Green and Sustainable Cyber-Physical Security Solutions for Body Area Networks

K. K. Venkatasubramanian, A. Banerjee, S. K. S. Gupta
IMPACT Lab (http://impact.asu.edu)
School of Computing and Informatics
Arizona State University
Tempe, Arizona 85287
{kkv,abanerj3,sandeep.gupta}@asu.edu

***Abstract*—Wireless sensor-based Body Area Networks (BAN) can play a major role in providing individualized health-care. Given their limited power sources, sensors in BAN have to be *energy-efficient* to ensure longevity and safety of the network. Recent years have seen the emergence of a new class of security solutions for BANs, called *cyber-physical security solutions*, which enable plug-n-play secure communication within a BAN using environment derived features. However, due to this environment-coupled nature, they require signal processing and mathematical routines which can be potentially very energy-intensive for individual sensors. In this paper, we characterize the "energy footprint"of a cyber-physical security solution, the Physiological signal based Key Agreement (PKA). The goal is to - 1) compute PKA's energy consumption, and 2) determine whether prominent energy scavenging techniques can be used to meet its requirements. Our results show that the energy requirements of PKA is small and is sustainable by many of the prominent energy scavenging techniques, such as body heat and ambulation, making it a "green" solution for large scale deployments.**

I. Introduction

Body Area Network (BAN) is a network of wearable and/or implantable wireless sensors, which enables pervasive, individualized, and real-time health management for the host (i.e. patient) it is deployed on [10]. Energy efficiency for sensors on the BAN is very important, primarily to improve the *sustainability* of the network, given the limited powering source available at each sensor. Sustainability is particularly useful in large scale deployments of BAN, as it improves the technology's eco-friendliness and green nature. For example, energy self-sufficiency using energy scavenging reduces the dependence on environment-unfriendly batteries. Additionally, it makes the BAN safer for the human body and has the potential to make BAN solutions more cost-effective. This need for energy-efficiency gains even more importance when sensors in a BAN implement secure communication protocols.

Recent years have seen the development of a new class of protocols called *cyber-physical security solutions*, which enable a plug-n-play secure inter-sensor communication within a BAN. These solutions are tightly coupled with their environment - the human body and require many signal processing and mathematical routines in order to function [13]. These requirements can potentially impose considerable overhead on individual sensors in terms of energy requirement. In [1], we illustrated our ability to successfully implement one such cyber-physical solution, called *Physiological signal based Key Agreement (PKA)* on a Crossbow mote-based BAN environment. Here we evaluate its energy requirements, which is very essential to establish the overall utility of the scheme for BANs.

In this paper, we characterize the energy consumption (footprint) of PKA. We analyze footprint of PKA to determine the aspects of the PKA protocol that are the most expensive, energy-wise. We analyze both the computation and communication energy costs for PKA, which we believe are comparable; the former therefore cannot be ignored as was done by many prominent non-cyber physical solutions [7] [16]. We further investigate prominent energy scavenging techniques to determine whether they can meet PKA's energy requirements. The principal motivation is to evaluate the possibility of eliminating the energy cost of utilizing PKA, within a BAN. In a way, by showing that energy scavenging can be used to meet PKA's energy requirements, we are extending its plug-n-play nature from a solely security perspective to its operation as well (the operation of PKA does not require any maintenance by the BAN user; deployment alone is sufficient).

The *contributions* of the paper are as follows: 1) Determination of the energy consumed by PKA and its various components, at different settings[1], by executing it on a mote platform instrumented to measure energy consumption; 2) Analysis of the results obtained to determine the energy-intensive components of the PKA, along with the overall computation and communication energy costs associated with it; and 3) Identification of the energy scavenging techniques which can meet these requirements. Our results show that PKA energy consumption increases as the security provided by it increases. When PKA provides the highest security for our implementation, it consumes an average power of 53.5mW and maximum power of 58.8mW, in the worst case (when the mote transceiver is always on). Further, the results show that the energy requirements of PKA have a comparable computation and communication component. Finally, the overall energy footprint of PKA is small enough to be sustainable by many of the prominent energy scavenging techniques, such as the body heat and the ambulation; thus making it more eco-friendly.

[1]PKA can be customized to provided different levels of security. In our implementation, we achieve security equivalent to brute-forcing 55 bit key up to 65 bit key. Higher security (more than 128 bits) is theoretically possible [13] but requires a more capable hardware

TABLE I
PKA Execution Parameters

Parameters	**Values**
Sampling	60 Hz
Sampling Duration	12.8 secs
FFT	256 points, 5 windows[a]
Polynomial Order	6
Feature Length	4 bytes
Polynomial Projection	4 bytes
Vault Size (Legit. and Chaff Points)	1K-5K
Vault Element Size	8 bytes
Vault Message Pckt Size	80 bytes (10 elements/pckt)
Acknowledge Pckt Size	30 bytes

[a] First 32 points/window were concatenated together for peak based feature generation

The paper is organized as follows, Section II presents a brief overview of the PKA protocol, followed by Section III, which defines the energy model which we utilize for our analysis. Section IV presents our experimental setup, results and analysis, followed by Section V, which presents some energy scavenging techniques which can meet PKA's energy requirement. Finally, Section VI concludes the paper.

II. Physiological signal based Key Agreement

In this section we review Physiological signals based Key Agreement (PKA) proposed first in [13] and utilized photoplethysmogram (PPG) signal based features to enable two sensors to agree on a common key.

Initially, both the sensors measure PPG signal in a loosely synchronized manner. A set of frequency domain features are then generated by first performing a windowed (256 point) FFT on the PPG signals and then detecting the peaks in the FFT coefficients. Peaks are local maxima in FFT coefficients. Features are then derived from the peaks by generating tuples each of which record a peak-value and its corresponding peak-index. These tuples (features) are then quantized and concatenated to form a feature vector.

Once the features have been generated, one of the two communicating sensors (designated sender) generates a random symmetric key (128bits long, longer keys can also be used) which it then hides using the feature vector obtained from the PPG signal. For this purpose of hiding the key a *fuzzy vault* cryptographic primitive [3] is used. The hiding process works as follows - 1) the sender generates a vth order polynomial (we choose 6th order for ease of implementation, higher orders are possible and provide greater security [13]), the coefficients of which are populated by the secret key which is to be hidden, 2) it then computes the polynomial at each of the points in the feature vector generated from the frequency domain representation of PPG signals, 3) each feature in the feature vector and its projection on the polynomial forms a set of *legitimate* coordinates of the form (x-value,y-value) which are then obscured by adding a large number of bogus, random coordinates called *chaff points*. Security of PKA is proportional to the size of the vault - i.e. number of chaff points [13]. This set of legitimate points and chaff points is called a *fuzzy vault*, and each coordinate point in it are called the *elements of the vault*. The vault is then transmitted to the other sensor (designated receiver) via the wireless medium. The receiver

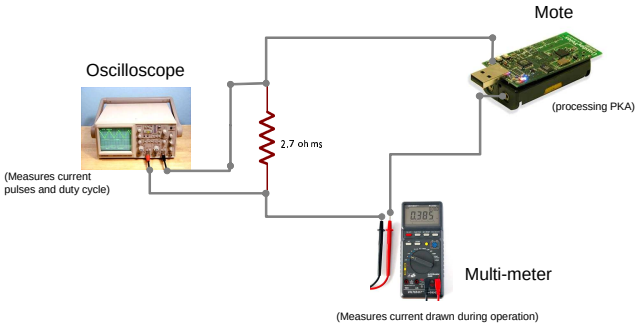

Fig. 1. **Energy Measurement Setup**

upon receiving the vault, identifies $v+1$ elements from the vault whose x-values are identical to its own feature values and tries to re-construct the polynomial hiding the secret key using *Lagrangian Interpolation*. Once it has generated the correct polynomial, it sends back an acknowledgment. Any adversary eavesdropping on this conversation does not know the legitimate points from the chaff and has to try all possible combinations of size $v+1$ from the vault to arrive at the correct key, which can be prohibitively expensive.

PKA thus involves a number of computationally complex stages such as computation of FFT, peak detection in signals, evaluation of polynomials, and interpolation of a polynomial from a set of points. It further, requires the communication of the entire vault for successful key agreement. Implementing each of these techniques on motes require many approximation and were still computation, memory and communication wise intensive compared to traditional mote based applications [1]. Table I shows our chosen parameters for implementing PPG-based PKA.

III. PKA Energy Analysis

In order to compute and analyze the energy consumption of PKA, we first define the energy consumption model used by us. We then compute the energy consumed by different stages of PKA and finally analyze them in detail. Before we present the energy model and its analysis, we give a brief description of our implementation setup.

A. Implementation Setup

A prototype of the PKA protocol was implemented as a part of the Ayushman health monitoring system [4] using photoplethysmogram (PPG) as the physiological signal of choice. We chose PPG signals because it allowed us to verify the validity of our results based on a *benchmark implementation* using Matlab which was presented in [13]. PPG signals measure the volumetric change in the distension of arteries due to the perfusion of blood through them during a cardiac cycle. We used Smith Medical pulse oximeter boards (specifications can be found at http://www.smithsoem.com/ applications/ oxiboards.htm) to collect the data from the volunteers. We used two TelosB motes with 8MHz processor to execute PKA.

B. Energy Model

There are two distinct components to energy consumption in PKA that we need to consider. The first is the *computational energy cost*, which quantifies the amount of energy consumed

TABLE II
PKA Stages' Current Draw and Timing Results

Mote	Stage	Current Draw (Radio-Off)	Current Draw (Radio-On)	Time (msec)
Sender/Receiver	Sensing	6.6mA	6.6mA	12800
	FFT Computation	1mA	19.56mA	2138
	Peak Detection and Quantiz.	0.14mA	18.72mA	12.4
	Feature Generation	0.11mA	18.72mA	13.6
Sender	Polynomial Gen. & Eval.	0.08mA	18.68mA	8
	Chaff Points Gen.	0.01mA	18.61mA	14
	Vault Tx (Size = 1K,2K,3K,4K,5K)	-	19.33mA	1350(1K), 2700(2K), 4000(3K), 5360(4K), 6750(5K)
	Ack Rx	-	19.20mA	20
Receiver	Vault Rx (Size = 1K,2K,3K,4K,5K)	-	19.41mA	1400(1K), 2750(2K), 4100(3K), 5370(4K), 6760(5K)
	Lagrangian Interpolation	0.43mA	19.04mA	50
	Ack Tx	-	19.11mA	17

during the execution of PKA, while the second is the communication energy, which quantifies the energy consumed in transmitting and receiving the vault. Traditionally, in the domain of sensor networks, the prevailing assumption has been that *communication energy costs* overwhelm computational costs. However due to the considerable processing requirement of PKA in terms of FFT computation, feature generation, polynomial generation, evaluation and Lagrangian interpolation, we suspect computational costs to be substantial portion of the total energy costs.

1) Computational Energy Consumption Model: Our energy model is based on the on-line energy estimation model described in [2]. The idea behind the model is to determine the time for which each hardware component in the system is on or off, and the current it draws during the process (functioning and idle). Energy consumed can then be determined by multiplying the current and time with the supply voltage (V). More formally, the model can be represented using the following linear equation:

$$E_{comp} = V \times (I_{pr}t_{pr} + I_{ps}t_{ps} + \sum_i I_{c_i}t_{c_i}) \quad (1)$$

Here, E_{comp} is the computational energy cost, V is the voltage used by the system, I_{pr} and t_{pr} are the current draw when the processor is running and the time for which it is running, respectively, I_{ps} and t_{ps} are the current draw when the processor is in the idle mode and the time for which it is in that mode, respectively, and $\sum_i I_{c_i}t_{c_i}$ gives the current and time required for the other components on the mote, for example sensing.

2) Communication Energy Consumption Model: The second important aspect is the communication energy requirements of PKA. We again use a model similar to the one computational one here by determining the time spent in transmission of the packets and time current drawn in process, and time spent in the receiver mode and its corresponding current draw. More formally:

$$E_{comm} = V \times (I_{tx}t_{tx} + I_{rx}t_{rx} + I_{roff}t_{roff}) \quad (2)$$

Here, E_{comm} is the computational energy cost, I_{tx} and I_{rx} are the current draw by the transceiver during transmission and reception, respectively, t_{tx} and t_{rx} is the time taken for transmission and reception respectively. While I_{roff} and t_{roff} are the current draw when the transceiver is switched off and the duration for which it is off, respectively, and V is the supply voltage.

IV. Energy Consumption of PKA

In this section, we present the result and analysis of the energy consumption of PKA protocol. Our results were through instrumentation of an implementation of PKA, using which we directly measured the current drawn for different stages of PKA and their duration of execution. Our aim was to determine the energy consumed by various stages of PKA for *one complete iteration of PKA*. We begin by describing our experimental setup and our results and then move on to analyzing them.

A. Results

The aim of the experiments was to determine the current drawn and its duration in different stages of the PKA execution so as to determine the energy consumed based on our energy models. In order to do so, we established an experimental setup as shown in Figure 1. As mentioned earlier, the protocol was executed on a pair of TelosB motes which attempted to use PPG signal from the human body in order to agree on a common key. Across the two power leads of the mote, a small resistance (2.7 ohm) was connected in series with an ammeter. An oscilloscope was connected across the resistance so as to visualize the voltage pulses generated (across the resistor) and to measure their duty cycle. The resistance value was chosen such that the voltage generated across it by the current pulse is clearly visible in the oscilloscope. Care was taken that the resistance chosen is not too large to affect the input impedance of the mote (which acts as a current source in this case).

In order to be able to analyze the energy consumption of the PKA protocol, our energy measurements divided a single execution of the protocol into eleven stages: 1) Sensing 2)

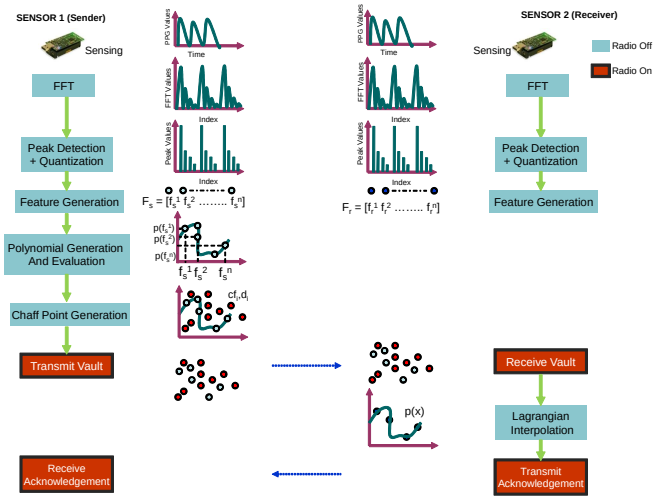

Fig. 2. Stages of PKA Protocol

FFT Computation, 3) Peak Detection and Quantization, 4) Feature Generation, 5) Polynomial Generation and Evaluation, 6) Chaff Points Generation, 7) Transmission of Vault, 8) Reception of Vault, 9) Lagrangian Interpolation, 10) Transmission of Ack, and 11) Reception of Ack. Stages 2 through 4 were executed by both the sender and receiver motes. Stages 5–7 and 11 were executed only by the sender, while Stages 8–10 were executed by the receiver only. We performed two sets of experiments, one with radio on during the entire execution of the PKA, in order to see the worst-case performance of the protocol. In the other experiment, the radio was switched on only when needed, i.e. when the sender and receiver are expecting to receive a message or transmit a packet (Stages 7–11 for sender, and Stages 7–9 and 10 for the receiver). For brevity, in the rest of the paper, we refer to the former set of experiments as *Radio-On* and latter as *Radio-Off*. Figure 2 shows the various stages of PKA protocol and which ones are put in idle state for the Radio-Off experiments.

Table II shows the results obtained from our experiments. The values closely match those reported for different functions of a TelosB mote in its original evaluation [8]. It can be seen from these results that the FFT computation, vault communication and acknowledgment, and Lagrangian interpolation are the most expensive stages in terms of computation. When the processor is in the idle state, we found that the mote consumed 0.01mA when radio was off, and 18.60mA when the radio was on. It can be seen that the current draw for the Radio-On experiment goes up dramatically for the mote. Now that we have the current draw results, we can now analyze the energy consumption of the entire protocol.

B. Analysis

The analysis of the energy consumption results has two parts: analyzing the energy costs for PKA, and analyzing the computation and communication energy costs for the protocol. The primary source of security for PKA for a given polynomial order is the number of elements in the vault. The larger the vault, the greater the number of combinations an attacker has to try to arrive at the correct key [13]. We therefore compare the energy consumed by one complete execution of PKA with respect to different chaff points in the vault.

Figure 3(a) shows the overall energy consumption by the sender and receiver for executing the protocol at five different vault sizes. The energy consumed in creating and opening larger vaults is greater than small vaults. This is because smaller vaults have lesser number of chaff points which sender needs to add to the legitimate points. Consequently lesser the number of packets need to be transmitted in order to communicate the vault to the receiver. Similarly, at the receiver's end, the number of combinations of the vault elements that the receiver has to compare with its own feature points, to identify the polynomial, is much smaller along with the time taken to receive the vault itself. Further, in the Radio-On experiment the receiver consumes slightly more energy than the sender as more current is drawn in receiving the packets than sending them. In the Radio-Off experiment, the sender consumes much less energy because it gets to remain off longer. These results underline the traditional *trade-off between security and energy*.

Figure 3(b) shows the computational energy consumption, for both sender and receiver during both Radio-Off and Radio-Off experiments with respect to the cost of sensing the PPG signal (which is a constant value). As expected, the cost of computing the larger vaults causes the energy consumption for the mote to go up as the vault size increases. Similarly, Figure 3(c) shows the communication energy consumption with respect to sensing cost, for both sender and receiver. It shows an increase in energy cost as the vault size increases due to the increased number of packets that need to be transmitted from the sender to the receiver. In both cases, for Radio-Off experiment, the sender consumes much less energy than all others because it gets to remain off longer.

We then compared the percentage of energy cost that computation takes compared to communication. Figure 3 (d) shows the results of our comparison which plots the ratio of computation cost and communication cost for different vault sizes. We find that for smaller vault sizes, the cost of computation outweighs communication by a factor of almost two (for Radio-On). But for larger vault sizes, which require extensive communication, the associated cost pre-dominates. This shows that computation energy cost for PKA is comparable to the communication energy cost, and should not be ignored. For Radio-Off experiments, the cost of computation is comparable to communication for receiver, and much lower for the sender.

The energy consumption for PKA essentially describes the cost of having a plug-n-play key agreement protocol. Traditional key agreement protocols either utilize key predeployment [7] or public key cryptography [5]. Key predeployment is free as it based on manual initialization, while Elliptic Curve Cryptosystem Diffie-Hellman (DH-ECC) protocol distributing a 163 bit key consumes about, 0.8J on the mote platform [5]. This illustrates the other important trade-off when it comes to PKA: *trade-off between usability and energy*. Highly usable solutions also have a greater cost, and this property needs to be considered when deploying BANs.

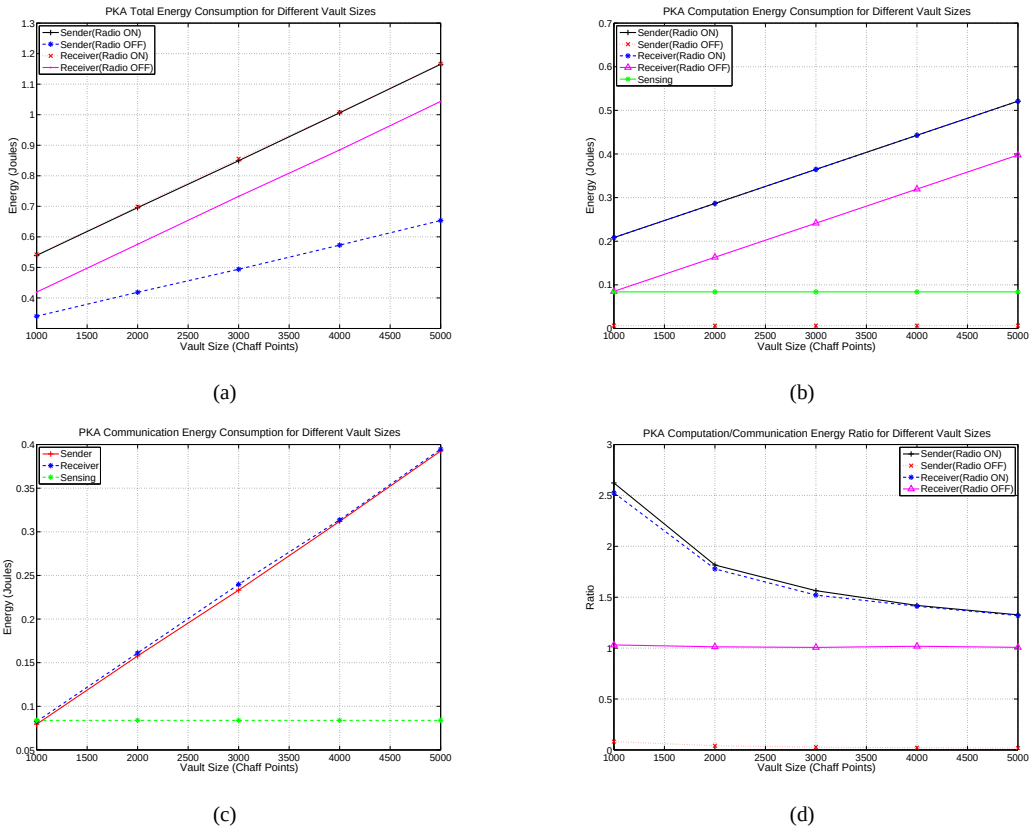

Fig. 3. a) Energy consumption for PKA protocol for different vault sizes, b) Energy consumed by the computation requirements of PKA for different vault sizes, c) Energy consumed by the communication requirements of PKA for different vault sizes, d) Ratio of energy computation and communication energy for different vault sizes.

V. Energy Scavenging

Now that we know the energy requirements of PKA, in this section we present a semi-formal discussion on the possibility of utilizing energy scavenging techniques in order to meet its (PKA's) requirements. The reason for investigating the use of energy scavenging techniques for "powering" PKA is to investigate if it can be made self-sufficient in terms of energy. Again, we focus on evaluating the scavenging techniques for powering the mote for one complete execution of PKA. We believe this ability to use energy scavenging to meet its requirements, enhances the plug-n-play nature of PKA by making it transparent to its users (host of the BAN) in terms of its energy requirements as well.

Currently, the TelosB motes that are being used to implement PKA in the BAN use AA batteries, from which they draw power for their operation. A typical AA battery has a voltage rating of 1.5 V and is rated at 2600 mAHour at 19 mA current (http://data.energizer.com/PDFs/E91.pdf). In the worst case (Radio-On scenario[2] at vault size of 5000 for the receiver), PKA requires an average power of 53.5mW (1.1665J energy for 21.8 seconds). The maximum power consumed by PKA is 58.8mW during the FFT computation. Thus with two AA batteries, used in the motes, we can run more than 6000 iterations of PKA. This is not a surprising result. To put things in perspective, the cost of normal operation of a mote (assuming it requires sensing, processing and transmission of a 30 byte data every n seconds) roughly consumes a maximum power of 57mW (during data communication). PKA versions with larger vault sizes or polynomial orders will be much more expensive. However, if we do not execute PKA regularly the overall effect of PKA on the mote can be lowered.

However, our aim here is to make PKA transparent to its users with respect to its energy requirements. We therefore look at some of the prominent energy scavenging techniques that can balance the energy requirement of PKA so that the motes battery be "spared", allowing it to be used for the regular sensing processing storing and transmitting operations. Much work has been done in energy scavenging in the domain for wearable sensors [9] [14] [15]. The focus of these works is mainly on developing hardware for scavenging. In [6] [11] the authors present a comprehensive study of the amount of energy available to be scavenged from different sources on the human body in for operating mobile devices.

In this work we discuss four prominent sources from which we can scavenge energy for running PKA. Note that we assume an *on-the-fly energy provisioning model* in which the energy is consumed as it is generated.

- **Body Heat:** Human body heat is a source of energy that can be scavenged. In [6], the authors suggest the use of neck braces that can be worn by host of the BAN

[2]We only consider the case of Radio On in this analysis as meet its energy requirement is guaranteed to meet the requirement of the Radio Off scenario.

TABLE III
Energy Scavenging Techniques for PKA

Scavenging Techniques	Source	Power Gain	Ideal Deployment Scenario
Body Heat	Latent heat of vaporization of perspiration	0.2W - 0.32W	Most Cases
Respiration	Chest expansion from breathing	420mW	Strenuous Physical Activity
Ambulation	Arm & leg movement	1.5W-1.6W	Physical Movement
Photovoltaic Cells	Sunlight	$100mW/cm^2$	Exposure to sun

to enable the scavenging. These neck braces scavenge energy from the latent heat of vaporization occurring due to the vaporization of the perspiration of the individual. The estimated power gain is 0.2 W to 0.32 W with this approach, which is sufficient for PKA.

- **Respiration:** Any form of movement on the body can be used to scavenge energy [6]. One of the prominent movement is due to respiration. It is estimated that about 420 mW of power can be extracted from a stretchable dielectric elastic band worn around the chest of an individual. This amount of power is sufficient for PKA, but can be extracted only from heavy breathing.
- **Ambulation:** Demonstrated systems have been successful in recovering 1.5 W of power from the human arm motion and more than 1.6 W of power from the ambulatory motion of human beings (using piezo-electric soles in shoes) [6], which is sufficient for PKA.
- **Photovoltaic Cells:** Photovoltaic cells can produce 100 mW/cm^2 of power when under sunlight [6], which is again sufficient for PKA.

It can be seen that PKA in the worst-case is energy-efficient enough to be sustained by each one of energy scavenging techniques described above. Further, eliminating the need for batteries also improves the overall green-nature of the scheme. Other sources such as those which depend upon vibration, blood pressure or from radio transmission have also been developed [11], but they do not provide enough energy to meet the requirements of a single execution of PKA. It can be seen from the energy characterization of PKA that these techniques are sufficient to sustain the PKA operation in a mote. The choice of a particular technique depends upon the scenario of deployment. For example, in the case of a patient who is completely bed-ridden one cannot use the energy scavenging techniques that are dependent on ambulation or on heavy breathing. Other techniques such as photovoltaic cells or body heat have to be used. However for an athlete the energy scavenging system can make use of the physical movements or the heavy breathing to generate enough energy for executing PKA. Table III summarizes the results.

VI. Conclusions and Future Work

In this work, we studied the energy requirements of a cyber-physical security solution (PKA) for BANs. The study was performed on the Crossbow mote platform and we found that the energy footprint of PKA is sustainable by the prominent energy scavenging techniques. Further, we found that the computational cost for the protocol is comparable to the communication cost and cannot be ignored. An important aspect of energy-efficiency that has not been considered in this paper is the need to minimize the detrimental effects of the sensors on their environment, i.e. improving BAN safety. For example, minimizing excessive heat dissipation on the tissue near the sensors due to their operation while maintaining the desired security level [12]. This interaction and trade-off between security and safety is an open research issue to be considered in our future work.

Acknowledgments

This research was funded in part by National Science Foundation Grant CNS-0831544. The authors would like to thank Georgios Varsamopoulos of IMPACT Lab, for help with improving the readability of the paper.

References

[1] A. Banerjee, K. Venkatasubramanian, and S. K. S. Gupta. Challenges of Implementing Cyber-Physical Security Solutions in Body Area Networks. April 2009. In Proc. of 4th International Conference on Body Area Networks (Accepted for Publication).

[2] A. Dunkels, F. Osterlind, N. Tsiftes, and Z. He. Demo-software-based sensor node energy estimation. pages 409–410, Nov 2007. In Proc. 5th ACM Conference on Embedded Networked Sensor Systems.

[3] A. Juels and M. Sudan. A Fuzzy Vault Scheme. page 408, 2002. In Proc. of IEEE Intl. Symp. on Inf. Theory.

[4] K. Venkatasubramanian et. al. Ayushman: A Wireless Sensor Network Based Health Monitoring Infrastructure and Testbed. In *Distributed Computing in Sensor Systems*, pages 406–407, July 2005.

[5] D. J. Malan, M. Welsh, and M. D. Smith. A Public-Key Infrastructure for Key Distribution in TinyOS Based on Elliptic Curve Cryptography. pages 71–80, Oct 2004. In Proc. of IEEE 2nd Intl. Conf. on Sensor & Ad Hoc Comm. & Networks.

[6] J. A. Paradiso and T. Starner. Energy scavenging for mobile and wireless electronics. *Pervasive Computing, IEEE*, 4(1):18–27, Jan.-March 2005.

[7] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and D. Tygar. SPINS: Security Protocol for Sensor Networks. *Wireless Networks*, 8(5):521–534, September 2002.

[8] J. Polastre, R. Szewczyk, and D. Culler. Telos: enabling ultra-low power wireless research. In *Proc. of the 4th international symposium on Information processing in sensor networks*, 2005.

[9] E. K. Reilly, E. Carleton, and P. K. Wright. Thin film piezoelectric energy scavenging systems for long term medical monitoring. In *BSN '06: Proceedings of the International Workshop on Wearable and Implantable Body Sensor Networks*, pages 38–41, 2006.

[10] L. Schwiebert, S. K. S. Gupta, and J. Weinmann. Research challenges in wireless networks of biomedical sensors. pages 151–165, July 2001. In Proceedings of the 7th Annual ACM/IEEE International Conference on Mobile Computing and Networking.

[11] T. Starner and J. A. Paradiso. Human generated power for mobile electronics. In *Low Power Electronics Design*, pages 1–35. CRC Press, 2004.

[12] Q. Tang, N. Tummala, S. K. S. Gupta, and L. Schwiebert. Communication scheduling to minimize thermal effects of implanted biosensor networks in homogeneous tissue. *IEEE Transactions on Biomedical Engineering*, 52(7):1285–1294, July 2005.

[13] K. Venkatasubramanian, A. Banerjee, and S. K. S. Gupta. Plethysmogram-based Secure Inter-Sensor Communication in Body Area Networks. pages 1–7, November 2008. In Proc. of IEEE Military Communications Conference.

[14] E. Yeatman, D. O'Hare, C. Dobson, and E. Bitziou. Approaches to self-powered biochemical sensors for in-vivo applications. In *Proc. of 3rd International Conference on Body Area Networks*, pages 1–2, 2008.

[15] E. M. Yeatman. Rotating and gyroscopic mems energy scavenging. *Wearable and Implantable Body Sensor Networks, International Workshop on*, pages 42–45, 2006.

[16] S. Zhu, S. Setia, and S. Jajodia. LEAP+: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks. *ACM Trans. on Sensor Networks (TOSN)*, 2(4):500–528, Nov 2006.