Secret Key Generation Rate vs. Reconciliation Cost using Wireless Channel Characteristics in Body Area Networks

Syed Taha Ali and Vijay Sivaraman
School of Electrical Engineering and Telecommunications
University of New South Wales, Australia
Email: taha@student.unsw.edu.au, vijay@unsw.edu.au

Diethelm Ostry
ICT Centre, CSIRO
Australia
Email: diet.ostry@csiro.au

***Abstract*—In this paper, we investigate the feasibility of real-time derivation of cryptographic keys in body area networks using unique characteristics of the underlying wireless channel. We perform experiments to confirm that motion does indeed provide significant highly correlated randomness on either end of the wireless link between basestation and mobile mote to enable real-time key generation. Furthermore, we demonstrate that channel characteristics for a dynamic body area network consist of two different components, a fast and a slow component, each of which make a qualitatively different contribution to key generation. These components can be isolated to address specific needs of the application scenario: the fast component can yield high entropy keys at a fast rate between basestation and mobile mote with some bit disagreement between the two devices; the slow component generates keys at a lower rate but with very high level of bit agreement. Our experimental results highlight this tradeoff, and our key generation protocol details the key extraction process.**

I. Introduction

Due to burgeoning national health expenditures and an escalating number of age-related disabilities, there is a great push in researching and deploying wireless sensor networks in healthcare. These body area networks, as they are referred to, typically consist of small sensors mounted on the human body that record vital signs and communicate wirelessly with a basestation for real-time analysis and archival. It is anticipated that the market for wearable wireless sensor devices will grow to more than 420 million devices by 2014 [1]. Securing these devices is a critical concern given the ethical and legal obligations attached to medical data. Wireless sensor devices are generally characterized by low power and very limited computation resources and therefore security implementation presents significant challenges.

Secret key agreement has significant advantages for body area networks: two devices would be able to generate new keys dynamically for communication. Key management would be greatly simplified, network entities would be freed from reliance on trusted third party servers which may not be always accessible, and devices would be able to form secure ad hoc networks. Furthermore, we anticipate most users of such devices may not have the motivation or skills to manually configure and keep track of secret keys for different devices.

The most popular secret key agreement mechanism is the Diffie-Hellman Key exchange which allows two endpoints, Alice and Bob, to securely agree upon a secret key communicating on an open channel in the presence of an eavesdropper, Eve. This method, however, requires complex exponentiation operations or, in the case of ECC variants (e.g. ECDH), scalar multiplication, which consumes significant time and resources on small sensor devices. In certain instances, the time to perform an ECDH key exchange on a wireless sensor device takes several tens of seconds [2]. In this paper, we explore an alternate approach that originates from information theoretic research, specifically, the concept of using temporal-spatial properties of the wireless link between two devices to dynamically generate secret keys.

For two communicating parties, Alice and Bob, the multi-path properties of a wireless channel are identical on both ends of the link. This channel response will be unique to Alice and Bob and motion on their part or in the environment gives rise to unpredictable variations in channel response due to multipath. In this case, the wireless channel shared by Alice and Bob can be considered as two correlated sources of random data that Alice and Bob can effectively extract secret keys from. The channel response is also spatially specific. In a multipath environment, due to scatter effects, an eavesdropper, Eve, who can receive all the exchanged traffic will essentially be measuring a different channel and would be unable to replicate the key.

Different channel characteristics have been considered for this purpose in the literature, including radio signal strength [3] [4], signal envelope [5] and signal phase [6]. We specifically use the received signal strength (RSS) because it is the most convenient to measure for most small devices.

In this paper, we present results of experiments where we collect and analyze wireless channel characteristics using one and more body-worn devices communicating in the presence of multiple eavesdroppers. Our findings indicate that channel variation in a dynamic body area network is very dependent not just on motion itself but also on mobility, i.e. the change in distance between the two devices and body orientation. These gives rise, respectively, to a **fast** and a **slow** component, and it

is especially significant that these distinct components can be processed separately to cater to specific application scenarios. The fast component typically yields secret keys at a very high rate, and is suited for highly dynamic scenarios such as athlete monitoring or disaster recovery or bootstrapping systems. However, this component also generates some mismatch between the two communicating parties, entailing the need for a bit correction or information reconciliation mechanism, thereby adding complexity and overhead. The slow component, on the other hand, can be mined for keys at a lower rate, but the bit agreement between both parties is very high and the reconciliation phase can be dispensed with entirely. This approach is more suited for general healthcare and long term patient monitoring where there is more flexibility in key generation and the implementation is relatively simple. We discuss this tradeoff in greater detail in later sections.

This paper makes the following contributions:

1) We verify experimentally that motion in a body area network creates significant correlated channel variation which can be effectively harnessed to generate secret keys in the presence of multiple eavesdroppers.
2) We describe a complete mechanism for isolating the components and extracting secret keys.
3) We present experimental results highlighting the differences in performance using the two components and suggest how they could be exploited to suit specific applications.

The rest of this paper is organized as follows: Section II covers prior work in this domain; Section III describes our experimental setup and discusses results; Section IV lists operating assumptions and presents our key generation mechanism; Section V analyzes performance and presents results. We conclude in Section VI.

II. Prior Work

Our work adds to the current research in using wireless channel characteristics to generate shared keys between two devices. A theoretical foundation for this approach is laid in [7] and [8] where the authors demonstrate that two parties, Alice and Bob, can generate secret keys using correlated information in the presence of an eavesdropper, Eve. The process generally consists of four distinct phases: Alice and Bob first *sample* the channel to exchange correlated information which Eve can only partially obtain by eavesdropping. Since most radios are half-duplex, the channel cannot be sampled simultaneously at both ends and sampling messages need to be sent in quick succession. The information obtained is then *quantized* to yield a bitstring. Alice and Bob then *reconcile* errors in their bitstrings by exchanging error correction messages or discarding mismatched bits. Different protocols have been proposed for information reconciliation [9]. In the final stage, *privacy amplification*, Alice and Bob reduce the amount of information available to Eve by discarding or rearranging some bits in their strings.

Work in this area has mostly focussed on methods for causing channel variation and on innovating quantizer design. Different quantization mechanisms for RSSI have been described for 802.11 WiFi in [10] and extended in [3]. In the latter, the authors consider the case of mobile entities and they present experimental results collected using two mobile laptops. They discover that dynamic scenarios can yield high entropy keys at a fast rate.

Wireless sensor devices have been specifically considered in [11] and [4]. In the first, the authors implement and test a ranking method on TelosB wireless motes which are randomly moved, to extract keys at very high rate. In [4], the authors vary channel frequency to vary channel response for MICAz motes and satisfactorily extract keys with high rate of key agreement. They specifically consider stationary deployments.

In [12], the authors investigate specifically the question of whether the near-body radio channel in body area networks can provide enough randomness to generate secret keys between two body-worn devices. Their results are based on simulation modeling of a near-body channel and indicate a potential key-generation rate of about 2 bits/second. The authors do not examine the actual key generation process itself.

To the best of our knowledge, we are the first to consider the case of motion specifically within a body area network, and, as our results indicate (in Section), discover that channel variation is seen to comprise two distinct components, a slow one and a fast one. Other work in this domain does not study the channel variation in great detail. Our contribution is unique in that we identify and describe these components and show how their individual properties can be harnessed for the key generation process.

III. Experimental Characterization of Channel Variation due to Motion in Body Area Network

We conducted experiments to study and characterize channel variation due to motion. Experiments were performed in an office space consisting of multiple cubicles (experimental arrangement in Fig.1). We used MicaZ motes, running TinyOS and operating in the 2.4 GHz band. The basestation and mobile mote are tagged as Alice and Bob, and multiple passive eavesdroppers, labeled Eve1, Eve2, and so on, are placed at various locations as depicted. The mobile mote is strapped on to the subject's right arm (Fig.2). Alice and Bob transmit 25 probe packets per second and sample the channel continuously. We collected RSSI traces for three different scenarios: in the first two, **Resting** and **Walking**, the basestation is stationary, and in the third, **Walking with Body Worn Network**, the basestation is also mounted on the human subject as he moves.

In the first instance, **Resting**, the subject is sitting in a chair facing the basestation at a distance of approximately 1.5 m. The mobile mote records the RSSI (received signal strength indicator) for the probe packets received from the basestation. The basestation and eavesdroppers record the RSSI for the probes transmitted by the mobile mote. The eavesdroppers do not record RSSI for probes transmitted by the basestation because the basestation is stationary for most of the scenarios and, the channel variation does not yield any useful data. Fig.3 plots the variation in RSSI for the basestation, the mobile mote

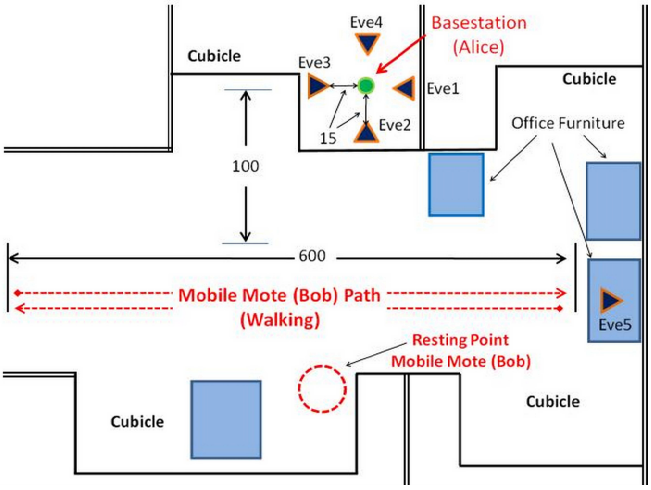


Fig. 1. Layout of Experimental Setup showing position of Basestation and Eavesdroppers and path taken by Mobile Mote (distances in cm)

Fig. 2. Mobile Mote on subject's arm

and select eavesdroppers. Results for the other eavesdroppers are fairly similar and are omitted for clarity.

As expected, the channel variation in the resting case is minimal and is only of about 2 dB from the mean. There are also significant differences in the two curves for basestation and mobile device, indicating low channel reciprocity. In fact, it can be seen that results for the mobile mote do not correlate with those of the basestation any better than those of Eve1. Eve5 is placed at a distance of about 3 m from the resting point and encounters significant packet loss (indicated by the large number of spikes reaching -94 dB).

In the second instance, **Walking**, the subject walks back and forth at a moderate pace along the path shown in Fig.1. Results for basestation and mobile mote RSSI values are plotted in Fig.4. For clarity, eavesdroppers' results are presented in Fig 5 which shows the variation at higher resolution. We note that the variation in the channel is over a greater range and there is a high degree of reciprocity between the basestation and the mobile mote, whereas the eavesdroppers are unable to replicate the variation in significant detail. The periodicity of the curves matches the back and forth walk of the subject: the peaks occur when the subject passes the basestation device such that the mobile mote directly faces it. The troughs occur when the subject is turning at the end of the path and the

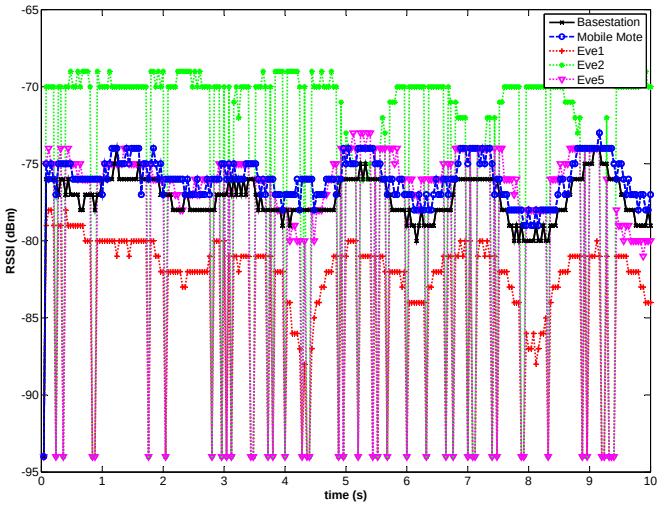


Fig. 3. Variation in RSSI for Resting Scenario

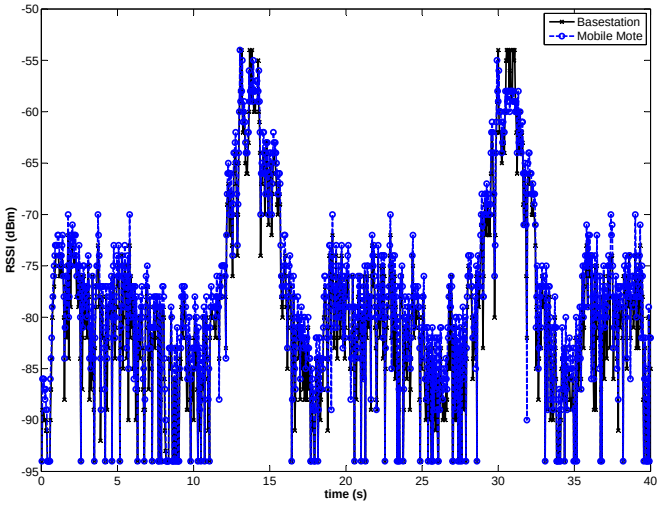


Fig. 4. Variation in RSSI for Walking Scenario

human body directly obstructs the line of sight between the two devices.

The results also present another very interesting insight: the channel variations can be seen to comprise two distinct components, a **slow component**, corresponding to the slow-varying shape of the curve, which has a longer period (approximately 15 seconds) and amplitude ranging from -94 dB to -54 dB. The **fast component** is overlaid on this and varies at a much faster rate and has far smaller range. In Fig.6, we use the Savitzky Golay filter [13] to isolate these two components and examine their feasibility for individual key generation. This filter performs a local polynomial regression and is ideal because it preserves the essential slow-moving features of the distribution. Fig.6(a) shows a segment of our baseline,

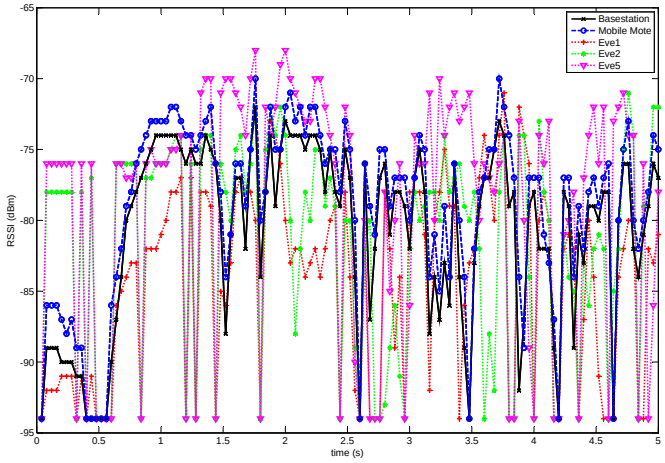
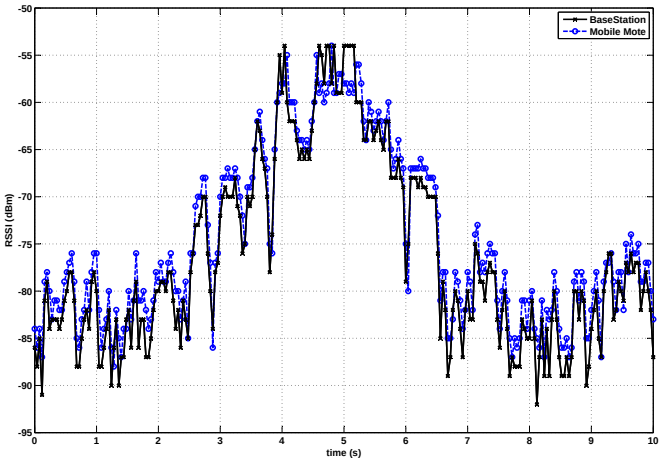


Fig. 5. Variation in RSSI for Walking Scenario (Detail.)

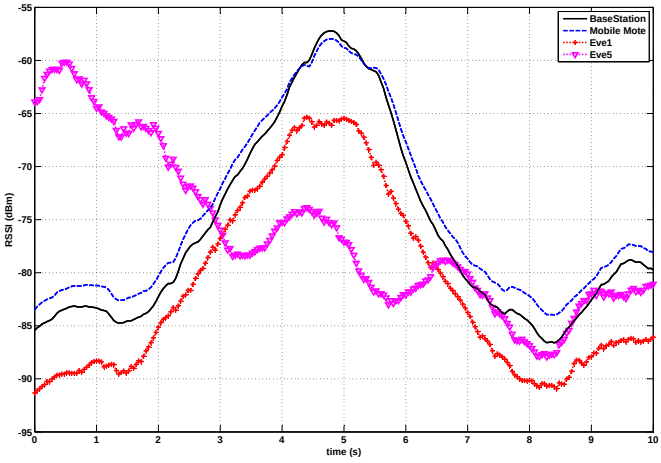
the original distribution of channel variation for basestation and mobile mote, to which the filter is applied to isolate the respective slow components in Fig.6(b). The fast components are obtained by subtracting the slow components from the original distribution in Fig.6(c). The filter is also applied to the results of two eavesdroppers.

Both components for basestation and mobile device appear correlated and show potential for key generation. Also, both can be seen to have distinct properties: the slow component varies at a slower rate and is the result of the changing distance between the two parties and the orientation of the human body, the variation in line of sight between basestation and mobile mote, due entirely to the subject's mobility. The slow rate of variation is a distinct disadvantage because it results in predictable key generation since the inherent entropy is low. Additionally, from Fig.6(b), it is observed that Eve1 can loosely approximate the broader shape of the slow component of the basestation and mobile mote. This is due to its proximity to the basestation and because the effects of distance and orientation vary at a slow rate. Eve5 situated at a distance ($2 \sim 3$ m) has a completely different result.

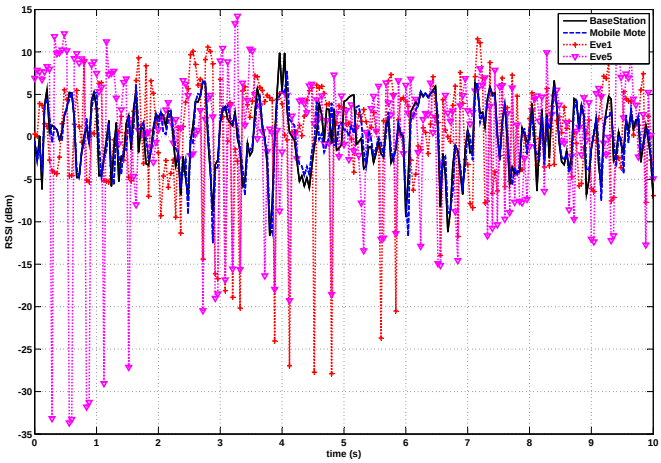
The fast component is due to the channel variations caused by the actual motion itself, the changing multipath properties. There is far more information in this channel profile, the rate of variation is much faster, and this has consequences for key generation in that there is a higher likelihood of generating mismatching bits. This component is also less prone to eavesdropping, as can be observed in Fig.6(c). Existing research in this domain, has primarily focussed on using this component, i.e. channel variation, for key generation purposes [3] [5]. The slow component has not been identified and studied as such because application scenarios in the literature have not focussed on distance variation and line of sight between communicating parties but specifically on motion itself. In the next section, we discuss how using these components individually as per application can lead to different advantages



(a) Baseline Distribution: Channel Variation



(b) Slow Component: Variation due to Mobility, Position and Orientation



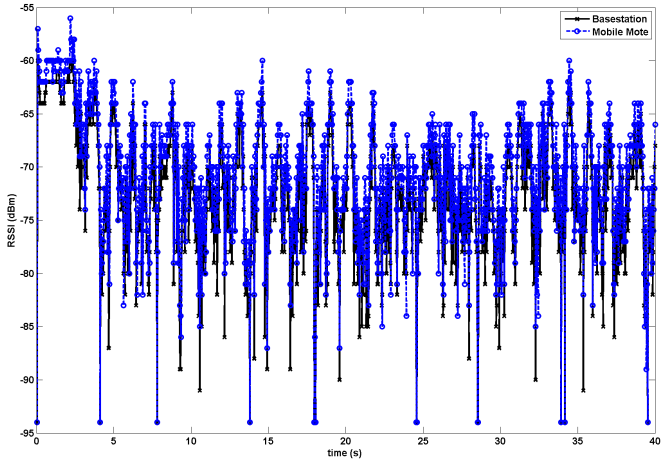
(c) Fast Component: Variation due to Motion

Fig. 6. Isolating Slow and Fast Components

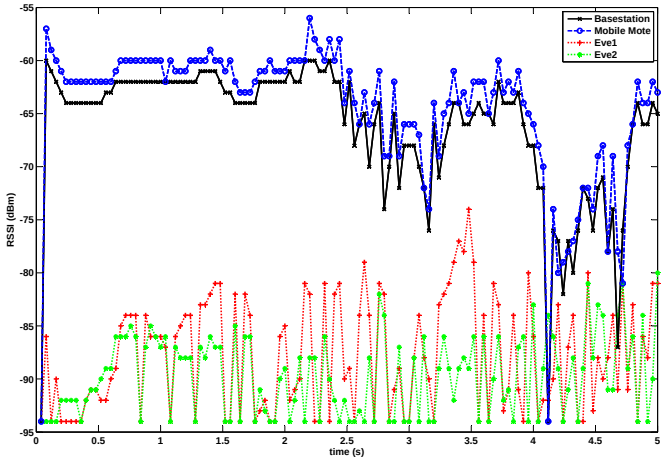
and improvements in performance.

In the final instance, **Walking with Body Worn Network**, both basestation and mobile mote are mounted on the human

subject to simulate a fully body-worn network. The basestation is tucked in the trouser pocket on the right hand side, the same side as the mobile device, which is still strapped to the right arm as earlier. Only two eavesdroppers are used in this scenario: Eve1 is also tucked into the subject's trouser pocket but on the left hand side. Eve2 is at the far end of the walk. Fig. 7(a) plots the variation in RSSI for basestation and mobile mote. Detailed results with eavesdroppers are presented in Fig. 7(b). The variation in range this time is much less because the basestation and mobile mote are in close proximity at all times. Packet loss is significantly reduced between the two parties. The results again show high correlation. Similarly, we note that the eavesdroppers have very poor success in replicating the results. Eve1 is also body-worn but encounters a fair amount of loss due to its position on the opposite side of the body from the mobile mote.



(a) Channel Variation for Basestation and Mobile Mote



(b) Channel Variation (detail) for Basestation, Mobile Mote and Eavesdroppers

Fig. 7. Variation in RSSI for Walking with Body Worn Network

IV. Key Generation Mechanism

In this section we outline operating assumptions and describe the mechanism to generate secret keys.

A. Operating Assumptions and Threat Model

We assume that secret-key generation is performed in a body area network in which one or both communicating devices may be body-worn and mobile. There may be one or more eavesdroppers in the environment which record communication between basestation and mobile mote. Eve can measure channel characteristics at the same time as the legitimate parties and knows the key extraction algorithm and parameters. Furthermore, we assume that Eve is separated from the basestation and mobile mote by at least a few multiples of the wavelength, and thereby restricted to measuring a different channel. In the case where the slow component is used to derive keys, this distance needs to be increased to at least 1m because the channel variation is far slower.

In this paper we do not address the issue of establishment of initial trust between basestation and mobile mote, nor consider active attacker who engage in jamming or packet injection. We leave these two concerns for future work.

B. Application Requirement

As noted earlier, each of the signal components have unique properties that we can tailor to suit certain applications. The fast component is more suited to high-rate key generation, more applicable to bootstrapping and key-renewal in dynamic ad-hoc scenarios such as athlete monitoring and disaster recovery where devices need to be unpacked and strapped on and be 'good to go'. The channel will need to be sampled intensively over a very short period of time. The key generation is liable to result in mismatching bits and an information reconciliation protocol is required to ensure both parties have the same bitstring. If the mismatch is sufficiently high, a further privacy amplification phase will be required to further secure the new key.

The slow component is fairly predictable and this drawback can be countered by sufficiently downsampling the signal, which in turn will result in a far slower key generation rate. This approach is suited to applications where there is far more flexibility in key generation such as day-to-day patient monitoring, monitoring the elderly, and general healthcare. Here a key need not be generated every few minutes or hours, but whenever is convenient and the process can be relegated to the background of normal network operations. There are distinct design advantages: the devices need not undertake specific channel sampling but could merely choose to sample the RSSI of the existing two-way traffic between them. Furthermore, as our results in the next section indicate, the key agreement using the slow component is so high that information reconciliation and privacy amplification need not be applied at all. The reconciliation mechanism typically requires a higher layer software implementation, it entails overhead in network traffic and adds to protocol complexity and extra dependencies. The tradeoff in this case is the filtering operation required to isolate the slow component. This filter consists of linear operations and can be easily implemented in ASIC.

C. Sampling

The mobile mote initiates the sampling process by transmitting packets with sequential counter values. The basestation records the RSSI value and responds to each with a packet of its own using the same counter value. In the case where the slow component is employed for key generation and the network traffic itself is being sampled, the response could consist of an ACK message. Paired transmissions must be spaced close together in time, in the order of $10 \sim 20$ milliseconds, in order to track channel variations in both directions simultaneously.

The mobile mote increments the counter value only when it receives a response from the basestation. The basestation can track which packets the basestation has received by checking if the counter value in the following packet has been incremented. This lets both parties keep a synchronized record of common probe packets that have been successful in both directions. The RSSI values of these are saved and indexed as per probe counter value. When enough values have been stored to generate a key, sampling is stopped.

D. Filtering and Quantization

We apply the Savitzky Golay filter to isolate the slow signal component. The filter takes two inputs, the polynomial order, *k*, and the frame size, *f*. The fast component is obtained by subtracting the slow component from the original distribution. Both signals are then quantized independently.

Several quantizers have been proposed in the literature. For simplicity, we use a basic mechanism described in [10] and modified in [3], in which essentially the basestation and the mobile device define an adaptive moving window of size *w*, within which they consider blocks of consecutive RSSI readings. For each block, two threshold values are calculated:

$$q+ = \mu + \alpha * \sigma \tag{1}$$

$$q- = \mu - \alpha * \sigma \tag{2}$$

where μ is the mean of the values, σ is the standard deviation and α is a configurable parameter such that $\alpha \geq 0$. If an RSSI reading within a window is greater than *q+*, it is taken to be a 1 and if it is less than *q-*, it is encoded as a 0. Values falling between the two thresholds are discarded.

A smaller value of α implies a higher bit extraction rate but leads to greater chances of bit mismatch between the two parties. A larger value of α will lead to greater agreement between the two devices at the cost of a lower bit generation rate.

E. Detecting Mismatching Bits

The basestation and mobile mote keep record of RSSI readings that successfully encode to a bit. Lists of these, indexed by counter value, are periodically exchanged during the key generation process to ensure that both parties derive their respective bitstrings from a common set of RSSI readings.

There will be some mismatch in Alice and Bob's bitstrings because the channel is not being sampled simultaneously at both ends but in very rapid succession. We propose a method to enable agreement at the byte-level: as soon as both parties generate a block of 9 bits, they compute and transmit the parity of the block. If the parity matches, the block can be used for key generation. To limit an eavesdroppers knowledge of the key, both parties discard the last bit of their respective blocks. However, if the parity does not match, they discard the block entirely. This method does not work for an even numbers of mismatching bits, but, as our experimental results indicate in the next section, this scheme can be configured to yield a bit agreement rate of over 95% and that minimizes the chances of there being more than one bit error per block. In the case of the slow component, the bit mismatch rate is sufficiently low to skip this reconciliation process altogether.

This process continues till the entire key has been assembled. To verify that both parties derived the same key, the basestation transmits a hash of its key with which the mobile mote verifies its own. If the key matches, the protocol has been successful. If the keys do not match, the entire key generation process is repeated.

V. Results

We apply our key generation mechanism on our experimental results and use the following metrics to quantify performance:

1) **Bit Mismatch**: the ratio of the number of mismatching bits between two devices to the total number of extracted bits. The objective is to minimize the mismatch between the mobile mote and the basestation to close to 0 and to raise it to a satisfactory high threshold (0.5) in the case of the eavesdroppers. For basestation and mobile mote, a bit mismatch close to 0 indicates very good key agreement between the two parties. For larger values, information reconciliation is required to identify and correct bit errors. For mobile mote and eavesdroppers, a mismatch close to 0.5 is ideal, indicating that, from the eavesdropper's point of view, there is an equal probability of a bit in the key being a 0 or a 1. The eavesdropper in this case has no advantage and the scenario would be equivalent to him having to toss a fair coin to guess the individual bits.
2) **Secret Bit Rate**: the average number of secret key bits extracted from the channel per unit time. A key rate of 9 bits/s means it would take approximately 8s to generate a 64 bit key. A rate of 1 bit/s would take approximately a minute.

In Table.I we presents the mobile mote's results of key generation performed using the original channel characteristics without isolating any of the components for the three different experimental modes. The figures confirm our earlier analysis that Resting is not conducive to key generation: the channel variation is not highly correlated for basestation and mobile mote, as evidenced by the bit mismatch, and the channel variation is small, leading to a very low secret bit rate.

Table.II shows results when key generation is performed on the fast component. Resting shows a dramatic increase in key

TABLE I
EXPERIMENTAL RESULTS: KEY GENERATION USING UNFILTERED RSSI CHANNEL PROFILE (W=3, α=0.75)

Mode	Mismatch: Basestation	Mismatch: Eve1	Mismatch: Eve5	Secret Bit Rate (bits/s)
Resting	0.36	0.46	0.45	0.64
Walking	0.03	0.49	0.48	8.87
Body Worn	0.03	0.49	0.48	9.58

TABLE II
EXPERIMENTAL RESULTS: KEY GENERATION USING FAST COMPONENT (W=3, α=0.75)

Mode	Mismatch: Basestation	Mismatch: Eve1	Mismatch: Eve5	Secret Bit Rate (bits/s)
Resting	0.38	0.53	0.51	8.01
Walking	0.05	0.46	0.48	9.50
Body Worn	0.04	0.48	0.47	10.18

generation rate but the bit mismatch with the basestation is still significant. The fast component yields a slightly higher secret bit rate than the original unfiltered RSSI profile for the Walking and Body Worn scenarios.

Table.III presents results for the downsampled slow component. The secret bit rates are obviously much lower than the other cases due to the downsampling, and, for the walking scenario, Eve1 has an advantage because of its close proximity to the basestation (15cm). However, the bit mismatch between the basestation and the mobile mote in this case is negligible. This mode can be seen to be very suited to scenarios where key generation requirements are not very stringent, and the key can slowly be amassed over time in the background to normal network operations. The information reconciliation stage can be dispensed with completely.

We believe our experimental results validate our earlier findings: to summarize, the fast component can speed up key generation rate (greatly for more stationary scenarios) but requires a dedicated sampling and information reconciliation phase, making it suitable for dynamic scenarios, such as bootstrapping systems, highly dynamic scenarios where an approach similar to the plug-and-play philosophy is required. In other less restricted cases, a low bit rate is perfectly adequate, leading to reduced overheads and dramatically less complexity in protocol and implementation.

VI. CONCLUSION

In this paper we have demonstrated the feasibility of using radio channel characteristics to derive secret keys in body area networks. Our experimental results confirm that the radio link is highly symmetric in both directions and that mobility causes sufficient channel fluctuation to generate keys at a fast rate. Eavesdroppers are unable to replicate the distribution with high accuracy even if they are moderately close to the communicating parties.

Furthermore, we have shown that the RSSI profile can be deconstructed to yield a slow and a fast component, each of which result in different advantages. We elaborate a protocol which builds on these and use experimental results to highlight the tradeoff.

TABLE III
EXPERIMENTAL RESULTS: KEY GENERATION USING SLOW COMPONENT (W=3, α=0.75, SAMPLING RATE = 1/S)

Mode	Mismatch: Basestation	Mismatch: Eve1	Mismatch: Eve5	Secret Bit Rate (bits/s)
Resting	0.21	0.47	0.53	1.17
Walking	0	0.30	0.53	1.27
Body Worn	0	0.48	0.58	1.21

For future work, we intend to fine-tune quantizer design and address the issue of establishing initial trust between the mobile device and basestation as a prelude to key generation.

REFERENCES

[1] A. R. Service, "Market for Wearable Wireless Sensors to Grow to More than 400 Million Devices by 2014," online, 2009.

[2] E.-O. Bla and M. Zitterbart, "Efficient Implementation of Elliptic Curve Cryptography for Wireless Sensor Networks," Universit at Karlsruhe, Tech. Rep., 2005.

[3] S. Jana, S. N. Premnath, M. Clark, S. Kasera, N. Patwari, and S. Krishnamurthy, "On the Effectiveness of Secret Key Extraction Using Wireless Signal Strength in Real Environments," in *International Conference on Mobile Computing and Networking (Mobicom'09)*. Beijing, China: ACM.

[4] M. Wilhelm, I. Martinovic, and J. B. Schmitt, "Secret Keys from Entangled Sensor Motes: Implementation and Analysis," in *WiSec'10*. Hoboken, New Jersey USA: ACM.

[5] B. Azimi-Sadjadi, A. Kiayias, A. Mercado, and B. Yener, "Robust Key Generation from Signal Envelopes in Wireless Networks," in *Conference on Computer and Communications Security (CCS'07)*. Alexandria, Virginia USA: ACM.

[6] J. E. Hershey, A. A. Hassan, and R. Yarlagadda, "Unconventional Cryptographic Keying Variable Management," *IEEE Transactions on Communications*, vol. 43, no. 1, 1995.

[7] U. M. Maurer, "Secret Key Agreement by Public Discussion from Common Information," in *IEEE Transactions on Information Theory*, vol. 39, 1993, pp. 733–742.

[8] U. M. Maurer and S. Wolf, "Secret Key Agreement Over a Non-authenticated Channel," in *IEEE Transactions on Information Theory*, vol. 49, 2003, pp. 832–851.

[9] G. Brassard and L. Salvail, "Secret-Key Reconciliation by Public Discussion," in *Workshop on the Theory and Application of Cryptographic Techniques on Advances in Cryptology*, 1994.

[10] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-telepathy: Extracting a Secret Keyfrom an Unauthenticated Wireless Channel," in *International Conference on Mobile Computing and Networking (Mobicom'08)*. San Francisco, California USA: ACM.

[11] J. Croft, N. Patwari, and S. Kasera, "Robust Uncorrelated Bit Extraction Methodologies for Wireless Sensors," in *International Conference on Information Processing in Sensor Networks (IPSN'10)*. Stockholm, Sweden: ACM/IEEE.

[12] L. W. Hanlen, D. Smith, J. A. Zhang, and D. Lewis, "Key-sharing via Channel Randomness in Narrowband Body Area Networks: Is Everyday Movement Sufficient?" in *Bodynets'09*, Los Angeles, California USA.

[13] A. Savitzky and M. J. E. Golay, "Smoothing and Differentiation of Data by Simplified Least Squares Procedures," in *Analytical Chemistry*, vol. 36:8, 1964, p. 16271639.