel paths using the channel response h, the original physiological signal (S), and channel noise (N), such that the signal at measurement ($\hat{S}$) will be

$$\hat{S} = h \cdot S + N \tag{1}$$

Since we use an electronic voltage signal, the signal does not travel outside of the body due to the high electrical resistance of air. Instead, the measured signal and noise both come through the body.

Section 6.2 evaluates the level of signal attenuation through body tissue, and construct a simplified, yet conservative model for channel amplitude response by studying the in-body signal propagation on a homogeneous tissue material. Then, in Section 6.3, we study the body noise by acquiring noise measurements on living human.

6.2 Channel Amplitude Response: Experiment with Homogeneous Tissue

To study the signal propagation attenuation in a body, we first examine homogeneous material, namely a lean slab of pork loin meat. We use an Arduino microprocessor to modulate a signal and read the voltages at the various receiver electrode locations. The receiving nodes are positioned at various distances from the sending node, and each node uses two independent electrodes between which it injects or reads the electrical potential difference. We separated the electrodes by a distance of 1 cm to emulate implanted medical devices. We took our readings tightly spaced in time, as described in Section 3.4, and we did not share a common ground between any two nodes. At each receiver location, we considered two electrode orientations: one parallel to, and another perpendicular to, the source electrodes. We transmitted at 1 Hz and sampled at 5 Hz to measure the signal attenuation.

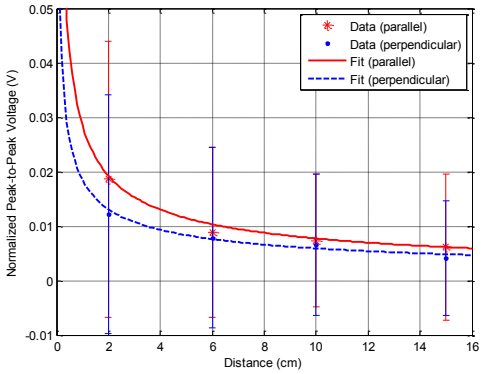

Figure 3: Signal propagation attenuation on homogeneous meat for path loss channel model

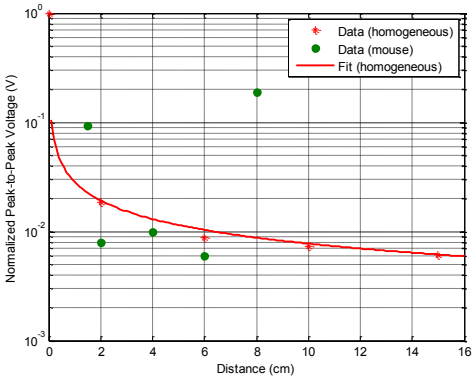

Figure 4: Signal propagation attenuation comparison between homogeneous meat and mouse

Due to the homogeneous nature of the medium and the lack of noise, our measurements yield a simple exponential fit that we can use for the channel path loss model for amplitude response. Figure 3 depicts the received time-average peak-to-peak voltage amplitude normalized to the source peak-to-peak voltage amplitude, and the 90% confidence intervals for both parallel and perpendicular orientations. Each data point represents at least 1000 sample readings. We also plot the least-squares exponential fit for the data measurements according to the path loss model and get $2.1 \cdot 10^{-3} \cdot d^{-0.5562}$ for the parallel orientation and $1.896 \cdot 10^{-3} \cdot d^{-0.4943}$ for the perpendicular orientation The parallel orientation always outperforms the perpendicular orientation, so we use the fit for the parallel orientation as our channel amplitude response function: $h = 2.1 \cdot 10^{-3} \cdot d^{-0.5562}$ where d is the distance in meters.

We validate our path loss channel model by comparing

it with the results from the mouse experiment. Figure 4 displays the signal attenuation measurements along with our path loss channel model h in a logarithmic scale. The measurements taken from the mouse are quite different from our path loss model, which is not unexpected due to the complex nature of mouse body structure as compared to the relatively uniform structure of the pork loin. The mouse measurements deviate from our path loss model by between -3.7 dB and +13.7 dB.

Since we are interested in the worst-case channel condition, we attempt to find a lower bound on the channel amplitude response, which we denote h_{LB}. To do so, we subtract 3.7 dB from our channel model:

$$h_{LB} = h - 3.7\text{dB} = 8.9582 \cdot 10^{-4} \cdot d^{-0.5562} \quad (2)$$

We use this channel amplitude response in the performance analysis of our scheme in Section 7. This is a conservative lower bound because the human body channel will be more heterogeneous than mouse channel due to substantially greater propagation distance; as the signal propagates, it will experience a more diverse channel attenuation level than the shorter mouse channel. The law of large numbers shows that as more diverse channel attenuations are added together, they will tend to diverge from the lower bound (since they converge to the mean). One path that will yield significant improvement over our attenuation model is that signals can first traverse the skeletal tissue (which shows less attenuation as demonstrated in the mouse experiment in Section 5.3) until it reaches the fat near the receiver sensor, and then it can penetrate the fat.

6.3 Channel Noise

We measure the magnitude of noise on human body with the electrodes deployed on the same locations as with previous experiments (as described in Table 1). Sampled at the rate of 50 Hz, the variance σ^2 (which is a scaled version of power) is shown in Figure 5. We use these measurements to compute the capacity of our scheme in Section 7.

The result confirms two facts that we already learned from the ECG experiment in Section 3. First, ECG signal, which constitutes noise in our scheme, is the strongest electronic signal in the body, with noise power decreasing in distance as we go further away from heart. Second, muscle produces more noise than highly resistive fat; for example, region $M1$ yields higher noise power than region P even though P (and thus ECG signal) is closer to heart; in contrast, in the ECG experiment, P has much higher correlation than $M1$, meaning that ECG is more dominant at P than $M1$. In addition, region A displays the lowest noise magnitude because it is far away from heart and the skeletal bone provides a high resistance path. Despite being near skeletal bone, region W produces surprisingly large amount of noise.

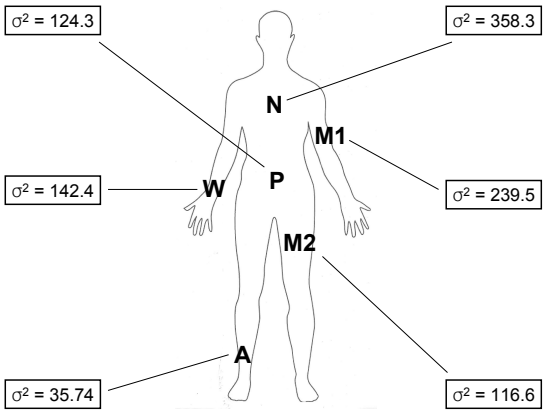

Figure 5: Human body noise variance in μV^2

7 Performance of Our Scheme

After demonstrating our scheme on dead mice in Section 5, we studied the channel of a living human being, namely, the channel amplitude response and noise characteristics, respectively, in Section 6 and Section 6.3. Since we can not test our scheme on a living human being due to the denial of our Institutional Review Board (IRB) application, which is required by our institution before any human experimentation, we use our channel model to analyze the effectiveness of our scheme for real-life applications on human body.

7.1 Capacity Performance Metric

We take an information-theoretic measure for our performance metric and introduce two relevant metrics, signal-to-noise-ratio (SNR) and channel capacity (R), in this section. From Equation 1, we observe that the signal-to-noise-ratio (SNR) is the following: $SNR = \frac{E[||S||^2]}{E[||N||^2]}$ where $||.||$ is the Euclidean (L2) norm and $E[.]$ is the time-averaged value. The channel capacity (R), or the mutual information between a signal S and the distorted copy $\hat{S}$, is the maximum possible reliable communication rate. To provide a simple approximate numerical value for our performance, we assume Gaussian noise and use the Shannon capacity:

$$R = B \cdot \log_2(1 + SNR) \quad (3)$$

Given the analog bandwidth (B), which is determined by the signal rate and the modulation scheme, we examine the effect of previously measured attenuation and noise on the capacity of our system.

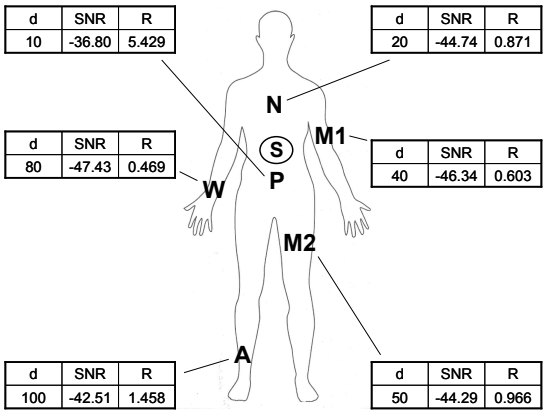

Figure 6: Channel capacity for our scheme (the distance d is in centimeters; the signal-to-noise ratio SNR is in dB; the capacity R is in bits per hour)

7.2 Worst-Case Performance

We assume that the transmitting source is located on the torso region above the belly button and investigate the worst-case capacity of a broadcasting source. Since all legitimate users in the body area network should be able to receive the injected signal, we study the body channel capacity of the worst-case scenario, for which we use the lower bound on the channel amplitude response (h_{LB}) and the deployment location that yields the lowest value. This also represents a lower bound on the performance.

If we transmit at 50 mV, which is well below the action potential, and h for our channel amplitude attenuation, the the received signal power is $\{50mV \cdot h_{LB}(d)\}^2$, where d is the distance. Then, we use the measured noise power in Section 6.3 to find the SNR, and consequently, derive the capacity from Equation 3 (we use B of 5 Hz as described in Section 5.2).

From Figure 6, which shows our computations of both SNR and capacity, we observe that the range of our SNR measurements across the body is 10.6 dB, and, excluding region P (that is close to the source transmitter), the difference in SNR measurements is within 5 dB. Despite the heterogeneous nature of the body, the differences of received SNR across the body is small. This is because, as the signal propagates on the channel path, the major noise source ECG also travels and gets attenuated, as we studied in Section 6.3. By injecting the signal on the torso (marked with S in Figure 6), the maximum distance to anywhere on the body is around 100 cm for people of normal height, and using our conservative lower bound for the channel amplitude model, the worst-case channel capacity across the entire body is 0.469 bits per hour (at region W).

7.3 Application to BAN

Our worst-case capacity of 0.469 bits per hour is too low for many applications. However, medical BAN applications are generally characterized by low occurrences of high-risk events (for which the other nodes in the network need to be notified) and do not require frequent exchange of secrets using our scheme. Furthermore, for key establishment applications, updates are only necessary when there is a change of infrastructure in the BAN (e.g., implanting a new device in a patient's body) which happens very rarely, or a node naturally misbehaves, which should also happen rarely. Thus, the low rate for key sharing may be acceptable.

Our scheme adheres to the BAN requirements listed in Section 1. As described in Section 7.2, the lower bound on our rate performance (0.469 bits per hour) is universal to all users. Furthermore, our scheme of using electrical signals for signaling has minimal hardware requirements, requiring only a transistor to act as a switch at the transmitter and an analog-to-digital converter at the receiver; electronic signaling does not require additional hardware for the transmitter or receiver front end, which would make the BAN device more bulky and power-consuming, since the body of the nodes are usually made of metal with high conductivity. In addition, our scheme complies with the requirement of power efficiency; it modulates slowly using a modulation known to be power-efficient.

8 Conclusion

In contrast to prior work which builds a reliable and secure scheme for key exchange while assuming correct data from physiological values, we study the process of acquiring the data measurements on physiological values and question the practicality of using such measurements for secret sharing in BAN applications. Our experiments with ECG signals (the most commonly used body physiological signals for BAN communication security) show that physiological values' measurements are not usually robust to where the sensor is deployed on the body. In particular, they yield very noisy measurements on body region that are muscular and adjacent to skeletal bone. We also discuss how such schemes leak information to outsider attackers equipped with remote sensing technology.

Our scheme uses voltage signalling operating below the action potential of human body to construct a secure side channel among the legitimate BAN members. We build and demonstrate the feasibility of our scheme on dead mouse, and analyze the capacity of our scheme by studying the human body channel with empirical data on homogeneous meat and a living human body. We adhere

to the settings of body area network applications by minimizing the hardware and processing requirement, which demonstrates the practicality of our scheme.

Acknowledgment

This material is based upon work partially supported by USARO under Contract No. W-911-NF-0710287 and by NSF under Contract No. NSF CNS-0953600. We would also like to thank Professor Jongsook Kim Kemper of the School of Molecular and Cellular Biology for providing us with the resource and environment to safely experiment with the heterogeneous tissue of dead mouse.

References

[1] ASAMI, K., TAKAHASHI, Y., AND TAKASHIMA, S. Dielectric properties of mouse lymphocytes and erythrocytes. *Biochimica et Biophysica Acta (BBA) - Molecular Cell Research 1010*, 1 (1989), 49 – 55.

[2] BALDUS, H., CORROY, S., FAZZI, A., KLABUNDE, K., AND SCHENK, T. Human-centric connectivity enabled by body-coupled communications. *Comm. Mag. 47*, 6 (June 2009), 172–178.

[3] BAO, S.-D., POON, C., ZHANG, Y.-T., AND SHEN, L.-F. Using the timing information of heartbeats as an entity identifier to secure body sensor network. *Information Technology in Biomedicine, IEEE Transactions on 12*, 6 (nov. 2008), 772 –779.

[4] BAO, S.-D., ZHANG, Y.-T., AND SHEN, L.-F. Physiological signal based entity authentication for body area sensor networks and mobile healthcare systems. *Conference Proceedings of the International Conference of IEEE Engineering in Medicine and Biology Society 3* (2005), 2455–2458.

[5] CHO, N., YOO, J., SONG, S. J., LEE, J., JEON, S., AND YOO, H. J. The human body characteristics as a signal transmission medium for intrabody communication. *IEEE Transactions on Microwave Theory And Techniques 55*, 5 (2007), 1080–1086.

[6] CORNELIUS, C., AND KOTZ, D. Recognizing whether sensors are on the same body. In *Proceedings of the 9th international conference on Pervasive computing* (Berlin, Heidelberg, 2011), Pervasive'11, Springer-Verlag, pp. 332–349.

[7] EINTHOVEN, W. Le telecardiogramme. *Arch Int de Physiol* (1906).

[8] FALCK, T., BALDUS, H., ESPINA, J., AND KLABUNDE, K. Plug 'n play simplicity for wireless medical body sensors. *Mob. Netw. Appl. 12*, 2-3 (Mar. 2007), 143–153.

[9] HALPERIN, D., HEYDT-BENJAMIN, T. S., RANSFORD, B., CLARK, S. S., DEFEND, B., MORGAN, W., FU, K., KOHNO, T., AND MAISEL, W. H. Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses. In *Proceedings of the 2008 IEEE Symposium on Security and Privacy* (Washington, DC, USA, 2008), IEEE Computer Society, pp. 129–142.

[10] KURUP, D., SCARPELLO, M., VERMEEREN, G., JOSEPH, W., DHARENENS, K., AXISA, F., MARTENS, L., GINSTE, D. V., ROGIER, H., AND VANFLETEREN, J. In-body path loss models for implants in heterogeneous human tissues using implantable slot dipole conformal flexible antennas. *EURASIP Journal on Wireless Communications and Networking* (2011).

[11] MAYRHOFER, R., AND GELLERSEN, H. Shake well before use: Intuitive and secure pairing of mobile devices. *Mobile Computing, IEEE Transactions on 8*, 6 (june 2009), 792 –806.

[12] PARTRIDGE, K., DAHLQUIST, B., VEISEH, A., CAIN, A., FOREMAN, A., GOLDBERG, J., AND BORRIELLO, G. Empirical measurements of intrabody communication performance under varied physical configurations. In *Proceedings of the 14th annual ACM symposium on User interface software and technology* (New York, NY, USA, 2001), UIST '01, ACM, pp. 183–190.

[13] PEYMAN, A., REZAZADEH, A., AND GABRIEL, C. Changes in the dielectric properties of rat tissue as a function of age at microwave frequencies. *Physics in Medicine and Biology 46*, 6 (1989).

[14] PICKHOLTZ, R., SCHILLING, D., AND MILSTEIN, L. Theory of spread-spectrum communications–a tutorial. *IEEE Transactions on Communications* (may 1982).

[15] POON, C., ZHANG, Y.-T., AND BAO, S.-D. A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health. *Communications Magazine, IEEE 44*, 4 (april 2006), 73 – 81.

[16] SAYRAFIAN-POUR, K., YANG, W.-B., HAGEDORN, J., TERRILL, J., AND YAZDANDOOST, K. A statistical path loss model for medical implant communication channels. In *Personal, Indoor and Mobile Radio Communications, 2009 IEEE 20th International Symposium on* (sept. 2009), pp. 2995 –2999.

[17] SIMON, M., OMURA, J.K., S. R., AND LEVITT, B. *Spread spectrum communications handbook*. McGraw-Hill: New York, 1994.

[18] SRIRAM, J. C., SHIN, M., CHOUDHURY, T., AND KOTZ, D. Activity-aware ecg-based patient authentication for remote health monitoring. In *Proceedings of the 2009 international conference on Multimodal interfaces* (New York, NY, USA, 2009), ICMI-MLMI '09, ACM, pp. 297–304.

[19] VENKATASUBRAMANIAN, K., BANERJEE, A., AND GUPTA, S. Pska: Usable and secure key agreement scheme for body area networks. *Information Technology in Biomedicine, IEEE Transactions on 14*, 1 (jan. 2010), 60 –68.

[20] VENKATASUBRAMANIAN, K., VENKATASUBRAMANIAN, BANERJEE, A., AND GUPTA, S. Ekg-based key agreement in body sensor networks. In *INFOCOM Workshops 2008, IEEE* (april 2008), pp. 1 –6.

[21] WEGMUELLER, M., OBERLE, M., FELBER, N., KUSTER, N., AND FICHTNER, W. Galvanical coupling for data transmission through the human body. In *Instrumentation and Measurement Technology Conference (IMTC) 2006. IEEE Proceedings* (april 2006), pp. 1686 –1689.

[22] WEGMULLER, M. S. Intra-body communication for biomedical sensor networks. *Ph.D. dissertation* (2007).

[23] XU, F., QIN, Z., TAN, C. C., WANG, B., AND LI, Q. Imdguard: Securing implantable medical devices with the external wearable guardian. In *INFOCOM* (2011), pp. 1862–1870.

[24] ZIMMERMAN, T. G. Personal area networks: near-field intrabody communication. *IBM Syst. J. 35*, 3-4 (Sept. 1996), 609–617.