Key Generation Based on Fast Reciprocal Channel Estimation for Body-Worn Sensor Nodes

Patrick Van Torre[1], Quinten Van den Brande[2], Jo Verhaevert[3], Jan Vanfleteren[4], Hendrik Rogier[5]
[1,2,3,5]Department of Information Technology, Ghent University/iMinds
[4]Department of Electronics and Information Systems, Ghent University/CMST,
Technologiepark-Zwijnaarde 15, 9052 Gent, Belgium,
Patrick.VanTorre@UGent.be

***Abstract*—With the advent of the Internet of Things, body-worn sensor nodes are continuously becoming more important. In case of bio-medical, rescue-worker or military applications sensitive data are often transmitted, requiring the need for encryption. The distribution of symmetric encryption keys is often an issue leading to security risks. Body-worn sensor nodes are generally employed in quickly varying channel conditions due to body movement. The radio-communication channel between such nodes is however reciprocal, allowing the extraction of an array of similar channel measurements at both ends of the link. These data can be used to build equal encryption keys at both link ends without the need for actual over-the-air key distribution. This paper studies the practical performance of an enhanced channel-based key generation system with a very short round-trip delay, allowing reciprocal channel assessment with increased accuracy. Measurements were performed using the new system and the results of the enhanced key generation are evaluated. Although the performance is slightly increased thanks to the shorter round-trip delay, the accuracy of the signal level detector still imposes limits.**

***Index Terms*—sensor nodes, key generation, encryption, antenna, propagation, measurement.**

I. Introduction

Body-worn sensor nodes are important for many modern-day applications, including health care, biomedical, military and rescue-worker systems. With the upcoming Internet of Things (IoT), wireless sensor nodes, including wearable nodes, will become more ubiquitous. A need for encryption exists because of the sensitivity of the data which are often transmitted. A set of algorithms is available for larger platforms to distribute symmetrical keys, but they are often prone to attacks and are also computationally demanding for wireless sensor nodes, employing low-profile low-power processors.

In the link between body-worn wireless sensor nodes, the radio-communication channel varies rapidly due to a number of physical causes. First of all, fading and shadowing is caused by the continuous movement of the nodes. Employing, e.g., the popular 2.45 GHz band as a working frequency, the wavelength is only 12 cm leading to quickly occurring maxima and minima, caused by alternating constructive and destructive interference of signals reflected in the environment. Such channel variations can lead to signal variation up to 35 dB. Additional shadowing occurs due to objects in the environment, as well as by the human body itself. Reorientation and changes of posture also result in a redirection of the antenna patterns, resulting in even more signal variation.

The radio channel employed by both users is reciprocal and hence also the channel variations. In case channel variation by the natural body movements is not fast enough, faster key generation can be obtained by means of reconfigurable antennas [1].

Theoretically, signal measurements performed at both link ends should be equal and therefore provide a direct source for unique symmetric key generation based on the channel behavior. The channel variation can indeed be considered random, unpredictable, and also unique for the legitimately communicating parties, further called Alice and Bob. An eavesdropper, further named Eve, does not share the same physical channel and therefore cannot record the same channel variations when intercepting the signals [2], [3].

In a practical application, there is however a small delay between reciprocal channel measurements. Common off-the-shelf wireless sensor transceivers operate in half-duplex mode, alternately switching between transmit (TX) and receive (RX) mode. Often the delay between reciprocal channel measurements is several milliseconds, allowing significant channel variation between both measurements [4]. Even if the measurement time slot is smaller than the coherence time of the channel, significant variation regularly occurs during signal notches caused by destructive interference within the measurement interval. This phenomenon leads to reduced measurement accuracy and key errors, ultimately compromising the key-generation rate due to the required thresholding to lower the Key Error Rate (KER).

In this paper the time slot for reciprocal channel measurement is reduced by almost an order of magnitude, to $614\ \mu$s instead of $5\ ms$ in earlier publications [4]–[6]. This is possible thanks to an embedded software update on the wireless nodes, enabling the automatic TX-to-RX and RX-to-TX turnaround mode of the ADF7242 transceiver.

Because of the much faster turnaround time, channel measurements are expected to be more accurate, resulting in a lower KER and an improved key-generation rate. However, the measurements illustrate that although a limited improvement is obtained, the performance gain is less than expected. Clearly, other non-identified causes of non-reciprocity are further limiting the key generation.

II. Materials and Methods

A. Measurement nodes

The wireless nodes employed for key generation are fully wearable units, composed of an RF circuit integrated onto a textile patch antenna. The circuit employs the Analog Devices ADF7242 transceiver, directly connected to the feed points of the dual-polarized textile antenna. The circuit further includes a Silicon Laboratories C8051F920 low-power low-profile micro controller, 1 Mbit Electrically Erasable and Programmable Read Only Memory (EEPROM) as well as a three-axis accelerometer with ± 3 g measurement range. The wearable node also includes a thin battery and hence is fully autonomous without any wired connections.

The front and back side of the nodes are visible in Fig. 1. Both nodes are operational and exchange packets in order to perform reciprocal channel estimations every 100 ms. Their signals are picked up by the Printed-Circuit Board (PCB) dipole antenna connected to the spectrum analyzer, which is configured in zero span to present a time domain plot of the received power.

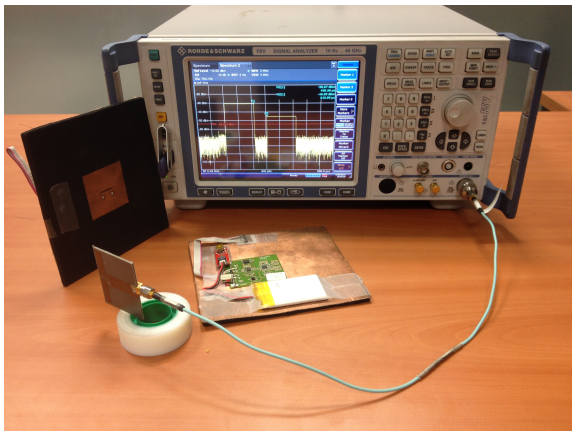

Fig. 1. Rohde & Schwartz FSV40 spectrum analyzer receiving the signals of the pair of wearable wireless nodes employed for key generation.

The measurement results are more clearly visible in the screenshot presented in Fig. 2. Alice's node is standing up, with its radiating patch facing towards the dipole, whereas Bob's node is laying face down on the table. The measurement is triggered by the first rising edge of the measured power, occurring at 0 μs, caused by Alice's transmission. Marker M1 shows the length of Alice's transmission, being 428 μs, together with a received power of -31 dBm. Marker M2 displays the start of Bob's responding transmission at 614 μs, defining the separation of the reciprocal channel measurements in the time domain. Note that Bob's signal produces a received power of -45 dBm on the dipole, 14 dB less strong than Alice's signal due to the difference in orientation of the antennas. Bob's packets are equal in length to Alice's packets and therefore his transmission also lasts 428 μs.

Transmissions are performed in IEEE802.15.4 mode, allowing a very reliable communication, with data integrity guaranteed by means of a Cyclic Redundancy Check (CRC).

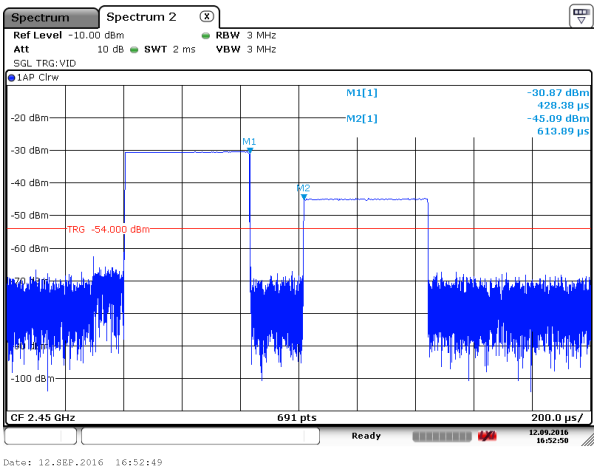

Fig. 2. Time-domain plot of the reciprocally transmitted signals, as captured by a Rohde & Schwartz FSV40 spectrum analyzer, displaying the 614 μs TX-RX turnaround time.

The transmission header consists of a preamble sequence and the Start Frame Delimiter (SFD). The channel measurement is performed during 128 μs, immediately following the SFD. The average value is transferred to the micro controller as an 8-bit Received Signal Strength Indication (RSSI) value expressing the received power in dBm. The measurement has a resolution of 1 dB and a specified accuracy of ± 3 dB [7].

B. Body-worn measurement setup

In the measurement for channel-based key generation, the nodes are worn on the torso of Alice and Bob. The nodes are taped on the front side of two T-shirts and are so flat and flexible that the wearers hardly notice their presence. Alice and Bob then perform a random walk for half an hour in a lab environment.

Measurements are performed first for a Line of Sight (LoS) path between Alice and Bob, and are then repeated for a Non Line of Sight (NLoS) path. The latter path is created by placing an array of radio frequency absorbers between the trajectories covered by Alice and Bob.

Measurements are performed without an eavesdropper (Eve) for several reasons. Eve cannot reliably detect and process the packets transmitted with a gap of only 186μs in between. The reduced round-trip delay does not make key extraction for the eavesdropper easier.

To allow faster operation, measurements by Alice and Bob are now directly saved to local EEPROM memory for later readout and post processing. Furthermore, the inability of an eavesdropper to extract RSSI measurements allowing to crack the key has already been shown in [4].

III. Measurement Results

A. Time-domain behavior

The time-domain plot in Fig. 3 displays an extract of a set of 16859 reciprocal channel measurements, performed during the following operational sequence:

- Alice transmits a packet.
- Bob receives this packet and measures the RSSI.
- Bob acknowledges reception by transmitting a packet, 614μs after Alice's start of transmission.
- Alice receives this packet and measures the RSSI at 614μs.
- Bob acknowledges reception a second time, by transmitting a packet 5 ms after Alice's start of transmission.
- Alice receives this packet and measures the RSSI at 5 ms.

Clearly the figure displays measurements that match well, with sporadic deviations. The measurement with smaller turnaround delay is often more accurate, showing more reciprocity, as is the case in the event marked 'B'. Here, Alice's channel measurement at 614μs accurately follows the fading dip measured by Bob, whereas this is not the case for the measurement after 5 ms.

However, other deviations remain, as for example marked by 'A'. There, both channel measurements by Alice fit well, but Bob's measurement is off by up to 10 dB. The cause of this repetitive phenomenon will be further analyzed in this paper. Clearly it is not caused by static system imbalances. The figure is representative for the signal behavior in the full set of 16859 measurement points.

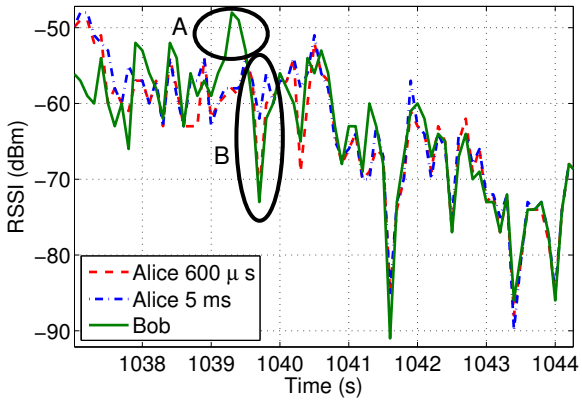

Fig. 3. A small extract of the reciprocal NLoS channel measurement performed by Bob and then by Alice, 614μs and 5 ms later.

B. Statistics and mutual information

The correlation coefficients for the RSSI values measured by Alice and Bob at time intervals of 614μs and 5 ms are calculated for the values expressed in dBm, as these are the values which are directly used by the quantizer. Table I shows that the correlation is slightly higher with the reduced measurement interval. Of course, the correlation is already very high for both cases, illustrating the large, but not perfect, reciprocity of the channel measurements. The mutual information between Alice and Bob's sets of values is listed in Table II. The mutual information is expressed in bits per channel sample and is slightly higher for channel measurements with the reduced measurement interval. The increase of correlation and mutual information thanks to the shorter measurement interval is however only around 1%.

TABLE I
CORRELATION COEFFICIENTS BETWEEN ALICE AND BOB'S RSSI VALUES, FOR LOS AND NLOS, AT 614μS AND 5000μS MEASUREMENT INTERVALS

	$\Delta t_1 = 614\mu$s	$\Delta t_2 = 5$ ms
LoS	0.8732	0.8595
NLoS	0.8561	0.8492

TABLE II
MUTUAL INFORMATION BETWEEN ALICE AND BOB'S RSSI VALUES, FOR LOS AND NLOS, AT 614μS AND 5000μS MEASUREMENT INTERVALS

	$\Delta t_1 = 614\mu$s	$\Delta t_2 = 5$ ms
LoS	1.2703 bit	1.2091 bit
NLoS	1.2648 bit	1.1960 bit

C. Key generation

In order to generate practical keys, the following procedure is used. A quantizer at Alice's side extracts one bit per channel measurement according to the following steps:

- Determine the moving average of the last 70 RSS values (corresponding to the average over the last 7 s) [4].
- If the current RSS value crosses a threshold of N dB above or below this value, a 1 or a 0 key bit is generated, respectively. Alice informs Bob about the generation of a key bit via the wireless channel, without revealing the actual value of the bit.
- In case the threshold is not crossed, no key bit is generated.

Bob's quantizer also extracts one bit per channel measurement:

- Determine the moving average of the last 70 RSS values.
- If Bob is informed by Alice that she has generated a key bit, Bob also generates a key bit:
  - A 1-bit is generated if Bob's measured RSS value is above the moving average
  - A 0-bit is generated otherwise

Higher threshold levels result in better matching raw keys, but limit the key generation rate as more measurements are dropped. The raw keys also need further reconciliation to exactly match. The $(11, 7)$-Hamming forward error correcting code is employed to achieve this. After pseudo-random bit interleaving, Alice's raw key, considered the master key, is subdivided into 11-bit groups. For each group, four Hamming check bits are transmitted to Bob, allowing Bob to correct key errors. Finally, de-interleaving is performed to undo the interleaving. Interleaving scrambles bits in pseudo-random order to spread subsequent key errors over a large number of code words, improving the performance of the reconciliation algorithm.

D. Key Error Rate after reconciliation

The resulting KER after reconciliation is displayed in Fig. 4 for the NLoS measurement and in Fig. 5 for the LoS scenario. The advantage of faster reciprocal measurements is only

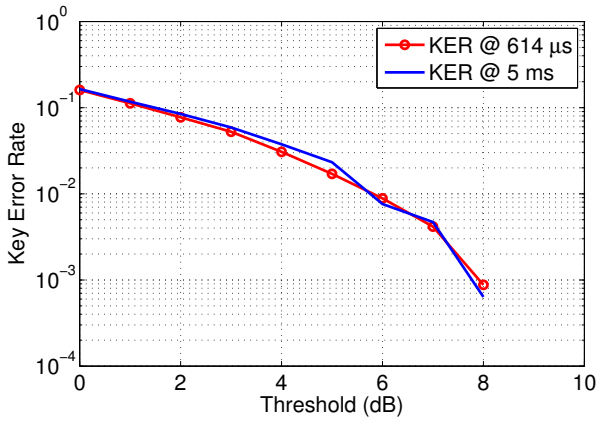

Fig. 4. Key Error Rate (KER) for the Non Line-of-Sight (NLoS) measurement after reconciliation with various thresholds, for reciprocal channel measurements within 5 ms and 614μs.

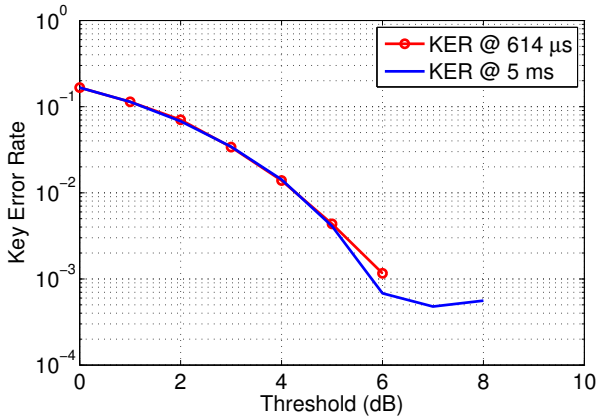

Fig. 5. Key Error Rate (KER) for the Line-of-Sight (LoS) measurement after reconciliation with various thresholds, for reciprocal channel measurements within 5 ms and 614μs.

visible in the NLoS measurement. Apparently the channel variation in the LoS case is not fast enough in order to obtain a further improvement at 614μs measurement interval instead of 5 ms. In the NLoS case an improvement is obtained, with a zero KER occurring at a threshold level of 7 dB for the 614μs measurement interval, instead of 9 dB for the 5 ms interval. Corresponding to earlier indoor measurements [6], the KER decreases with a steeper slope for the LoS case, compared to the NLoS case.

E. Analysis of measurement accuracy

In order to study the nature of the remaining measurement inaccuracies, the average response of Alice and Bob's detectors is displayed in Fig. 6. The graph shows the average of the signal strengths in dBm as measured by Alice, corresponding to each set of equal signal values measured by Bob. For example, each time Bob measures a signal level of -60 dBm the corresponding signal level measured by Alice is collected and the average of all these collected values is represented in the graph as the corresponding average value for Alice's detector. Note that the NLoS and LoS measurements both have 16859 and 19958 measurement points, respectively. Compared to the LoS measurement, the range of signal levels is more limited for NLoS, due to the higher attenuation in the propagation path. The average response of the detectors matches very well over the whole range of the measurement, corresponding to the ± 3 dB accuracy mentioned in the data sheet [7] of the transceiver chip.

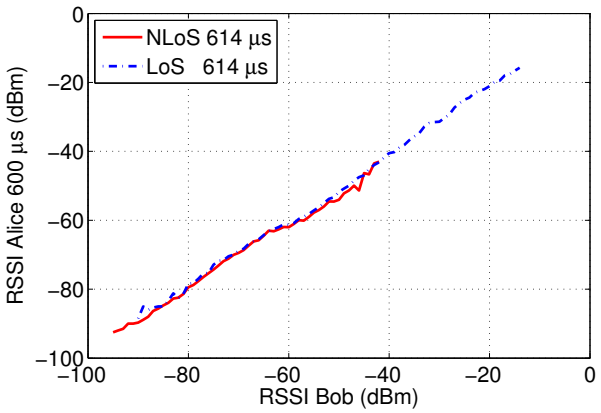

Fig. 6. The average response of the reciprocal detectors at 614μs measurement interval.

A histogram of the errors for the NLoS and LoS measurements is displayed in Fig. 7. The error value in dB is defined as the difference between the signal levels measured by Alice and Bob, with the 614μs interval. The LoS measurement is truncated to 16859 signal values, in order to make both data series equal in length. The histograms of the errors are very similar for NLoS and LoS propagation, both showing a symmetric distribution. Around 80% of the errors are within ± 3 dB and around 90% of errors within ± 6 dB, corresponding to the detector's specifications. The errors of reciprocal measurements performed each 100 ms are also not correlated in time, with larger errors appearing sporadically and at random.

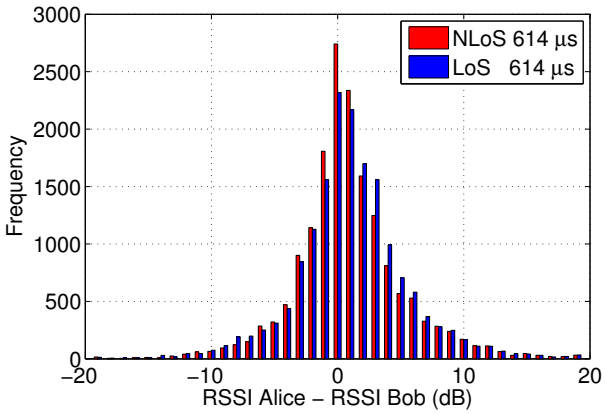

Fig. 7. Histogram of the difference between Alice and Bob's measurements for both time intervals.

IV. Discussion

The research and development to obtain faster reciprocal channel measurements, as outlined in this paper, was performed with the expectation that measurements performed by Alice and Bob would match significantly better with only 614μs delay in between them, compared to 5 ms in previous publications [6]. However, the improvement in practical key generation is limited and only visible for the measurement in NLoS conditions, where the threshold level for a zero KER is 2 dB lower, resulting in fewer discarded channel samples and hence a higher key-generation rate.

Measurements at the faster measurement interval are shown to be more accurate, with a slightly higher correlation coefficient and a comparably increased mutual information for the measurement sets recorded by Alice and Bob. As the improvement by decreasing the measurement time by an order of magnitude is limited, the channel is clearly sampled fast enough for body centric propagation conditions.

The remaining differences in measurements performed by Alice and Bob are therefore not due to channel variation within the measurement time. The correlation for both channel measurements performed by Alice at 614μs and 5 ms is as high as 0.95 and hence significantly higher than the correlation between Bob's measurements and Alice's measurements despite the much shorter time interval of 614μs.

Static imbalances cannot cause the sporadically occurring deviations between measurements performed by Alice and Bob. Moreover, an analysis of the average signal levels detected by Alice corresponding to each set of equal signal levels measured by Bob resulted in an accurate characteristic, revealing little static system imbalance.

A potential issue is the fact that the ADF7242 transceiver's impedance at the antenna port differs a lot depending on the receiving or transmitting state, the data sheet [7] lists $74.3 - 10.7j\Omega$ and $43.7 - 35.2j\Omega$, respectively. Possibly the variable capacitive loading of the antenna's matching circuit due to the proximity of the human body has effects which are different depending on the receiving or transmitting state. This phenomenon is currently being further investigated, but is not expected to be the main source of remaining differences in reciprocal measurements.

A further analysis of the measurements displays a symmetric distribution of the measurement errors, which are defined as the difference in signal levels measured by Alice and Bob, separated in time by 614μs. Considering that 90% of the errors are within ± 6 dB, combined with the symmetric error distribution with rapidly decreasing probability for the larger measurement errors, the remaining errors in the reciprocal channel measurements are likely due to the inaccuracy of the transceiver chip's signal level detector. This detector is not developed or specified as a measurement device but merely as a means of received signal strength indication.

V. Conclusions

Reciprocal channel measurements performed by body-worn sensor nodes can be used to extract encryption keys. This was documented in earlier publications, where some differences in channel measurement values remained. It was assumed that fast channel variation was the cause of these differences, considering the reciprocal measurements were separated 5 ms in time.

The embedded software of the body-worn sensor nodes was modified, allowing to reduce the interval at which reciprocal channel measurements are performed by almost an order of magnitude, from 5 ms (in previous publications) to 614 μs. A measurement campaign was organized, collecting large measurement sets for Line of Sight as well as Non Line of Sight propagation conditions.

The measurements successfully reproduce earlier results, with correlation and mutual information slightly improved thanks to the faster reciprocal channel measurements. However, only a limited performance enhancement is observed for practical key generation. The enhancement only occurs in case of a Non Line-of-Sight propagation path, where the threshold level required for a zero key error rate is reduced by 2 dB. Further apparent non-reciprocity in the channel measurements can probably be attributed to inaccuracy of the received signal strength indication in the transceiver chip.

Acknowledgment

Part of this work was supported by BELSPO (Belgian Federal Science Policy Office) through the IAP (Interuniversity Attraction Poles) Phase VII BESTCOM (BElgian network on STochastic modelling, analysis, design and optimization of COMmunication systems) project.

References

[1] Mehmood, R.; Wallace, J.; Jensen, M. Key establishment employing reconfigurable antennas: Impact of antenna complexity. *IEEE Transactions on Wireless Communications* 2014, *13*, 6300–6310.

[2] Chen, C.; Jensen, M. Secret key establishment using temporally and spatially correlated wireless channel coefficients. *IEEE Transactions on Mobile Computing* 2011, 10, 205–215.

[3] Premnath, S.N.; Jana, S.; Croft, J.; Gowda, P.L.; Clark, M.; Kasera, S.K.; Patwari, N.; Krishnamurthy, S.V. Secret key extraction from wireless signal strength in real environments. *IEEE Transactions on Mobile Computing* 2013, *12*, 917–930.

[4] Van Torre, P.; Castel, T.; Rogier, H. Encrypted body-to-body wireless sensor node employing channel-state-based key generation. In Proceedings of the *10th European Conference on Antennas and Propagation (EuCAP)*, Davos, Switzerland, 10–15 April 2016; pp. 1–5.

[5] Castel, T.; Van Torre, P.; Rogier, H. RSS-based secret key generation for indoor and outdoor WBANs using on-body sensor nodes. In *Proceedings of the 2016 International Conference on Military Communications and Information Systems (ICMCIS)*, Brussels, Belgium, 23–24 May 2016; pp. 1–5.

[6] Van Torre, P. Channel-Based Key Generation for Encrypted Body-Worn Wireless Sensor Networks. In *Sensors* 2016, 16, 1453.

[7] Analog Devices, Low Power IEEE 802.15.4/Proprietary GFSK/FSK Zero-IF 2.4 GHz Transceiver IC", ADF7242 datasheet, 2010.