Key-sharing via channel randomness in narrowband body area networks: Is everyday movement sufficient?

Leif W. Hanlen, David Smith, Jian (Andrew) Zhang, Daniel Lewis*
NICTA
Canberra, Australia
leif.hanlen@nicta.com.au

ABSTRACT

We consider secure communication for Body-Area-Networks (BAN's). We examine the near-body radio channel of BAN's as a source of common randomness between two sensors. The movement of the subject and associated fading is used to hide a secure key from Eve. We examine recently approved radio channel models of the IEEE 802.15.6 Task Group, and show that the common randomness is too low rate for unconditional encoding. We find a key-generation rate around 2bits/second. We suggest the channel randomness may be better used in generating perpetually new keys for an AES-style encryption – eg, a 128bits key every minute – via a randomness scavenging procedure.

1. INTRODUCTION

A significant problem for Body-Area-Networks (BANs) is the possibility of network intruders. Several research groups have applied more- or less- sophisticated technologies to intercept (detect), spoof, and potentially attack Bluetooth and Radio Frequency Identification (RFID) based networks. Bluetooth class 2 (range 10m) devices have been intercepted at a range of 1.78km [1]: the 3 meter transmit range of BANs is not a major hurdle for a well-resourced intruder.

The limited power and resources of BAN nodes, the potential value of the data transported on a BAN and the substantial impact for damage caused by unauthorised access[1] all motivate a security scheme which can be defended against a worst-case attacker. It is sensible to assume an attacker will have *unlimited* resources and that an attacker may be located within the normal BAN.

Our reasoning behind such generous allowances for the attacker are that if we wish to perform extreme security for the BAN (beyond AES) then we ought to ensure any algorithm is robust against extreme attacks. A number of possible applications requiring high security, while allowing reasonable movement include [3]; assessing emergency service personnel and performance; social networking (privacy/authenticity) and wireless medical implants. *What secret sharing rate does the random nature of a BAN-link offer, using simple system-on-chip transceivers?*

We are not interested in developing an algorithm to show *how* the key could be generated — such an algorithm is quite laborious: see *e.g.* [4] or [5, Def.4] — rather we wish to know *is a key-generating algorithm feasible?*

1.1 Problem set up

Two (trusted) sensors — which we shall call Alice and Bob — wish to communicate securely in the presence of another (untrusted) device, Eve. Eve has unlimited computing and transmit power, she can intercept all transmissions between Alice and Bob, and she can spoof the radio channel. We would like Alice and Bob to have unconditionally secure communications in this case — which requires a source of joint randomness. Cases such as random identifiers [6] do not succeed here, since Eve may "pretend" to be an identified network participant.

The remainder of this paper is arranged as follows: In 1.2 we discuss mobility in the BAN channel, and in particular consider channel variation for on-body to on-body transmissions. In 1.3 we investigate recent work on body-area-networking security and consider the need for sources of joint randomness. Section 2 investigates the limits of using a BAN-radio as a source of randomness for key generation. We offer simulation results based on a published BAN channel simulator in Section 3 and draw conclusions in Section 4.

1.2 BAN channel model and dynamics

Channel modelling and characterisation for BANs at various frequencies under both wireless and body-coupled scenarios has been carried out. The channel model document for IEEE-802.15.6 (BAN) task group [7] provides a large number of physical measurement results, while a (large) number of authors have outlined measurement campaigns such as [8, 9, 10].

For a subject performing normal activity — office movement and running on a treadmill — we have previously found the average fade rate was 2.69Hz [11] from the mean, when

*L. Hanlen, D. Smith, J. Zhang also hold adjunct appointments with the Research School of Information Sciences and Engineering, Australian National University. NICTA is funded through the Australian Government's *Backing Australia's Ability initiative*, in part through the Australian Research Council. This work supported under the NICTA *Human Performance Improvement* project

[1]In the literature review of [2] an RFID-deep brain stimulator had caused a "severe rebound tremor" in a patient due to (accidental) reprogramming via interference from coexisting RFID's.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.
Bodynets '09 Los Angeles, California USA
Copyright 2009 ICST 978-963-9799-41-7 ...$5.00.

Digital Object Identifier: 10.4108/ICST.BODYNETS2009.5941
http://dx.doi.org/10.4108/ICST.BODYNETS2009.5941

Figure 1: Treadmill running experiment; hip to chest measurement; subject running shown (left) with wearable 2400MHz antenna (right). Wireless transmissions in office at -10dBm. Experiments with male and female subjects, with speeds of 2.5km/h to 12km/h.

using a -10dBm transmit power. We have found that the channel is stable (static) for 10-25ms [12]. These results have been used to develop a channel simulator for BAN [13], which we use here to investigate the entropy rate of the channel. Figure 1 describes the physical setup of the test equipment.

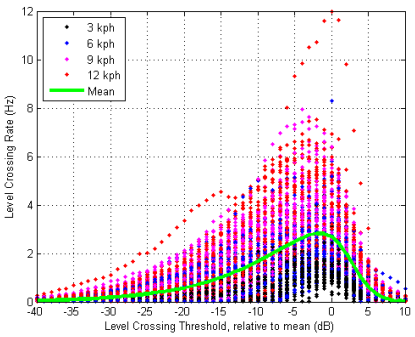
Figure 2 characterizes the random BAN link. Level crossing rates for walking and running are shown, as well as a typical signal for a walking subject. Figure 3 shows the outage probably for a collection of test subjects and activity levels. A brief consideration of the implicit randomness of a BAN link shows that the channel is variable for different people and different activity levels, and also for different measurement positions on the body. The channel variation is low, (long stability time), and the channel is a single-tap (flat) fading link. This variability *may* be a reasonable source for key generation, which we consider below.

1.3 Security requirements

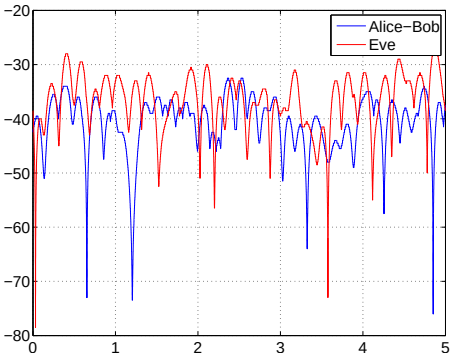
BAN security requirements must satisfy some simple tests – implement-able with a minimum hardware- software- overhead, *reasonably* strong and should not require substantial user input. We quote from the IEEE 802.15.6 Technical Requirements Document [14] *[The] mechanism should be energy efficient and lightweight. When supported, the highest level of security shall be equal to or stronger than that provided by AES (Advanced Encryption Standard) 128 bits (FIPS-197) [15].... Consideration should be given to secure device pairing (or association). [Pairing] consists of device authentication and key exchange.*

Computationally secure systems (*e.g.* public-key) require a computationally expensive operation to be performed for a successful brute-force attack – *e.g.* factoring large integers. They rely on the principle that the computational cost of obtaining the cipher-data is substantially more than the value of the data. Information-theoretic systems are secure as there is no method of obtaining the cipher other than pure guessing. For this reason information-theoretic ciphers are also called *unconditionally secure.*

The review [2] outlines a wide variety of security algorithms, and requirements for wireless sensor networks in medical environments. Recent work by Leon-Salas et al. [16] proposed a PN (pseudo-noise) sequence both for multiple-access and encryption via DSSS (Direct Sequence Spread Spectrum). The PN sequence is changed for each data-bit to mimic the one-time pad of Shannon [17] *i.e.* to achieve



(a) Level crossing rate



(b) RSSI estimate

Figure 2: Level crossing rates vs receive sensitivity (mean is set to 0dB) from physical experiments, and typical receive signal for Alice, Bob and Eve.

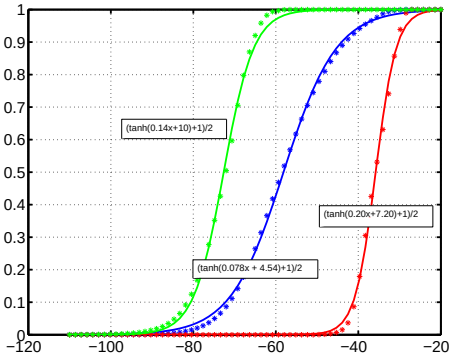


Figure 3: CDF of receive signal power, over all measurements and all subjects. Curves show minimum (green), mean (blue) and maximum (red) outage probability respectively, with corresponding $\frac{1}{2}(\tanh(\alpha x+\beta)+1)$ curve-fit in solid lines

Digital Object Identifier: 10.4108/ICST.BODYNETS2009.5941
http://dx.doi.org/10.4108/ICST.BODYNETS2009.5941

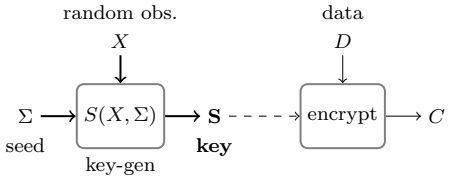


Figure 4: Key-generation from seed Σ and random process X. The key S is used to encrypt data D (for authenticity or secrecy) to produce cipher C. The key-gen function may be arbitrarily complex, but is deterministic.

perfect secrecy. The changing PN sequence may be viewed as a long key S where each N bits correspond to 1 message bit. To generate S, a deterministic key-generator is used.

For perfect secrecy, the entropy of the key S must be *at least* as large as the entropy of the message M [17]. Another way of writing this is the key is as long (or longer) than the message *i.e.* $|S| \geq |M|$. In [16] $|S| \approx N \times |M|$, however the entropy of the key is only equal to the entropy of the seed Σ — since S is a deterministic function of Σ [18] hence

$$H(S) \leq H(\Sigma) \leq H(M) \tag{1}$$

since it would seem unreasonable to have a fixed seed Σ of sufficient entropy that the message (all messages for all time) has lower entropy than the key — eventually, the message will be longer than the seed. Contrast (1) with the requirements of [17]

$$H(M) \leq H(S) \tag{2}$$

If $|\Sigma|$ is small, then the only way to generate a large S from Σ is to use a source of randomness.

Figure 4 outlines the (prior to output to a wireless channel) process of encrypting data with a secret key S. The key is generated from a combination of a seed Σ and random observations X. In [16] X is not used, and the key-gen process is self contained.

We consider cryptographic schemes which use a controlled form of randomness to perpetually generate new keys. In particular, randomness which arises from the physical channel between the wireless sensors. A need for such schemes has been observed for medical wireless sensor networks [19]. Online key-generation from the channel has been proposed for narrowband-fading in [4], however the authors there operated under fast mobile fades, and hence assumed a reasonably fast key generation. Channel-keys have been considered for UWB in [20], due to available multipath. From [5] it has been shown that a channel which does not use joint randomness must rely on computational (vs information theoretic) secrecy.

Figure 5 shows how Alice and Bob may agree on a shared secret key S, over a public channel in the presence of an eavesdropper Eve, using the work of [5]. Alice and Bob wished to agree on a secret key over a non-secure network. This is achieved by Alice observing X, Bob observing Y and Eve observing Z where X, Y, Z had a joint probability P_{XYZ}. Alice and Bob may generate local, secret keys which are provably secure from Eve. The details of the key-generation may be taken *e.g.* from [4].

Our notation is as follows: Alice wishes to send information securely to Bob, with an eavesdropper Eve. S denotes

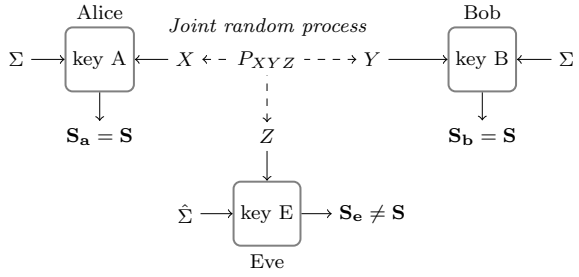


Figure 5: Full key-generation process. Alice, Bob and Eve all make observations of a random process with joint probability P_{XYZ}. The output S is the key in Figure 4.

the shared, secret key between Alice and Bob. D is the (clear) data from which C is the cipher data. Σ denotes some side information – such as a seed or prior key. Subscripts *e.g.* D_i denote particular bits.

2. BAN CHANNEL KEYS

We would like to generate S such that (2) holds. Since BAN data rates will be between 10kbps to 10Mbps [14] – hence we would like to have keys generated at a rate of *at least* kilobits per second. If the channel is not sufficiently random, we may reconcile ourselves to generating a stream of Σ values for a seed-intialized scheme such as [16], or a new private key for an AES-style system [15]. We will shortly see that the weak BAN sensor is a serious limitation on strong physical keys – we will consider real transceivers, which have characteristics likely to be seen in a future BAN.

As the secret key S is manufactured from joint randomness in the public channel, the rate of the key[2] is limited by conditioning of Eve's observations. The key rate can be bounded[3] from [5, Thm.1]:

$$H(S) \leq I(X; Y \downarrow Z) + I(S; ZC) \tag{3}$$

and $I(X; Y \downarrow Z)$ is defined [5]

$$I(X; Y \downarrow Z) \triangleq \inf \left\{ I(X; Y|\hat{Z}) : P_{XY\hat{Z}} = \sum_{z \in \mathcal{Z}} P_{XYZ} P_{\hat{Z}|Z} \right\} \tag{4}$$

and the infimum over all possible choices of $P_{\hat{Z}|Z}$. A looser (more tractable) bound for (3) is given by [21, eqn.4]:

$$H(S) \leq \min \{ I(X; Y), I(X; Y|Z) \} \tag{5}$$

which arises from denying Eve write-access to the channel.

2.1 Achievable rate for RSSI-based key

Most transceiver systems allow RSSI (Receive Signal Strength Indication) measurements as part of their Carrier-Sense circuitry. As such, we consider RSSI measurements from the channel as a relatively non-invasive key source – *i.e.* we do not require specialised key-generation measurements.

Part of the achievable rate for a channel-based key is the entropy rate of the channel – the rate at which Alice and Bob

[2]The rate at which new bits can be added to a secret key *e.g.* how many seconds before a 128bit key may be formed?
[3]Assuming the desired probability of failure is very small

Digital Object Identifier: 10.4108/ICST.BODYNETS2009.5941
http://dx.doi.org/10.4108/ICST.BODYNETS2009.5941

and glean new information from observing their respective channel gains. A significant reduction of this rate occurs when the practical implementation is considered. We outline the major limitations for key-generation:

1. movement (dominant random source) provides limited channel entropy;
2. the channel that Eve observes is correlated with the channel between Alice and Bob — reducing the effective channel entropy, and
3. the BAN sensors that Alice and Bob use are not high resolution – introducing quantisation limits.

2.1.1 Channel entropy (realistic sampling rate)

The channel for a walking subject (1.5 km/h) has a time-stability of 15ms and a variation in fade magnitude between +10dB to -70dB from the mean. We can assume that measurements are iid (under the condition that the sample rate is below 60Hz) and taken from a Weibull distribution, which gives every sample an entropy of

$$\gamma \cdot \left(1 - \frac{1}{\alpha}\right) + \log\left(\frac{\beta}{\alpha}\right) + 1 \text{ nat/s} \quad (6)$$

Where (6) is taken from [22]; γ is the Euler-Mascheroni constant $\gamma \approx 0.57721$, α and β are (respectively) the shape and scale parameters of the Weibull distribution. We have found that $\alpha = 0.98$ and $\beta = 0.99$, which gives an entropy of 1.44 bits-per-sample. One sample every 15ms gives 96.0bps.

Numerical analysis indicates that the entropy of this channel is approx. 21.5bps — the discrepancy is due to the (optimistic) assumption that we obtain independent Weibull distributed random variables every 15ms, in reality we are observing a correlated samples (with correlation coefficient less than 0.9), but not independent samples.

The maximum rate for generating new key bits from a walking subject, using observed channel power is below 100bps. *This rate cannot be increased by* e.g. *adding noise at Alice or Bob, and is likely to be substantially lower when Eve is considered.*

From (2) it is easy to see that such a low bit rate will not support unconditional security for any reasonable data rate (*i.e.* $H(M) > 100$bps). Further, this rate is the best we can hope for with perfect sensing and independent channels — we now observe the damage caused by real sensing and placing Eve in reasonable proximity to Alice and Bob.

2.1.2 Independence from Eve (realistic joint entropy)

Eve will be capable of measuring the channel: we consider two simple cases. We assume Eve measures an offset channel – same distribution, independently faded. In this case the conditional entropy is reduced to approximately 0.054bits per sample – numerically we find the entropy rate of the 60Hz, conditioned channel is 3.24bps. We have separately found that the key generation rate for the simpler case (Eve measures a noisy version of Alice-Bob channel, even for a reduced noise) is similar.

2.1.3 Bits per sample (realistic resolution)

The low-power CC2500 transceiver from Texas Instruments allows 8bit or 0.5dB resolution — the lesser of the two — for RSSI measurements at 1kHz sampling. The bit rate may be doubled by inclusion of secondary factors such as Link Quality – with the caveat that since the fading of the channel is largely flat the Link Quality samples will be highly correlated with the RSSI samples *i.e.* we cannot expect 16 independent bits per sample.

The effect of the RSSI sampling implies we can have *at most* 8kbps data, however the channel entropy is the limiting factor. For the same samples as subsection 2.1.1, quantization reduces the entropy from 4.26 to 1.68 bit per sample.

Combining all effects, we envisage a key-bit generation rate from RSSI measurements of 4bps.

2.2 Protocol

Each time Alice wakes to transmit (noting that the BAN sensors are likely to have low duty cycling) she must perform carrier sense – to avoid collisions – as part of this process, RSSI values are found. The algorithm is outlined below

```
Tx-cycle for Alice
 1  Assuming key-sharing (pairing) has been achieved already.
 2  If not, data is held at step 12 until pairing achieved.
 3  Wake for Tx, k ← k + 2
 4  repeat  measure RSSI (carrier sense)
 5          Y_i ← RSSI
 6          i ← i + 1
 7     until RSSI < threshold-Tx
 8  send C_k = f(Y_0 ... Y_i)
 9  store K bits for NewKey
10  if K > KeyLength
11     then Key ← NewKey
12   Transmit encrypted packet using Key
13  Sleep
```

The Tx-cycle for Bob is equivalent. The index k is not a global variable – nor is it transmitted – it is simply a bookkeeping exercise to align the C_k transmissions in the text.

The RSSI values measured by Alice do not need to match with Bob's channel measurements[4]. however, since both $X = \{X_0, \ldots X_i, \ldots\}$ and $Y = \{Y_0 \ldots\}$ are generated from the same fading process *and they include the common channel* between Bob and Alice, $I(X;Y) > 0$.

The results below have been simulated under the assumption of continuous transmission. For duty-cycled transmission the keys are generated slower (due to less frequent channel sampling), however the use of the keys is also reduced: so the overall system security remains essentially the same.

3. SIMULATIONS

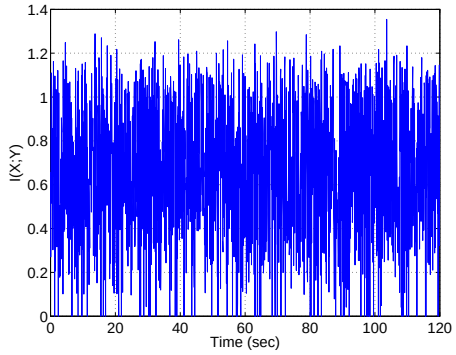
To calculate (5) we used Matlab^{TM} code from [23]. We outline the code in section A We consider a particular scenario of a subject moving at 1.5km/hr (a moderate walking pace) with a hip-to-chest link. Such a case might arise for ECG data being (securely) sent to a body-worn processor. We have previously argued that the channel is reasonably static for 15ms under these conditions.

We used results from our BAN simulator [13]. We generated a sequence of RSSI values $s = \{s_0, \ldots\}$ from the channel, sampled at 10kHz and quantised to 0.5dB. We then took 15ms observation periods (150 samples) to form the

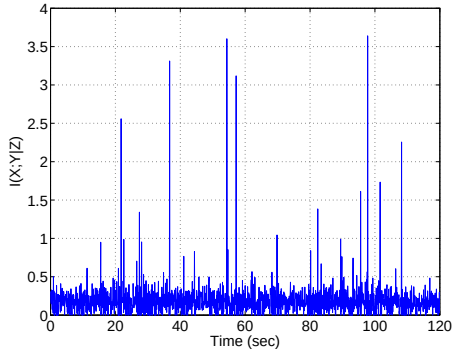
[4]We only require that there is a non-zero mutual information between them. This is a very loose constraint, only forcing Alice and Bob to have random sources which are not identically independent over all time.

Digital Object Identifier: 10.4108/ICST.BODYNETS2009.5941
http://dx.doi.org/10.4108/ICST.BODYNETS2009.5941

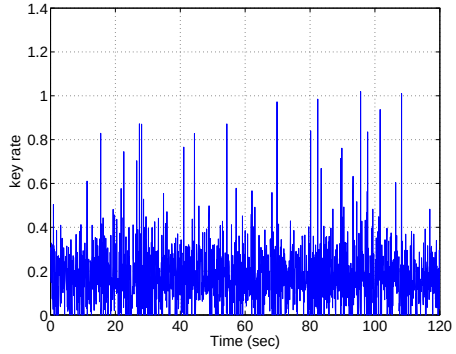
measurements of Alice $x = \{s_m, \ldots, s_{m+149}\}$ and Bob y respectively. A similar process was used for Eve z. We modeled the busy channel by considering a time-offset between Alice's and Bob's RSSI measurements.



(a) Channel estimate Alice-Bob



(b) Channel estimate by Eve



(c) Key rate between Alice-Bob with Eve

Figure 6: Mutual information between Alic-Bob and Alice-Bob with Eve. The key generation rate Fig 6(c) is the minimum value from Fig 6(a) and Fig 6(b), as given by (5)

Figure 6 shows the key rate for the conditions outlined above. We have used the key-rate to generate new 32bit keys in Figure 7 — the length of the key is irrelevant, it is simply to give a scale to the time taken to generate a new key. As can be seen from the plot, new keys can be created at approximately 2bits per second.

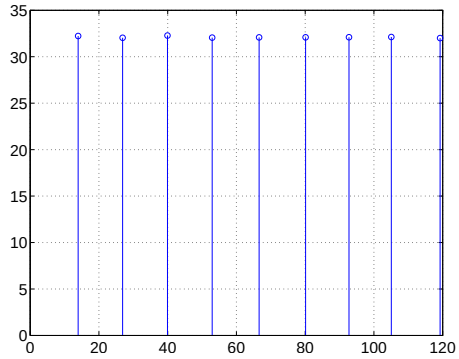


Figure 7: Key generation at 32-bits per new key. New keys are generated at rate of 2bits per second

Finally, we consider the case where Eve can observe the channel between Alice and Bob, at a higher fidelity than Alice and Bob — such as the case in the Blue-snarfing example [1]. The SNR for Eve is 1000× the SNR for Alice-Bob. We used direct measurements via National Instruments shown in Fig 1. The channel measurements and resultant key-rate are shown Fig 8, with comparison to the key-rate given by 7. Note (due to new arrangement) the new key-rate is smaller, but still non-neglible.

4. CONCLUSIONS

We have shown through theoretical bounds that the key-sharing rate for a BAN based on channel RSSI measurements is likely to be quite low — on the order of 4bit/sec. Simulations have shown the rate may be closer to 2 bits per second. While this does show that key-sharing is possible, it suggests that unconditional security is unlikely for any practical communication rates.

We suggest the random channel measurements may be used to generate the seed for AES-style systems. Thus a new 128bit AES key could be created every minute. This would not meet the Shannon one-time-pad level of security, but would be substantially improved over a one-off AES key.

APPENDIX

A. ENTROPY & MUTUAL INFORMATION

The empirical entropy $H(x)$ of the sequence

$$\{x\}_0^n = \{x_0, \ldots, x_n\}$$

is given by calculating the histogram $\{h\}_0^K$ of $\{x\}_0^n$, and then summing the $\log_2$ of the k histogram bins.

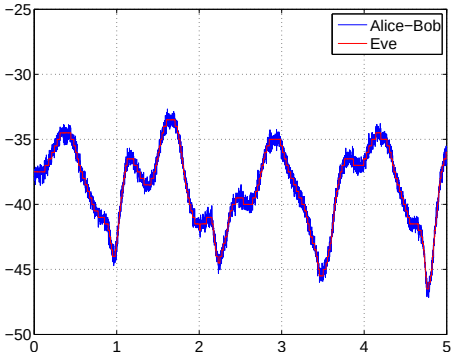
$$H(x) \approx -\sum_{k=0}^{K} h_k \log_2(h_k)$$

This gives the overall sequence entropy, to find the entropy in bits/second, we multiply by the sequence length.

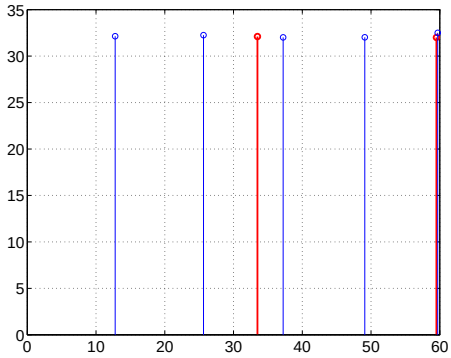
Mutual information is found via [18]

$$\begin{aligned} I(x;y) &= H(x) + H(y) - H(x,y) \\ I(x;y|z) &= H(x|z) - H(x|y,z) \\ &= H(x,z) + H(y,z) - H(x,y,z) - H(z) \end{aligned}$$

Digital Object Identifier: 10.4108/ICST.BODYNETS2009.5941
http://dx.doi.org/10.4108/ICST.BODYNETS2009.5941



(a) Channel



(b) Time taken to generate 32bit keys. Red lines denote Eve with supergain receiver, blue lines correspond to previous simulation

Figure 8: Key generation rate estimation using empirical measurements.

B. REFERENCES

[1] Long distance snarf. `http://trifinite.org/trifinite_stuff_lds.html`.

[2] Ellen Stuart, Melody Moh, and Teng-Sheng Moh. Privacy and security in biomedical applications of wireless sensor networks. In *Intl. Symp. App. Sci. Bio-Med. Comm. Tech.*, Aalborg, Denmark, October 25 2008.

[3] Daniel Lewis. 802.15.6 call for applications - response summary, July 2008.

[4] Michael A. Tope and John C. McEachen. Unconditionally secure communications over fading channels. In *MILCOM*, pages 54–58, 2001.

[5] Ueli M. Maurer and Stefan Wolf. Secret-key agreement over unauthenticated public channels – Part I: Definitions and a completeness result. *IEEE Trans. Inform. Theory*, 49(4):822–831, April 2003.

[6] Joshua R. Smith. Distributing identity. *IEEE J. Robot. Automat.*, 6(1):49–56, March 1999.

[7] Kamya Yekeh Yazdandoost and Kamran Sayrafian-Pour. Channel model for body area network (BAN) IEEE P802.15-08-0780-02-006. https://mentor.ieee.org/802.15, November 2008.

[8] Adam T. Barth, Mark A. Hanson, Harry C. Powell, Dincer Unluer, Stephen G. Wilson, and John Lach. Body-coupled communication for body sensor networks. In *Bodynets*, 2008.

[9] Shuo Xiao, Vijay Sivaraman, and Alison Burdett. Adapting radio transmit power in wireless body area sensor networks. In *Bodynets*, pages 52–59, 2008.

[10] William G. Scanlon and Simon L. Cotton. Understand on-body fading channel at 2.45 GHz using measurements based on user state and environment. In *Loughborough Antennas and Propagation Conference*, pages 10–13, Loughborough, UK, March 2008.

[11] Dino Miniutti, Leif W. Hanlen, David B. Smith, Jian (Andrew) Zhang, Daniel Lewis, David Rodda, and Ben Gilbert. Narrowband channel characterization for body area networks [IEEE-802.15.08.0421.00.0006]. Technical report, IEEE802.15.6, June 2008.

[12] Jian (Andrew) Zhang, David B. Smith, Leif W. Hanlen, Dino Miniutti, David Rodda, and Ben Gilbert. Stability of narrowband dynamic body area channel. *IEEE Antennas Wireless Propagat. Lett.*, page to appear, 2009.

[13] David B. Smith, Dino Miniutti, Jian (Andrew) Zhang, and Leif W. Hanlen. Matlab code for generating BAN fading profile [IEEE P802.15-08-0850-00-0006]. https://mentor.ieee.org/802.15, November 2008.

[14] Bin Zhen, Maulin Patel, SungHyup Lee, EunTae Won, and Arthur Astrin. TG6 technical requirements document (TRD) IEEE P802.15-08-0644-09-0006. https://mentor.ieee.org/802.15, September 2008.

[15] Advanced encryption standard (AES): Fips-197. `http://www.governmentsecurity.org/articles/articles2/fips-197.pdf_fl/`, November 26 2001.

[16] Walter D. Leon-Salas, Yugyung Lee, and Deep Medhi. Joint encryption/multiple access for body area sensor networks. In *Bodynets*, 2008.

[17] Claude E. Shannon. Communication theory of secrecy systems. *The Bell System Technical Journal*, 28(4):656–715, May 1949.

[18] Thomas M. Cover and Joy A. Thomas. *Elements of Information Theory, Second Edition*. Wiley-Interscience, 2006.

[19] Thomas Falck, Heribert Baldus, Javier Espina, and Karin Klabunde. Plug 'n play simplicity for wireless medical body sensors. In *Pervasive Health Conference and Workshops*, pages 1–5, November 2006.

[20] Robert Wilson, David N. C. Tse, and Robert A. Scholtz. Channel identification: Secret sharing using reciprocity in ultrawideband channels. *IEEE Trans. Infor. Forens. Sec.*, 2(3):364–375, September 2007.

[21] Ueli M. Maurer and Stefan Wolf. Unconditionally secure key agreement and the intrinsic conditional information. *IEEE Trans. Inform. Theory*, 45(2):499–514, March 1999.

[22] Weibull distribution. `http://en.wikipedia.org/wiki/Weibull_distribution`, December 2008.

[23] Rudy Moddemeijer. Matlab library of Rudy Moddemeijer. `http://www.cs.rug.nl/~rudy/matlab/`, February 2001.

Digital Object Identifier: 10.4108/ICST.BODYNETS2009.5941
http://dx.doi.org/10.4108/ICST.BODYNETS2009.5941