A Novel Algorithm for Secret Key Generation in Passive Backscatter Communication Systems

Mohammad Hossein Chinaei[†], Diethelm Ostry[⋆], Vijay Sivaraman[†]

[†]University of New South Wales, Sydney, Australia
[⋆]Data61, CSIRO
m.chinaei@unsw.edu.au, diet.ostry@data61.csiro.au, vijay@unsw.edu.au

Abstract. The extreme asymmetry of passive backscatter communications systems such as passive Wi-Fi, while allowing significant reduction of node power consumption for communications, imposes severe resource limitations on implementing secure communications. Target applications for this technology are typically driven by the promise of low power consumption, up to four orders of magnitude lower than commercial Wi-Fi chipsets. Industry standard security approaches using encryption technology are problematic in this power regime, particularly as the potential low complexity and size of passive nodes will encourage application to high-density networks of very small, energy-poor devices. Generation of shared symmetric keys through reciprocal channel measurements, for example of received signal strength (RSS), is a natural approach in this situation. However previous work in this area has focused on the symmetric case where base station and nodes communicate at the same radio frequency. Backscatter communications uses two frequencies, typically a pilot beacon transmitted by a base station on one frequency, and response on a shifted frequency. This paper describes a protocol for RSS-based shared key generation for this architecture and reports the results of an experimental implementation using software radio emulation of backscatter communication.

Keywords: Physical layer security · Secret key generation · Passive sensors · Backscatter communication

1 Introduction

Power consumption remains a key limiting constraint in achieving long-lived networks of wireless sensor nodes, and communications is typically a major component of their power budget. The appearance of many applications requiring small low-power sensors in areas such as the Internet of Things (IoT), wearable devices, and implantable medical sensors, has attracted a great deal of research interest in techniques able to achieve low-power communications. The most extreme approaches to date employ backscatter technologies which can reduce power consumption by orders of magnitude through transfering as much as possible of the power-consuming transmitter functionality of the wireless communications

system out of the nodes and into the base station. Instead of implementing an active wireless transmitter, with correspondingly large power consumption, a node or "tag" employing backscatter communications uses relatively simple RF circuitry to receive, modulate, and reflect either ambient wireless transmissions or beacon signals provided by a base station or "reader".

For example, the authors in [1] presented a "Wi-Fi backscatter" approach as a practical technology for wireless communication for passive sensors. A Wi-Fi backscatter tag is able to send data at a rate of a few kbps to a commodity receiver over a range of 2 meters by modulating ambient Wi-Fi communications packets and thereby influencing the channel state visible to the reader. In [2] the authors propose a similar technique to modulate ambient Bluetooth low power packets and extended the range to over 9 meters. In [3–6] the authors extend the idea of backscatter communication using Wi-Fi signals using different approaches. Interference cancellation is proposed in [3] so that the same frequency can be used by both beacon signal from reader to tag and the reflected signal from tag to reader. In [4–6] the authors use dual frequencies to achieve compatibility with current commercial Wi-Fi devices.

In "passive Wi-Fi" [5], the reader (which can employ standard Bluetooth and Wi-Fi chipsets) sends out a continuous wave (CW) beacon on a Bluetooth frequency. The passive tag modulates its information on the received beacon, shifts its frequency and reflects a normal Wi-Fi (802.11b) packet back to the reader. This technology can provide in principle up to 11 Mbps at 10^{-4} times lower power than current active Wi-Fi chipsets. All these reported technologies have been implemented and tested under real world conditions and for some of them IC implementations have also been designed. It appears likely that many novel applications will become feasible with these new ultra-low-power passive technologies based on backscatter communication.

One of the attractive new application areas is wearable devices, for example for physiological and medical monitoring purposes. Such devices are ideally small and lightweight which restricts their battery capacity and so makes them ideal candidates for using the ultra-low-power backscatter communications technologies. However the communications system in this and other applications may carry sensitive information, e.g. commercial, personal and medical data and so a security capability is often mandatory. In view of the limited computational capabilities of the devices, their deployment in perhaps not-easily-accessible locations, and potentially in large numbers, it is challenging to devise practical security mechanisms to protect their data. Cryptographic means of implementing data confidentiality require the secure distribution of keys between the communicating devices and this is a power-intensive task in a wireless system, making it problematic for ultra-low-power devices.

The use of the wireless channel itself (often termed the physical (PHY) layer for convenience) as a source of shared key material has been studied extensively in recent years [7, 8]. From physical principles, the channel is intrinsically reciprocal, i.e. both parties in a wireless communication see the same propagation parameters to within a constant factor, and an eavesdropper in a sufficiently

removed location cannot determine those shared parameters. What makes this appealing in the low-power regime is that measurements of the channel parameters can often be made as part of the usual communications protocol without incurring the power overhead of a cryptographic key-exchange protocol. Regular re-keying is generally required in practice for maintaining security and so the secret key generation rate is also a matter of concern in some applications. Researchers have explored high rate key bit extraction in [9–11]. However, in [12], it is shown that for IoT and wearable sensors where high bit rate is not a critical issue, low-complexity algorithms provide benefits in overall device energy consumption.

All the previous work on using the wireless channel to generate shared keys has addressed active symmetric communications where the two communicating parties alternately transmit to each other and make independent measurements of channel properties at the same frequency. However, the inherent asymmetry of passive backscatter communication makes this approach inapplicable. In the "passive WiFi" scenario for example, the reader emits a beacon at one frequency and the tag reflects a WiFi signal at a different frequency. A new approach is needed to generate shared keys from wireless channel properties at two frequencies and in a way which is secure from eavesdropping.

In the remainder of this paper we describe such an approach. Our specific contributions are:

1. We describe a straightforward secret key generation scheme modified for use by passive sensors which implement asymmetric backscatter communication. We develop a three-step protocol to measure received signal strength (RSS) at dual frequencies, allowing a reader and tag to establish a secret shared key with high agreement in principle. We use the universal software radio peripheral (USRP) platform to test the approach experimentally.
2. We identify a specific problem with key generation based on wireless channel parameters caused by the dual frequency operation inherent in many practical backscatter schemes like "passive WiFi".
3. We propose an enhanced of the basic algorithm and device design to allow secure shared key generation in the backscatter communications system.

The rest of the paper is organised as follows: in Section 2, the basic system architecture is outlined and the protocol for secret key generation is developed. In Section 3, an experimental evaluation of the protocol is presented. A theoretical and practical analysis is carried out to establish the security risks of the proposed protocol. In Section 4, an enhancement of the protocol and device is described and evaluated. The paper is concluded in Section 5 with directions to future work.

2 Basic system architecture

2.1 System model

A data communications transmitter typically comprises a digital baseband processor which constructs an analog signal at a convenient low (baseband) fre-

quency and an RF section which shifts the signal to the final frequency and amplifies it to the required power level. To achieve adequate transmit power, the RF section usually uses an architecture which consumes far more power than the baseband processor. Backscatter communication eliminates the power consuming analog RF part of the transmitter and effectively offloads its function to the reader device (which could be a smart phone in practice). Passive tags do not have the usual active transmitter function but instead essentially piggyback information on ambient communications signals or a reader–generated beacon. Their RF circuitry is far less complex and requires far less power than an active transmitter. Of course also it generates far less RF signal power and so there is a corresponding cost in range reduction. It is convenient to shift the frequency of the tag's reflected signal so that the reader's beacon signal can be at a placed at a non-interfering frequency (e.g. in the Bluetooth band for a backscattered signal in the WiFi band).

PHY layer secret key generation relies on reciprocity of electromagnetic propagation, i.e. two communicating parties under general conditions will independently see identical channel properties. In other words, if two parties, reader and tag, consecutively exchange signals with each other (in less than channel coherence time, i.e. the time during which the channel is effectively constant) so that each can estimate the channel they see, their estimates would match. However, there are two major differences in the backscatter scenario. First, the tag is not able to make an independent transmission but can only reflect the reader's beacon signal. Second, the tag and reader receive signals at different frequencies which may be sufficiently separated to have different channel propagation properties (for example in passive Wi-Fi they are 11MHz apart).

2.2 Asymmetric channel measurements

There are a number of channel characteristics on which key generation can be based, for example the spectrum of multipath components, complex (magnitude and phase) link gain, and received signal strength (RSS). RSS is by far the easiest to implement and measure, particularly by resource constrained devices and so is best suited to backscatter nodes. Our basic system model includes a reader, a tag and an eavesdropper (Eve). The tag is assumed to have two different operation modes, reflecting and listening. In reflecting mode, the tag can only retransmit the modified beacon signal back to the reader. However, in the listening mode, the tag can listen to the reader and measure the RSS of its beacon signals.

The channel characteristics (e.g. RSS) between the legitimate parties, reader and tag, are assumed to fluctuate sufficiently for key generation. The fluctuation may be due to tag motion for example or the motion of other nearby entities which change the multipath environment. Eve is presumed to be a passive attacker who is able to measure the RSS of different signals transmitted from the reader or reflected from the tag but does not transmit any signals.

The reader transmits a beacon signal at f_1 and receives the tag's reflection at f_2 which causes the RSS at the reader to be influenced by the channel gains at

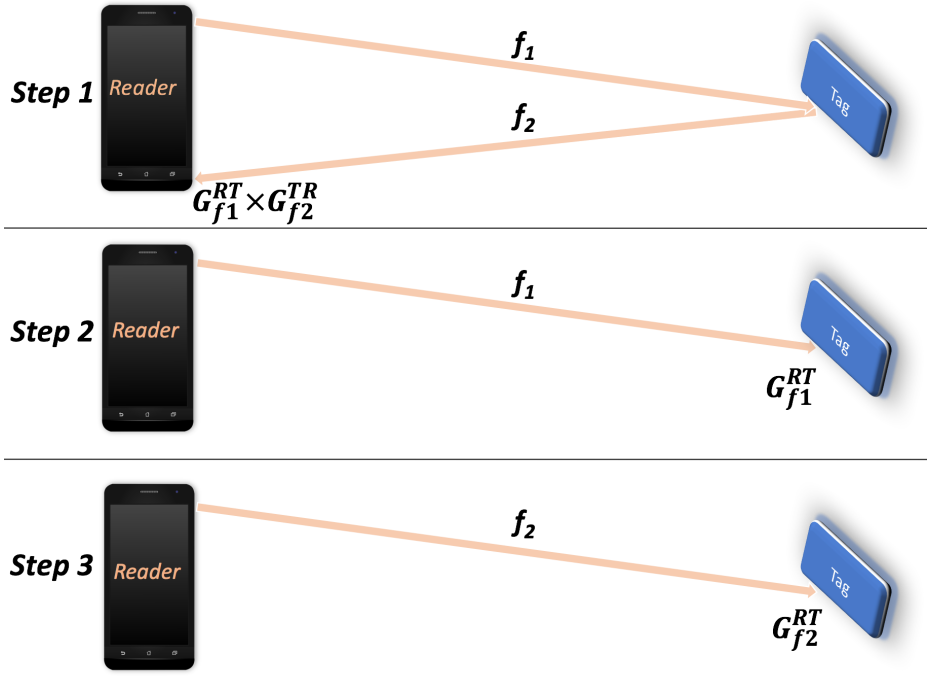

Fig. 1. Asymmetric channel measurement steps

both f_1 and f_2. The reader uses this composite RSS to generate its key. Accordingly, the tag also needs to be provided with the same channel gain information at the same two frequencies. To achieve this, our basic protocol [13] uses the following three-step scheme (see Fig. 1):

1. The reader transmits a CW beacon signal at f_1 to the tag (which is in the reflection mode at this step). The tag reflects the received signal at the second frequency, f_2. The reader measures the RSS of the reflected signal which is the product of channel gains at the two frequencies, i.e. $G_{f_1}^{RT} G_{f_2}^{TR}$.
2. The tag listens at frequency f_1. The reader transmits a CW beacon at f_1. The tag measures the RSS giving it an estimate of channel gain at f_1, i.e. $G_{f_1}^{RT}$.
3. The tag listens at frequency f_2.The reader transmits a beacon at f_2. The tag measures the RSS to estimate the channel gain at f_2, i.e. $G_{f_2}^{RT}$.

The three steps take place consecutively and one set of three steps forms a single round of the key generation protocol. At the end of each round, the tag and reader have independent estimates of the same channel properties. The tag multiplies the gains it measured at steps 2 and 3 to form an estimate of $G_{f_1}^{RT} G_{f_2}^{RT}$. The reader measures its estimate of $G_{f_1}^{RT} G_{f_2}^{TR}$ in step 1. If the channel

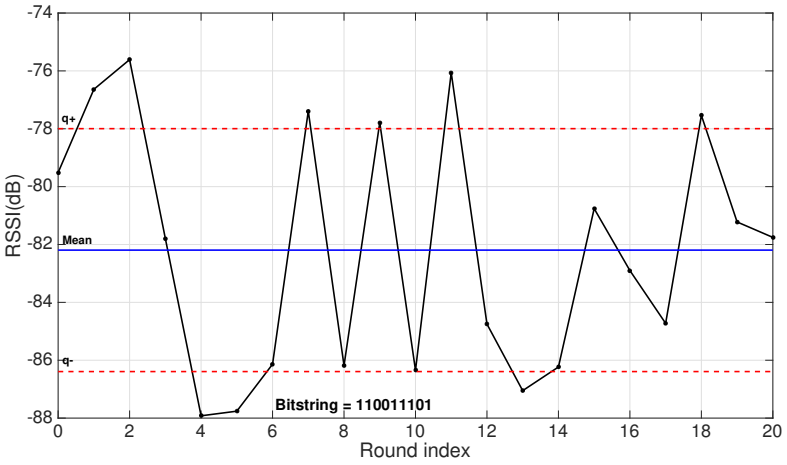

Fig. 2. Level crossing quantisation technique.

has remained essentially constant over the duration of a protocol round the tag's and reader's estimates of the gain product would be expected to be in high agreement because of channel reciprocity and so can be used as a source of shared entropy for key generation.

The gain product $G_{f_1}^{RT} G_{f_2}^{RT}$ is used by the reader and tag to generate their keys. The eavesdropper Eve is able to make two different estimates of this product after every round of the protocol. The first estimate is available at step 1, where she receives the reflection signal from the tag, the product of two channel gains: reader-tag link at frequency f_1, $(G_{f_1}^{RT})$ and tag-Eve link at frequency f_2, $(G_{f_2}^{TE})$. This estimate will be termed Eve's reflection estimate: $G_{f_1}^{RT} G_{f_2}^{TE}$. Eve's second estimate, termed the product estimate, is generated by multiplying the RSS values she sees at steps 2 and 3 (channel gains of reader-Eve link at f_1 and f_2), i.e. $G_{f_1}^{RE} G_{f_2}^{RE}$.

2.3 Quantisation process

After a sequence of protocol rounds in which consecutive channel measurements are made, both reader and tag apply a quantisation process to convert the raw channel measurements into a key bit string. We use the level crossing quantisation technique first proposed in [14]. In this method, an adaptive sliding window of length W_Q is defined to select a block of consecutive raw measurements. In each block upper and lower levels are defined as follows:

$$q+ = \mu + \alpha\sigma$$

$$q- = \mu - \alpha\sigma$$

where μ is the measurement mean, σ is the standard deviation, and $0 \leq \alpha \leq 1$ is a parameter which can be adjusted to trade off key bit rate against key bit agreement. Each of the RSS measurements inside the window produces a key bit value of 1 if it is greater than the upper quantisation level ($q+$) and 0 if it is smaller than the lower level ($q-$). Measurements which fall between two levels of quantisation are discarded (see Fig.2). The quantisation parameters are the same for both legitimate sides of the communication and we assume Eve knows the quantisation algorithm.

When the parameter α is small, most of the RSS measurements contribute key bits, leading to a higher key bit generation rate although the key bit agreement is likely to decrease drastically due to deriving key bits from uncorrelated noise. On the other hand, for α near 1 and higher, many usable RSS measurements are discarded, thereby reducing the key bit generation rate, but also reducing key discrepancies due to noise. In our target application, higher key agreement is desirable in order to minimise the cost of any subsequent key reconciliation process [12].

2.4 Security Considerations

Threat Model: In this work we are concerned with the threat posed by an eavesdropper who is able to detect all key-generation communications. An eavesdropper is assumed to have full knowledge of the system protocols and is not limited substantially in computational power or receiver capability (e.g. she can receive at multiple frequencies simultaneously). However we restrict an eavesdropper to be passive, i.e. is unable to generate spoofing signals.
Secrecy: A crucial assumption is that any eavesdropper is sufficiently far from the legitimate parties that her radio channel characteristics are uncorrelated with those of the legitimate parties. A half-wavelength separation is theoretically adequate in a multipath–saturated environment, but in practice considerably greater distances may be required [8] and in general the extent of eavesdropper–exclusion zones must be established through measurement or propagation modeling. Backscatter systems have relatively short range due to their passive nature reducing the tag's signal power and this may make an eavesdropper who is close enough to detect the backscattered signal more physically evident.

Although two frequencies are used in backscatter systems, we do not rely on their being uncorrelated. In fact the enhanced algorithms we introduce in Section 4 attempt to remove the effect of propagation variations at one of the frequencies. Under our system assumptions, the channel variation at the second frequency can be assumed to be adequate for key generation.

We note that in our protocols, the reader drives the protocol sequence and can therefore in principle monitor the radio environment and detect some spoofing attacks, e.g. by listening for false beacon signals or signal collisions which would indicate attempts to inject counterfeit backscatter signals over the legitimate backscatter signals. The true backscatter signal is returned essentially instantaneously apart from propagation delays, making it more difficult for an active attacker with powerful transmitter (to operate at a standoff for example)

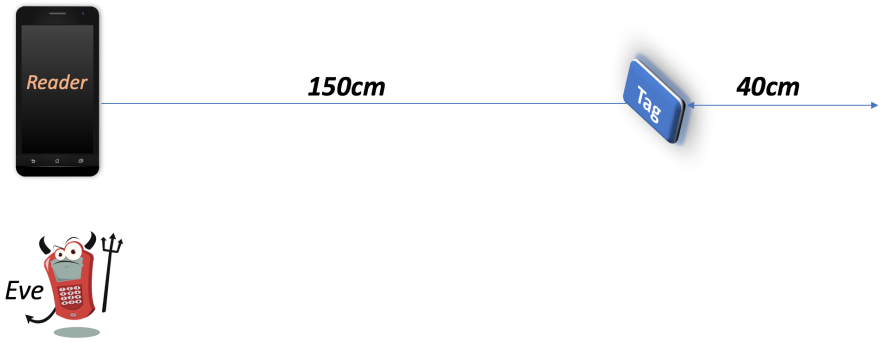

Fig. 3. System model

to impersonate a legitimate backscatter node. It would also be difficult for an active attacker to ensure that her signal levels at the reader were such that they did not reveal she could not be a backscatter device.

3 Evaluation and analysis

3.1 Evaluation

System model and channel measurements We implemented and evaluated the performance of our proposed protocol on USRP software–defined radios. The three nodes in our scenario are represented by three different USRPs, each connected to a PC running LabView software as the control interface. The dual frequencies chosen were $f_1 = 2.171GHz$ and $f_2 = 2.182GHz$, different from standard Wi-Fi and Bluetooth frequencies because of equipment limitations, but $11MHz$ apart as in passive Wi-Fi. The corresponding wavelength is about $14cm$.

Since we are extracting keys from wireless channel characteristics, the channel is required to fluctuate sufficiently to provide key generation at an adequate rate [12, 14] and this is achieved in our experiments by moving the tag through a sequence of positions. In the configuration shown in Fig. 3, the reader and eavesdropper Eve are stationary and the tag moves randomly about 5cm after each 5 rounds of the protocol. The distance between the two legitimate parties (reader and tag) is varied between $150cm$ to $190cm$. In each experiment, Eve is located at a different distance from the reader. We chose the configuration where Eve is close to the reader as the worst case since her channels are then most geometrically similar to the tag–reader channels used for key generation.

In the first experiment (Fig. 4), Eve is located 42cm, about 3λ, from the reader. In subsequent experiments, this distance is increased to 52cm (4λ) and 84cm (6λ), shown in Fig. 5 and Fig. 6, respectively. In each figure, we have four

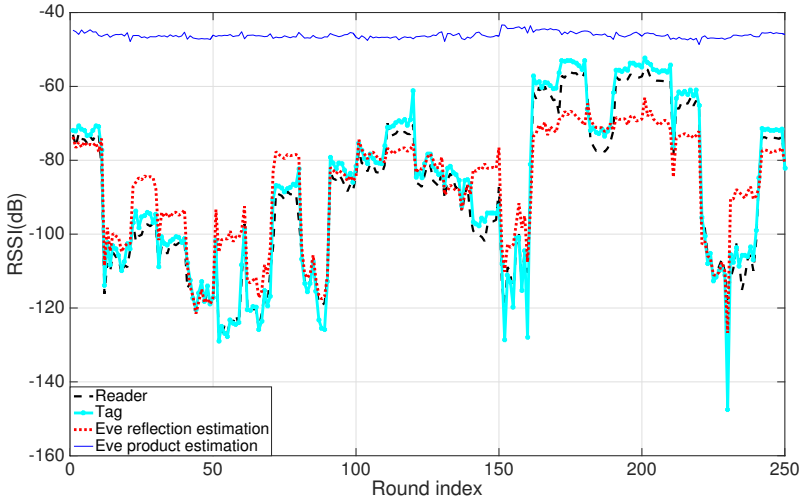

Fig. 4. RSS measurements when the distance between reader and Eve is 42cm $\approx 3\lambda$.

different curves corresponding to reader's RSS measurement of the backscattered signal, the tag's estimation, which is the product of its RSS measurements at steps 2 and 3, Eve's reflection estimation, based on what she measures at step 1, and Eve's product estimation, based on the product of her RSS measurements at steps 2 and 3. Each experiment comprises 250 protocol rounds lasting about 12 minutes. The Pearson correlation coefficients between measurements at different nodes are shown in Table 1. The correlation coefficient always lies in the range $[-1, 1]$, where 1, 0, and -1 represents perfect correlation, no correlation and anti-correlation respectively.

Table 1. Correlation coefficient between different node signals

Distance between Reader and Eve	Correlation between Reader and Tag	Correlation between Reader and Eve reflection estimation	Correlation between Reader and Eve product estimation
42cm $\approx 3\lambda$	0.99	0.90	0.16
56cm $\approx 4\lambda$	0.99	0.90	0.02
84cm $\approx 6\lambda$	0.99	0.80	0.16

Secret Key generation: As outlined in Section 1, we use a level crossing quantiser to generate key bits from the RSS measurements of reader and tag. All of the nodes in the experimental scenario record the round index of a successful measurement, i.e. one which produced a key bit. The actual shared key bit string

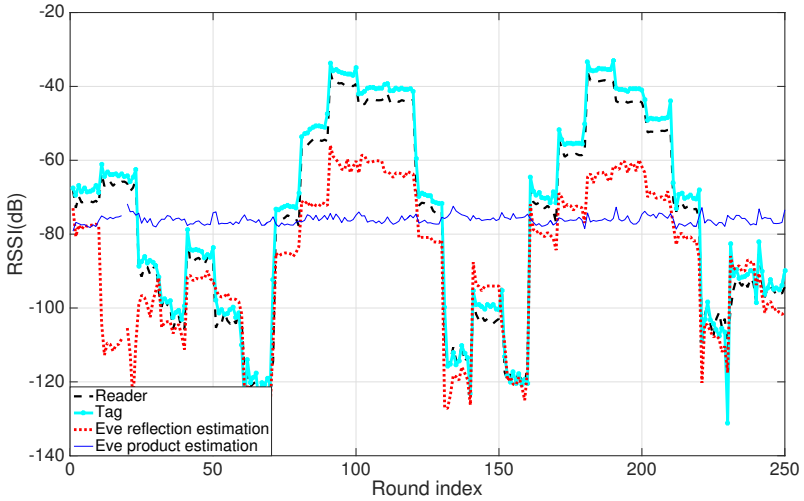

Fig. 5. RSS measurements when the distance between reader and Eve is 56cm $\approx 4\lambda$.

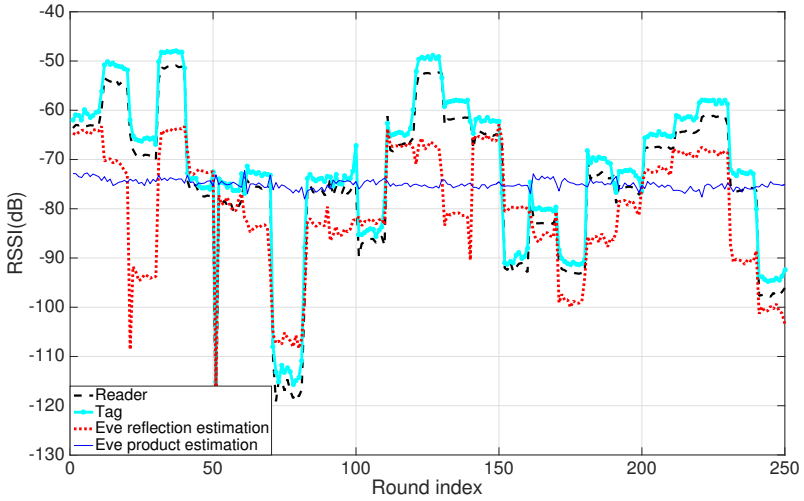

Fig. 6. RSS measurements when the distance between reader and Eve is 84cm $\approx 6\lambda$.

is established through subsequent communication between reader and tag over a public channel. The reader and tag agree on a key bit sequence by exchanging their successful round indices. They discard any bits which do not correspond to a successful round index for both. In this way the reader and tag only keep the key bits formed from successful round indices at both sides. Since a public channel is used by the legitimate parties to exchange successful round indexes, Eve also knows the exact round indices used for secret key generation. However,

if the RSS measurements at Eve are uncorrelated with the shared measurements at the tag and reader, the successful round indices alone are not be helpful to her. Table 2 shows the key bit agreement between three parties for different window sizes (W_Q) of the quantiser with $\alpha = 1$.

Table 2. Key agreement between different nodes

Distance between Reader and Eve	Key agreement between Reader and Tag	Key agreement between Reader and Eve reflection estimation	Key agreement between Reader and Eve product estimation
42cm $\approx 3\lambda$, W_Q=5	96.96%	81.31%	46.96%
42cm $\approx 3\lambda$, W_Q=10	100%	83.64%	51.40%
42cm $\approx 3\lambda$, W_Q=20	100%	83.96%	52.35%
56cm $\approx 4\lambda$, W_Q=5	92%	74.71%	49.41%
56cm $\approx 4\lambda$, W_Q=10	100%	81.73%	49.13%
56cm $\approx 4\lambda$, W_Q=20	100%	88.43%	49.25%
84cm $\approx 6\lambda$, W_Q=5	93.87%	75.50%	45.91%
84cm $\approx 6\lambda$, W_Q=10	100%	77.81%	47.57%
84cm $\approx 6\lambda$, W_Q=20	100%	76%	47.27%

3.2 Analysis

Table 1 shows that when the three measurement steps in a round were completed in less than channel coherence time, the correlation between RSS measurements at the legitimate parties was 0.99, giving a very high key agreement (see Table 2). The actual agreement level depends on the size of the sliding window used in quantisation process. Greater window size leads to a higher agreement level at the cost of larger memory size and more complexity in the hardware, but requires channels with only slowly changing means. For our experimental implementation, 100% key agreement was reached with a sliding window size of 10 samples.

The product estimation Eve generates by multiplying the measured RSS at steps 2 and 3 is almost constant for all of the experiments (Fig. 4, Fig. 5, and Fig. 6) with the reader and Eve fixed in position during each experiment. When Eve uses this estimate she has only around a 50% chance of deriving the legitimate key (i.e. no better than a coin toss), and the agreement level

does not change significantly with sliding window size. On the other hand, Eve's reflection estimate is in close agreement with the measurements at the reader and this results a near 80% agreement between Eve's key based on the reflection estimate and the legitimate key. This level of agreement is a serious problem which jeopardises the security of our first proposed protocol.

Problem statement: In active channel measurement scenarios where the nodes communicate symmetrically and alternately, an eavesdropper Eve located more than a half-wavelength away from the legitimate nodes could not in principle form a valid measurement of the legitimate channel (the channel between the reader and tag). However, in the passive backscatter case, Eve's estimate of the RSS gain product based on the reflected signal is strongly correlated to the reader's measurements. Our experiments show that even when Eve is 6λ away from the reader the correlation coefficient between the reader's measurements and Eve's measurements is 0.80, which leads to near 75% key agreement. Here we analyse the reflection behaviour of the tag in detail to identify the underlying problem which causes the unacceptably high key agreement for an eavesdropper situated at even relatively large ranges from tag and reader.

Referring to Section 2.2, in the first step of protocol the reader transmits a beacon at f_1, the tag shifts its received signal to f_2 and reflects it back to the reader. The reflected signal is measured by both the reader and Eve. As a result, measurements of the reflected gains at the reader and Eve are:

$$\text{Reader reflection measurement} = G_{f_1}^{RT} G_{f_2}^{TR} \tag{1}$$

$$\text{Eve reflection measurement} = G_{f_1}^{RT} G_{f_2}^{TE} \tag{2}$$

where $G_{f_1}^{RT}$, $G_{f_2}^{TR}$, and $G_{f_2}^{TE}$ are channel gains for reader to tag link at frequency f_1, tag to reader link at frequency f_2, and tag to eve link at frequency f_2, respectively. All of the gain terms in Equations (1) and (2) are positive random variables as they represent an attenuation factor. But as shown below, even when the three gain terms are statistically independent, the RSS measurements of the reflected signal by Eve and the reader are not necessarily uncorrelated.

Assume X, Y, and Z are statistically independent random variables with means μ_X, μ_Y, and μ_Z and variances σ_X^2, σ_X^2, and σ_X^2 respectively. (In our case, X and Y will represent the RSS values from tag to reader and tag to Eve, and Z the RSS from reader to tag.) Here we are interested in the correlation coefficient between products such as ZX and ZY under the assumption of statistical independence. The correlation coefficient ρ_{XY} of the processes X and Y is defined as

$$\rho_{XY} = \frac{\sigma_{XY}}{\sigma_X \sigma_Y} = \frac{E[(X - \mu_X)(Y - \mu_Y)]}{\sigma_X \sigma_Y}$$

If X and Y are independent, $\rho_{XY} = 0$, and if they are linearly dependent, $|\rho_{XY}| = 1$. Now consider the product random variables ZX and ZY. Their correlation coefficient is:

$$\rho_{ZX,ZY} = \frac{E[(Z^2XY - \mu_Z^2\mu_X\mu_Y]}{\sqrt{var(ZX)var(ZY)}}$$

Now for independent Z,X, and Y:

$$\begin{aligned} var(ZX) &= E[(ZX - \mu_{ZX})^2] = E[Z^2X^2] - \mu_{ZX}^2 \\ &= \sigma_Z^2\sigma_X^2 + \mu_Z^2\sigma_X^2 + \mu_X^2\sigma_Z^2 \\ \text{and } var(ZY) &= \sigma_Z^2\sigma_Y^2 + \mu_Z^2\sigma_Y^2 + \mu_Y^2\sigma_Z^2 \end{aligned}$$

So

$$\begin{aligned} \rho_{ZX,ZY} &= \frac{\mu_X\mu_Y(E[Z^2] - \mu_Z^2)}{\sqrt{(\sigma_Z^2\sigma_X^2 + \mu_Z^2\sigma_X^2 + \mu_X^2\sigma_Z^2)(\sigma_Z^2\sigma_Y^2 + \mu_Z^2\sigma_Y^2 + \mu_Y^2\sigma_Z^2)}} \\ &= \frac{\mu_X\mu_Y}{\sqrt{(\mu_X^2 + \sigma_X^2(1 + (\frac{\mu_X}{\sigma_Z})^2))(\mu_Y^2 + \sigma_Y^2(1 + (\frac{\mu_Y}{\sigma_Z})^2))}}. \end{aligned} \tag{3}$$

This shows that when X and Y have non-zero means and Z is not a constant ($\sigma_Z^2 \neq 0$), the correlation of the products ZX and ZY is in general non-zero, even though X, Y, and Z are statistically independent.

Returning to our passive tag scenario with RSS given in Equations (1) and (2), this result shows that because the reader and Eve reflection signals both contain the common randomly varying factor $G_{f_1}^{RT}$, their correlation is unlikely to be zero and so their derived key strings will likely have an unacceptable agreement, borne out by the experimental measurements in Tables 1 and 2.

Correlation analysis: From the experimental measurements we can derive the gains of the individual signal paths comprising the reflected signals measured by the reader and Eve. Since we have used USRPs for our experiments (rather than actual passive tags), the tag is able to measure the gain $G_{f_1}^{RT}$ at the first step of a protocol round. We can derive the RSS corresponding to $G_{f_2}^{TR}$ and $G_{f_2}^{TE}$ from the reflection signal at the reader and Eve and the RSS measurements at the tag in the first step.

$$G_{f_2}^{TR} = \frac{\text{Reader backscatter measurement}}{\text{Tag measurement at } f_1}$$

$$G_{f_2}^{TE} = \frac{\text{Eve backscatter measurement}}{\text{Tag measurement at} f_1}$$

Using this approach we are able to derive the correlation between the different links and the corresponding RSS measurements at Eve and reader for various Eve locations (see Table 3). Our results show that the channel gains of tag to Eve and tag to reader at f_2 become less correlated with greater separation. However, this does not lead to lower correlation in Eve and reader measurements, as none of them are zero-mean random variables (see Equation 3).

Table 3. Correlation coefficient between RSS measurements at different links

Distance between Reader and Eve	Correlation between RSS at $G_{f_1}^{RT}$ and $G_{f_2}^{TR}$	Correlation between RSS at $G_{f_2}^{TR}$ and $G_{f_2}^{TE}$	Correlation between Reader and Eve reflection estimation
42cm $\approx 3\lambda$	0.80	0.41	0.90
56cm $\approx 4\lambda$	0.80	0.43	0.90
70cm $\approx 5\lambda$	0.81	0.34	0.93
84cm $\approx 6\lambda$	0.77	0.24	0.80
98cm $\approx 7\lambda$	0.75	0.16	0.90

The theoretical (Eqn. 3) and experimental (Table 3) analysis in this section shows that in contrast to secret key generation using bidirectional active communications where a separation of more than half a wavelength between Eve and legitimate nodes theoretically results in uncorrelated channel measurements, the common beacon signal in the passive backscatter case causes high correlation between measurements at Eve and reader.

4 Enhanced algorithm for secret key generation

The evident agreement between the RSS of the tag reflected signal as measured by the reader and eavesdropper makes it unsuitable for generating a secret key. As discussed in the previous section, the tag reflects the beacon back to the reader and eavesdropper (with frequency translation). Although the reflected signal subsequently goes through uncorrelated channels to the reader and eavesdropper, the first channel traversed by the beacon, from reader to tag, is common to both reader and eavesdropper and causes a correlation between the reader and eavesdropper's measurements of RSS.

One approach to removing this correlation and blinding the eavesdropper to the reader–tag channel is to modify the effect of this common channel. In this section, we will discuss two algorithms to achieve this, one at the reader side and one at the tag side. We show that the enhanced algorithm at the reader side can be easily attacked by Eve. On the other hand, an enhanced algorithm at the tag side can remove the common random factor ($G_{f_1}^{RT}$) from the reflection signal and result in nearly uncorrelated RSS measurements at the reader and eavesdropper.

4.1 Reader–side enhanced algorithm

One capability an enhanced reader might use is to modify the key generation process by controlling the power level of the beacon signals used in different steps of the key–generation protocol. Note that Eve's best estimate of the secret key is based on her measurement at the first step of the protocol. Beacons sent by the reader at step 2 and 3 are used by the tag for key generation but Eve's estimation

based on her calculation of their product is uncorrelated to the tag's and reader's measurements. Hence the reader can best prevent Eve from measuring the actual channel gains by interfering with her estimate made in step 1 of the protocol.

In the reader–side enhanced algorithm, the reader sends out the beacon in step 1 at a random power level to falsify Eve's estimate of the reflected RSS. Since the random power level is chosen by reader itself, it can easily extract the true channel gain from the reflection signal RSS. On the other hand, this does not affect the step 2 and 3 RSS measurements at the tag and the high correlation between measurements at the reader and tag can be expected to remain unchanged. Table 4 shows the key agreement between the reader and tag, and Eve when the beacon power is randomised in this way at the reader side.

Table 4. Key agreement between different nodes for reader–side enhanced algorithm

Distance between Reader and Eve	Key agreement between Reader and Tag	Key agreement between Reader and Eve reflection estimation	Key agreement between Reader and Eve product estimation
42cm $\approx 3\lambda$, W_Q=5	96.96%	47.47%	46.96%
42cm $\approx 3\lambda$, W_Q=10	100%	48.59%	51.40%
42cm $\approx 3\lambda$, W_Q=20	100%	46.22%	52.35%
56cm $\approx 4\lambda$, W_Q=5	92%	52.87%	49.41%
56cm $\approx 4\lambda$, W_Q=10	100%	46.52%	49.13%
56cm $\approx 4\lambda$, W_Q=20	100%	57.08%	49.25%
84cm $\approx 6\lambda$, W_Q=5	93.87%	50.51%	45.91%
84cm $\approx 6\lambda$, W_Q=10	100%	42.23%	47.57%
84cm $\approx 6\lambda$, W_Q=20	100%	46.93%	47.27%

Potential attack: The reader transmits the beacon signal at f_1 with a random sequence of amplitudes, say α_0, α_1, α_2,... If the reader and Eve are both stationary so that $G_{f_1}^{RE}$ is constant for a time, Eve will receive these beacon signals with amplitudes $s_0 = \alpha_0 G_{f_1}^{RE}$, $s_1 = \alpha_1 G_{f_1}^{RE}$, $s_2 = \alpha_2 G_{f_1}^{RE}$ and so on. If she takes ratios of the signals, eg $\frac{s_1}{s_0} = \frac{\alpha_1}{\alpha_0}$, $\frac{s_2}{s_0} = \frac{\alpha_2}{\alpha_0}$ ... she can estimate the α_i to within a scale factor (α_0 in this case). This estimate would then allow her to correct her reflected estimation of $\alpha_i G_{f_1}^{RT} G_{f_2}^{TE}$ signal and find $G_{f_1}^{RT} G_{f_2}^{TE}$ to within a constant

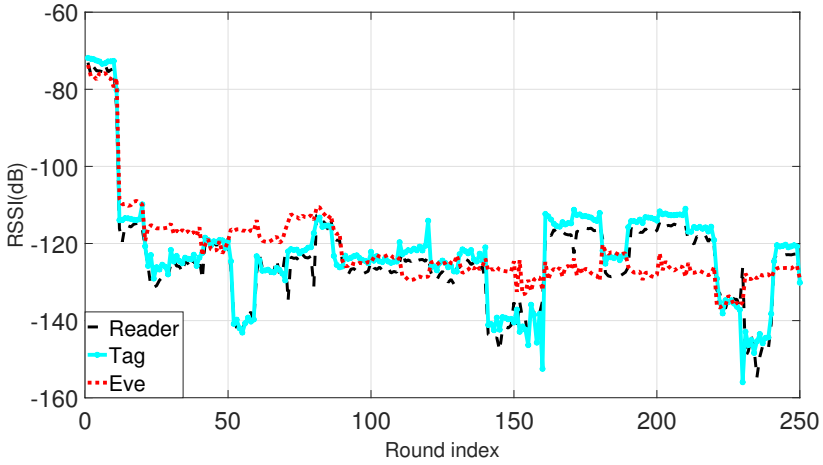

Fig. 7. RSS for tag–side enhanced algorithm, reader and Eve are 42cm $\approx 3\lambda$ apart.

scale factor, which does not affect key bit quantisation, and so she can discover the key bits.

4.2 Tag–side enhanced algorithm:

In this section, we propose an algorithm at the tag side instead to eliminate the effect of the common reader–to–tag channel. We assume an ideal tag which can accurately control the strength of its reflection signal. However a passive tag is not able to amplify the received beacon but only reduce the amplitude of its reflection. As explained in [4], the tag is in principle able to change its reflection characteristics by altering the impedance load on its antenna and so control the power level of the reflection signal. The power level of the reflection signal can stated in the form:

$$P_{Reflection} = P_{Beacon} \frac{| \Gamma_1^* - \Gamma_2^* |^2}{4} \tag{4}$$

where Γ_1^* and Γ_2^* are the complex conjugates of the reflection coefficients corresponding to the two impedance states. The backscattered signal can be reflected at different power levels corresponding to the range $[0, P_{Beacon}]$. If the tag can keep the reflected power at some constant level in step 2 of successive rounds of the key generation process, the damaging effects of the common random factor ($G_{f_1}^{RT}$) can be eliminated. The reader and eavesdropper now see just the single channel gains $G_{f_2}^{TR}$ and $G_{f_2}^{TE}$ respectively, and these channel gains are uncorrelated given our assumptions.

To implement the tag–side power management algorithm, we need to swap the order of step 1 and step 2 in each protocol round so that the tag can estimate the reader-tag channel gain as a first step. So in the new sequence, the tag is in the

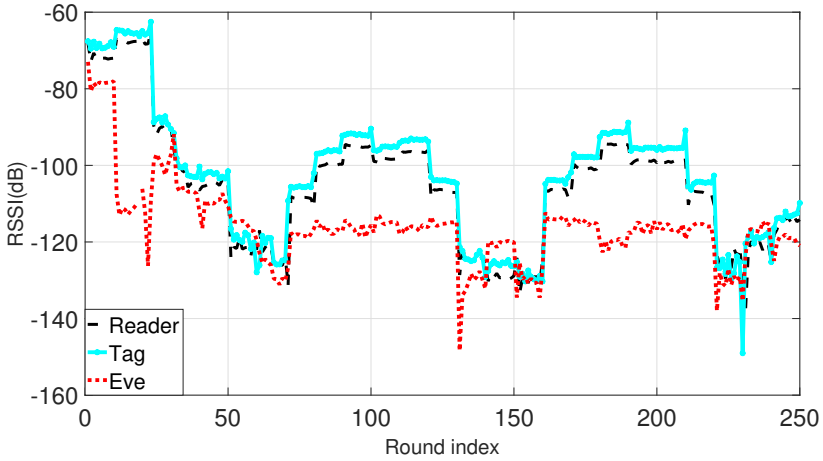

Fig. 8. RSS for tag–side enhanced algorithm, reader and Eve are 56cm $\approx 4\lambda$ apart.

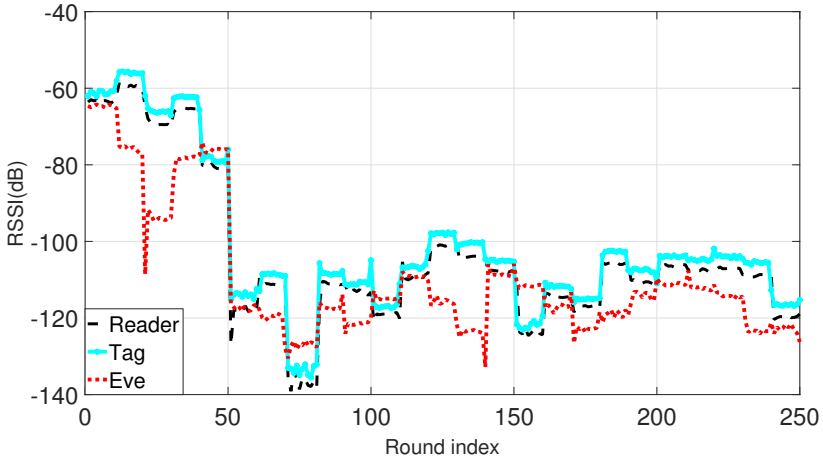

Fig. 9. RSS for tag–side enhanced algorithm, reader and Eve are 84cm $\approx 6\lambda$ apart.

listening mode in step 1 and measures $G_{f_1}^{RT}$. In step 2 the tag is in the reflection mode and controls the reflected power to remove the effects of $G_{f_1}^{RT}$ from the reflection signals $G_{f_1}^{RT}G_{f_2}^{TR}$ and$G_{f_1}^{RT}G_{f_2}^{TE}$ seen by the reader and eavesdropper respectively.

For a simple proof-of-concept demonstration of the approach, we consider time epochs in which the tag adjusts its reflection according to the factor $k(i)$ (with i the protocol round index within an epoch):

Table 5. Key agreement between different nodes for tag–side enhanced algorithm

Distance between Reader and Eve	Key agreement between Reader and Tag	Key agreement between Reader and Eve
42cm $\approx 3\lambda$, W_Q=5	82%	51.28%
42cm $\approx 3\lambda$, W_Q=10	89%	50%
42cm $\approx 3\lambda$, W_Q=20	97%	51%
56cm $\approx 4\lambda$, W_Q=5	83.33%	51.19%
56cm $\approx 4\lambda$, W_Q=10	94.11%	55.39%
56cm $\approx 4\lambda$, W_Q=20	98.34%	60%
84cm $\approx 6\lambda$, W_Q=5	86%	54%
84cm $\approx 6\lambda$, W_Q=10	100%	55.51%
84cm $\approx 6\lambda$, W_Q=20	100%	59.48%

$$k(i) = \begin{cases} 1 & i = 1, \\ \frac{min(G_{f_1}^{RT}(1),\ldots,G_{f_1}^{RT}(i))}{G_{f_1}^{RT}(i)} & i > 1, \end{cases} \tag{5}$$

where $G_{f_1}^{RT}(i)$ is the RSS at f_1 in round i. Eve's and the reader's reflection measurements in round i are then:

$$\text{Reader reflection measurement} = k(i)G_{f_1}^{RT}(i)G_{f_2}^{TR}(i)$$

$$\text{Eve reflection measurement} = k(i)G_{f_1}^{RT}(i)G_{f_2}^{TE}(i)$$

In step 3 of a protocol round, the reader sends a beacon at f_2 to the tag (which operates in the listening mode) and the tag measures $G_{f_2}^{RT}$. In the enhanced tag–side key generation algorithm, the reader and Eve generate a key based on their measurements at step 2, while the tag multiplies its measurements at step 1 and 3 to compute its product term (from which its key is derived) as:

$$\text{Tag product measurement} = k(i)G_{f_1}^{RT}(i)G_{f_2}^{RT}(i)$$

The effect of the factor $k(i)$ is to reduce the variability of the reader–tag channel at f_1 to a piecewise constant since $k(i)G_{f_1}^{RT}(i) = \min(G_{f_1}^{RT}(1), \ldots, G_{f_1}^{RT}(i))$. Even though in the ideal case the effect of the common reader–tag channel at f_1 has been largely removed and so does not contribute to key generation, the

remaining component at f_2, i.e. $G_{f_2}^{RT}(i)$ is sufficient for random key generation under our system assumptions (as in symmetric non-backscatter systems).

In order to emulate an ideal tag, we have applied the tag–side enhanced algorithm to the channel gain measurements made in the experiments described in Section 3 above. The results are shown in Figs. 7 to 9 and Table 5 and demonstrate that the correlation effects due to the common reader–tag channel have been considerably reduced, with key agreement rates between Eve and the legitimate parties now approaching the desired 50% levels. An investigation of improved forms for the factor $k(i)$ in Equation (5) is left for future work.

5 Conclusion

In this paper, we proposed a novel algorithm for generating shared secret keys in passive backscatter communications systems by measuring wireless channel characteristics at dual frequencies. Restricted capabilities and severe power limitations are typical of passive backscatter sensors and make shared secret key generation based on reciprocal channel characteristics an attractive approach. Previous work on physical–layer secret key generation has focused on the symmetric case where both parties use comparable active transceivers to exploit the symmetric channel characteristics at a single frequency. However, passive backscatter systems operate at dual frequencies, and are asymmetric, with only the reader device being able to transmit arbitrary signals.

A simple RSS–based key generation approach modified for dual frequency operation has been implemented on USRP software–defined radios acting as an emulation of the reader–tag backscatter system and shows good key agreement between the legitimate parties. However the reflection signal from the passive backscatter tag contains a beacon component common to both the tag and an eavesdropper and this compromises the secrecy of the shared key. To overcome the effect of the common beacon component we have described an enhanced algorithm based on giving the tag the additional capability of being able to control its reflected power. The enhanced algorithm was demonstrated using USRP emulation and showed significant improvement in restricting an eavesdropper's ability to derive the secret key by intercepting the communications of the legitimate parties.

6 Acknowledgements

The authors would like to thank Prof. Sherman Chow and the anonymous reviewers, whose valuable suggestions greatly improved the manuscript. We also would like to express our very great appreciation to Ms Samira Saadatpour for her valuable technical assistance in experimental implementations.

References

1. B. Kellogg, A. Parks, S. Gollakota, J. R. Smith, and D. Wetherall, "Wi-fi backscatter: internet connectivity for rf-powered devices," *ACM SIGCOMM Computer Communication Review*, vol. 44, no. 4, pp. 607–618, 2015.

2. J. F. Ensworth and M. S. Reynolds, "Every smart phone is a backscatter reader: Modulated backscatter compatibility with bluetooth 4.0 low energy (ble) devices," in *2015 IEEE International Conference on RFID (RFID)*. IEEE, 2015, pp. 78–85.
3. D. Bharadia, K. R. Joshi, M. Kotaru, and S. Katti, "Backfi: High throughput wifi backscatter," *ACM SIGCOMM Computer Communication Review*, vol. 45, no. 4, pp. 283–296, 2015.
4. B. Kellogg, V. Talla, S. Gollakota, and J. R. Smith, "Passive wi-fi: bringing low power to wi-fi transmissions," in *13th USENIX Symposium on Networked Systems Design and Implementation (NSDI 16)*, 2016, pp. 151–164.
5. V. Iyer, V. Talla, B. Kellogg, S. Gollakota, and J. Smith, "Inter-technology backscatter: Towards internet connectivity for implanted devices," in *Proceedings of the 2016 conference on ACM SIGCOMM 2016 Conference*. ACM, 2016, pp. 356–369.
6. P. Zhang, D. Bharadia, K. R. Joshi, and S. Katti, "Hitchhike: Practical backscatter using commodity wifi." in *SenSys*, 2016, pp. 259–271.
7. T. Wang, Y. Liu, and A. V. Vasilakos, "Survey on channel reciprocity based key establishment techniques for wireless systems," *Wireless Networks*, vol. 21, no. 6, pp. 1835–1846, 2015.
8. Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proceedings of the IEEE*, vol. 104, no. 9, pp. 1727–1765, 2016.
9. S. N. Premnath, S. Jana, J. Croft, P. L. Gowda, M. Clark, S. K. Kasera, N. Patwari, and S. V. Krishnamurthy, "Secret key extraction from wireless signal strength in real environments," *IEEE Transactions on mobile Computing*, vol. 12, no. 5, pp. 917–930, 2013.
10. S. Jana, S. N. Premnath, M. Clark, S. K. Kasera, N. Patwari, and S. V. Krishnamurthy, "On the effectiveness of secret key extraction from wireless signal strength in real environments," in *Proceedings of the 15th annual international conference on Mobile computing and networking*. ACM, 2009, pp. 321–332.
11. N. Patwari, J. Croft, S. Jana, and S. K. Kasera, "High-rate uncorrelated bit extraction for shared secret key generation from channel measurements," *IEEE Transactions on Mobile Computing*, vol. 9, no. 1, pp. 17–30, 2010.
12. S. T. Ali, V. Sivaraman, and D. Ostry, "Eliminating reconciliation cost in secret key generation for body-worn health monitoring devices," *IEEE Transactions on Mobile Computing*, vol. 13, no. 12, pp. 2763–2776, 2014.
13. M. H. Chinaei, V. Sivaraman, and D. Ostry, "An experimental study of secret key generation for passive wi-fi wearable devices," in *A World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2017 IEEE 18th International Symposium on*. IEEE, 2017, pp. 1–9.
14. S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-telepathy: extracting a secret key from an unauthenticated wireless channel," in *Proceedings of the 14th ACM international conference on Mobile computing and networking*. ACM, 2008, pp. 128–139.