In-Band Ambient FSK Backscatter Communications Leveraging LTE Cell-Specific Reference Signals

Jingyi Liao, Xiyu Wang, *Graduate Student Member, IEEE*, Kalle Ruttik, *Member, IEEE*, Riku Jäntti, *Senior Member, IEEE*, and Dinh-Thuy Phan-Huy

***Abstract*—A long term evolution (LTE) signal is ubiquitously present, which make it an attractive signal source for ambient backscatter communications (AmBC). In this paper, we propose a system that uses LTE cell-specific reference signals (CRSs) transmitted by a base station as an ambient source and channel estimator at the user equipment (UE) as an AmBC receiver. One of the challenges in AmBC is direct path interference (DPI): The direct signal from the transmitter to the receiver is several orders of magnitude stronger than the scattered path. We propose a solution that operates withing the original LTE band. In order to mitigate the DPI, the backscatter device (BD) performs a frequency shift keying (FSK) modulation that introduces an artificial Doppler shift to the channel which is larger than the natural Doppler but still small enough such that it can be tracked by the channel estimator at the UE. We demonstrate the feasibility of the proposed system by Proof-of-Concept implementation and compare its performance against the simulation results. Measurement results show that we could achieve bit error probabilities less than 10^{-2} with ambient LTE signal having SNR of 5 dB operating on 486 MHz band having 7.68 MHz bandwidth.**

***Index Terms*—Ambient backscatter communications, LTE cell-specific reference signals, channel estimation.**

I. Introduction

THE INTRODUCTION of ambient backscatter communications (AmBC) [1] in mobile networks [2] has recently been proposed for the sustainable development of asset-tracking services [3], and to overcome the limitations of solutions based on radio frequency identification (RFID). In RFID-based asset tracking, an energy-autonomous and passive RFID tag is illuminated by an RFID reader, with a radio frequency (RF) carrier-wave [4]. The communication range is limited by the reader transmit power [5]. The communication range can be compensated by increasing the number of readers of portals, but a massive deployment of such devices is not sustainable. In comparison, AmBC systems [1] usually involve three communication nodes instead of only two: an ambient source of RF signals, a backscatter device (BD), and an AmBC receiver device. The BD is similar to a tag. The AmBC receiver reads the BD's message, without having to generate any RF carrier wave, as the BD directly uses the ambient source. Therefore, AmBC provides higher spectrum efficiency and greater communication range when strategically placing the three communication nodes.

In an AmBC system, a BD can be implemented with an antenna connected to various matching impedance, through an RF switch driven by a micro-controller. According to the message to be transmitted, the BD switches between impedance to alter and reflect the impinging ambient signal. The AmBC receiver receives a composite signal. One is the direct path signal transmitted from the ambient source and another is backscattered by the BD that contains the target message. However, the direct path signal from the transmitter to the receiver has several orders of magnitude larger power than the BD-modulated scattered path signal. This results in direct path interference (DPI) to the AmBC receiver. In addition, the fast phase and amplitude variations of the ambient source signal are unknown to the receiver. These two factors drastically lower the signal-to-noise ratio (SNR) of the BD signal which hampers the AmBC receiver performance.

Among different ambient sources, Long Term Evolution (LTE) signals are ubiquitous and their controlling signals are easily available to its UEs. Specifically, an LTE base station (BS), a.k.a. eNodeB, periodically sends a primary synchronization sequence (PSS) and secondary synchronization sequence (SSS), allowing the UE receiver to become synchronized to the transmitter. Then, the UE performs a cell search to determine which cell to connect to. In addition to the synchronization signals, the eNodeB transmits cell-specific reference signals (CRS) that the UE utilizes for estimating the downlink channel. In LTE, these signals are broadcast even if the cell is idle, meaning that no downlink traffic is being scheduled. Furthermore, using these signals at the receiver does not require it to be registered with the BS. These facts highly motivate us to consider the LTE downlink signal as the ambient signal in this paper. Therefore, AmBC systems make use of these repetitive signals that the BSs broadcast. The AmBC receiver does not have to do any signaling with the eNodeB. The UE channel-estimator output can be used for demodulating the messages transmitted from the BD.

Manuscript received 28 January 2023; revised 7 April 2023; accepted 15 May 2023. Date of publication 25 May 2023; date of current version 19 July 2023. This work was supported in part by the European Project Hexa-X under Grant 101015956, and in part by the Business Finland Project eMTC under Grant 8028/31/2022. *(Corresponding author: Jingyi Liao.)*

Jingyi Liao, Xiyu Wang, Kalle Ruttik, and Riku Jäntti are with the Department of Information and Communications Engineering, Aalto University, 02150 Espoo, Finland (e-mail: Jingyi.Liao@aalto.fi; Xiyu.Wang@aalto.fi; Kalle.Ruttik@aalto.fi; riku.jantti@aalto.fi).

Dinh-Thuy Phan-Huy is with the Networks, Orange Innovation, 92326 Châtillon, France (e-mail: dinhthuy.phanhuy@orange.com).

Digital Object Identifier 10.1109/JRFID.2023.3280108

In the previous work, we used the on-off keying (OOK) modulation in AmBC [6]. Unfortunately, a simple OOK signal occupies frequencies, where Doppler components from all the channel paths are also present, making it difficult to separate the backscatter path from the DPI [7]. In addition, the symbol duration (i.e., switching period) used by the BD tends to be long compared to the channel coherence time, making the BD signal vulnerable to fast fading. To address these problems, this paper proposes a frequency shifting approach to separate the direct and scattered channels, but rather than moving the whole scattered signal on an adjacent band, we shift only the scattered signal channel tap away from the natural Doppler. Hence, the backscatter signal will not contaminate communications on other bands. On the other hand, the backscatter communication frequency usually is less than 1 kHz, which is slow enough for the receiver channel equalizer to track the additional channel variations caused by the BD [8]. Channel does not change in one LTE subframe (1 ms), which guarantees that the UE estimates a stable channel based on CRS.

Contributions: In this paper, we propose to use frequency shift keying (FSK) type modulation in an AmBC system using LTE downlink signals as the ambient source. For the FSK backscatter signal, the backscattered path is separated from the direct path in the frequency domain, so that the DPI can be cancelled. The BD introduced artificial frequency shift, which we refer to as the *frequency key*, is selected to be higher than Doppler effect, and to be lower than channel-estimation tracking speed. Also, the fact that CRS signals are presented only at certain orthogonal frequency division multiplex (OFDM) symbols, limited the frequency key selection. Moreover, FSK allows for noncoherent reception that does not depend on the channel parameters. The contributions are listed as follows.

- The BD signal is generated by the same OOK modulator as in [6], but the generated waveform is selected to approximate FSK. We also discuss square-wave FSK that uses rectangular pulses instead of sinusoidal signals. We investigate the impact of non-uniform CRS sampling frequency. The FSK frequency keys are carefully selected to cooperate with a non-uniform LTE CRS sampling.
- The AmBC receiver directly utilizes the channel estimates obtained from the LTE CRS pilot signal, instead of the full channel state information. Two types of receivers, coherent and noncoherent methods, are proposed. The simulation proves that the coherent method outperforms energy detector.
- Finally, the proposed system is validated by a proof-of-concept implementation and corresponding measurements. This implementation validates that the proposed receiver's process can be applied to any receivers as long as they can be synchronized to the LTE eNodeB.

The paper is structured as follows: Section I introduces AmBC, as well as the motivation and contribution of this work. Section II reviews the relevant prior art; Section III describes the components of the proposed system; Section IV outlines how the UE channel estimator can be used as an AmBC receiver; Section V simulates this AmBC system performance and designs a measurement to validate it; and finally, a conclusion is draw in Section VII.

II. Prior Art

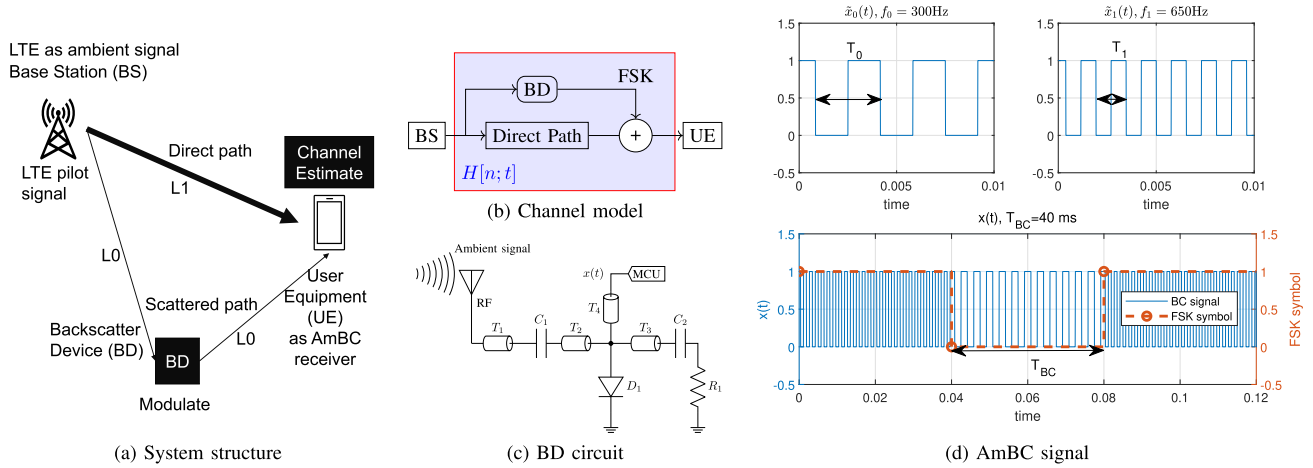
A. Ambient Backscatter Communications

Improving the AmBC receiver performance, several methods to mitigate DPI have been proposed in the literature including spatial methods [9], [10], polarization-based methods [11], [12], and frequency-shifting-based methods [9], [13]. Spatial methods require the receiver to be equipped with multiple antennas while the polarization methods require special receiver antennas to be used [2]. Frequency-shifting techniques seek to separate the direct path and scattered path signals on different bands which increases the spectrum occupancy of the BD signals. Ambient signal is shifted from one channel to neighbour channel. Then the codeword of ambient Wi-Fi signal is phase shifted [14], which requires an idle adjacent non-overlapping Wi-Fi channel in advance.

Another challenge of rapidly varying and unknown ambient source signal is mitigated by using long symbols at the BD and average over the ambient source signal variations at the energy detector [1]. While this worked well in the case of TV broadcast transmissions that are almost continuous, the approach does not lead to good performance in the case of cellular-generated signals that vary drastically in time, based on the scheduled traffic [3], [15], [16]. In order to improve AmBC performance in a cellular setting, our recent paper [6] proposed to use knowledge about the pilots of the ambient source at the AmBC receiver side. Previously, a similar approach has been utilized in the context of the Wi-Fi standard [17]. Unfortunately, Wi-Fi pilot transmission is sporadic and thus is sub-optimal for reading BD signals.

Unlike a bursty WiFi signal [17], an LTE signal is continuous and ubiquitous signal, which is a potential candidate for the ambient signal [6], [18]. Some signals in LTE always exist and broadcast in all subframes and cells such as PSS and SSS, CRS and physical broadcast channel (PBCH) [19]. In [18], the BD phase first synchronizes with the LTE PSS and then performs a frequency-shifting operation with frequency greater than the LTE bandwidth to solve the DPI problem. Synchronization to PSS is utilized in order to remove the natural phase offset of the physical layer which allows the receiver to track the artificial phase shift caused by the BD. The receiver eliminates phase offset based on LTE PSS and SSS, then demodulates the BD phase modulation.

The method proposed in this paper differs from the above works in two ways. Firstly, the method preforms a much smaller frequency shift such that the backscattered signal remains in the LTE band. Secondly, the method uses the UE channel estimator as a receiver and does not require the BD to be synchronized to the LTE base station. The utilized frequency shift adds an artificial Doppler to the scattered path that can then be utilized at the channel estimator to separate the direct and scattered path from each other. The method proposed in this paper leads to higher spectral efficiency and



(a) System structure (b) Channel model (c) BD circuit (d) AmBC signal

Fig. 1. (a) High-level structure of the proposed system. (b) Backscatter device causes the channel to vary. (c) Circuit diagram of the BD where T_1, T_2, T_3, T_4 are transmission lines, C_1, C_2 are capacity, D_1 is a diode, and R_1 is load. (d) Periodic rectangular wave of FSK 0 and FSK 1. Signal and FSK symbol relationship of backscatter.

simpler BD and receiver structures, but supports much lower data rates.

B. Applications

In [3], it is proposed to use a cellular BS as an ambient source, and to use a UE as an AmBC receiver, to develop a service for asset tracking with ubiquitous coverage. It is almost "free", i.e., without generating additional waves, without additional energy, and without deploying massively new equipment such as portals. An energy-autonomous BD harvesting solar energy, called crowd-detectable zero-energy-devices (CD-ZEDs) are put on the asset to be tracked. Each time the BD (or CD-ZED) enters the close proximity of a UE (connected to the cellular network and geo-localised), the BD is detected by the UE and this contact event is reported to the network. Thanks to the anonymous participation of the crowd of UEs, the localisation of the BD is tracked over the cellular network coverage area. Such a CD-ZED concept is one example of the more general category of energy-autonomous devices called zero-energy devices (ZEDs) [20]. Such an asset-tracking service is one example of ambient Internet of Things (AIoT) applications that is currently being discussed in the standardisation of cellular networks [21]. Finally, ZED is one of the key technologies identified for the building in future of a sustainable 6G [22].

The CD-ZED concept is applicable to all generations of mobile networks. AmBC in 5G networks has been studied in [2] where it was shown that a BD can be detected by a UE as long as the UE is within the BS coverage and the tag is close to the UE. This is confirmed by successful experiments of ambient backscattering communications conducted with ambient signals from commercial 4th generation (4G) and 5th generation (5G) networks in [3], in very few test locations, far from the BS. The previous works [15], [16] used power-detector-based receivers that have limited performance due to the high variability of the mobile downlink signals. Very recently, to improve 4G AmBC performance, [6] proposed to use knowledge about the pilots of the ambient source (i.e., the BS) at the AmBC receiver (i.e., UE) side. This is expected

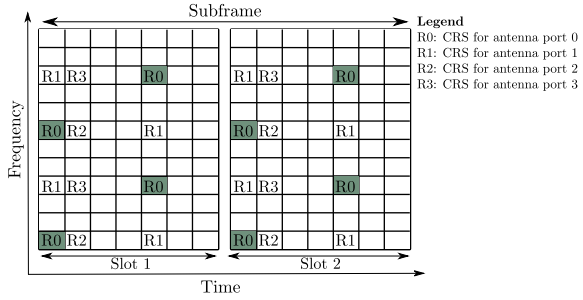


Fig. 2. LTE Release 8 cell-specific reference signal for antenna ports 0, 1, 2, and 3.

to improve the AmBC receiver performance as the ambient pilots are known and the channels can be estimated at the receiver.

III. System Description

Let us consider a bi-static AmBC system, as shown in Fig. 1(a), in which a BD is illuminated with the LTE downlink signal and a UE is used as a receiver. All three system nodes are equipped with a single antenna. We first describe the LTE signal and the downlink channel estimation in an LTE system in Section III-A. Then, we discuss the BD modulator in detail in Section III-B and the use of a channel estimator as a receiver in Section IV.

A. Ambient LTE Signal

LTE uses OFDM for the downlink transmission from the BS (also known as the eNodeB) to the UE. OFDM is a multi-carrier modulation system where data is transmitted as a combination of orthogonal narrowband signals known as subcarriers. In LTE, the subcarrier spacing is 15 kHz and the number of carriers utilized depends on the channel bandwidth that can vary between 1.4 MHz up to 20 MHz. The OFDM symbols are grouped into resource blocks that consists of 12 subcarriers having 180 kHz bandwidth and of 7 consecutive symbols having a total duration of 0.5 ms. In the LTE system, the BS transmits CRS in every slot having length $T_{slot} = 0.5$ ms. Fig. 2 illustrates the CRS allocation

for antenna ports 0 to 3 when the system is using a normal cyclic prefix. LTE networks may operate using different CRS configurations. In a non-shifted CRS configuration, all cells use the same CRS time and frequency resources. In a shifted CRS configuration, different cells transmit CRSs on resources that are shifted in frequency. The non-shifted configuration avoids the interference of CRSs on data transmissions, but is also associated with a systematic CSI estimation error; especially noticeable at low traffic. Using the shifted configuration, the CRSs interfere with data transmissions, but the CSI estimation error is smaller [23]. In this paper, we consider the case of shifted CRS, and the AmBC receiver uses pilots transmitted from antenna port 0.

In the frequency domain, the received signal for the symbols $t \in \{0, T_{slot}/2 + \Delta T, T_{slot}, 3/2T_{slot} + \Delta T, \ldots\}$ containing the CRS for the given antenna port can be written as

$$S_r[n; t] = H[n; t]S_t[n; t] + Z[n; t],$$

where n is the subcarrier number containing the CRS at time t and $Z[n, t]$ denotes the receiver noise. In Fig. 2, n represent row and t represent column. The frequency response of the channel is given by $H[n; t]$. The CRS reference symbol $S_t[n]$ is already known by the receiver and thus it can obtain a frequency-domain channel estimate

$$\hat{H}[n; t] = \frac{S_r[n; t]}{S_t[n; t]}. \tag{1}$$

The UE samples the channel at 4 kHz rate, but the sampling intervals are irregular. This sampling rate limits the Doppler frequencies the UE channel estimator and equalizer can handle.

From the channel estimation point of view, the BD is an additional multi-path component as illustrated by Fig. 1(b). In this paper we propose that the BD uses FSK to separate the direct path from the BD modulated scattered path in the frequency domain. Hence, the UE channel estimator sees the BD as an additional multipath component with time-varying Doppler frequency which is higher than the natural Doppler frequency in the direct path.

B. Back Scattered Signal

The BD performs load modulation on the incident signal illuminating its antenna, as shown in Fig. 1(c). That is, it varies its complex antenna load impedance between two states Z_0 and Z_1. The BD reflection coefficient is given by

$$\Gamma_L = \frac{Z_L - Z_a}{Z_L + Z_a},$$

where Z_L denotes the load impedance in state $L \in \{0, 1\}$ and Z_a is the antenna impedance [24]. In the OOK case, we would in an ideal case have $Z_1 = 0$ or $Z_0 = Z_a$ resulting in that all signals are scattered back or nothing at all. In a practical implementation, the load impedance is switched by a diode in a control circuit [25]. In Fig. 1(c), a micro controller unit (MCU) controls that diode switch D1, whether a load antenna with impedance ($\Gamma_0 = 0$) or a short circuit antenna ($\Gamma_1 = -1$).

The commonly-used OOK modulation maps the two reflection coefficients to the information bits 0 and 1. Let $x(t) \in \{\Gamma_0, \Gamma_1\}$ be the backscatter symbol, the impulse response of the channel from the BS to the UE is

$$h[\tau; t] = x(t) \sum_{\ell \in \mathcal{L}_0} a_\ell[t]\delta[\tau - \tau_\ell(t)] + \sum_{\ell \in \mathcal{L}_1} a_\ell[t]\delta[\tau - \tau_\ell(t)], \tag{2}$$

where $a_\ell(t)$, $\tau_\ell(t)$ are the time-varying amplitude and delay of the ℓ^{th} multipath component and $\delta(\tau)$ denotes the Dirac delta function. The bandwidth of the channel tap gain $a_\ell(t)$ is defined by the Doppler f_D frequency shift in the channel. In Fig 1(a), the direct path components $\mathcal{L}_1$ from an LTE eNodeB to the UE is indicated by the thick arrow. The thin arrow from the BS to the UE via BD represents $\mathcal{L}_0$ BD-modulated scattered components. We cannot observe this channel directly, but instead we can obtain frequency domain samples of it based on the CRS signal transmitted by the base station.

Specifically, when the BD applies the OOK modulation, as in the previous work [6], the impulse response of channel $h[\tau; t]$ are different when BD is in on ($x(t) = 1$) or off ($x(t) = 0$) status in Eq. (2). For OOK, the ambient signal and Doppler effect strongly influence the channel estimation making it difficult for the receiver to distinguish between $h_{\text{on}}[\tau; t]$ and $h_{\text{off}}[\tau; t]$.

$$h_{\text{on}}[\tau; t] = \sum_{\ell \in \mathcal{L}_0} a_\ell[t]\delta[\tau - \tau_\ell(t)] + \sum_{\ell \in \mathcal{L}_1} a_\ell[t]\delta[\tau - \tau_\ell(t)]$$

$$h_{\text{off}}[\tau; t] = \sum_{\ell \in \mathcal{L}_0} a_\ell[t]\delta[\tau - \tau_\ell(t)]$$

In [6], the BD added known pilot symbols to its message in order to set a decision threshold for the OOK demodulator. This caused large overhead.

Alternatively, the BD modulator can switch between two load impedance in frequency $f_k, k \in \{0, 1\}$, to represent information 0 and 1, which is referred to as FSK modulation. FSK shifts the frequency of the scattered signal away from the direct path signal to avoid the DPI. Therefore, in this paper, we consider that the BD applies FSK modulation. In an FSK case we can implement a noncoherent receiver that is robust against a natural Doppler and avoids the need for pilot transmission.

The BD aims at causing an artificial Doppler that is higher than the natural Doppler in the channel such that the receiver would be able to distinguish between the direct path components (multipath components in $\mathcal{L}_1$) and BD-modulated scattered components (multipath component in $\mathcal{L}_0$). The BD does this by generating a periodic rectangular wave $\tilde{x}_k(t) = \tilde{x}_k(t + T_k)$:

$$\tilde{x}_k(t) = \sum_{n=-\infty}^{\infty} \text{rect}\left[\frac{2(t - nT_k)}{T_k}\right], \quad k = 0, 1$$

where rect(t) is the unit rectangular pulse and the index k indicates whether bit 0 or 1 was transmitted. $\tilde{x}_0(t)$ and $\tilde{x}_1(t)$ are sparse-square or tight-square waves with infinite extension, as two above subplots of Fig. 1(d). However, the BD symbol

duration is T_{BC}, which is the red dash line in the lower subplot of Fig. 1(d). Hence the generated BD pulse is

$$x_k(t) = \text{rect}\left(\frac{t}{T_{BC}}\right)\tilde{x}_k(t). \quad k = 0, 1$$

In the time domain, $x_0(t)$ or $x_1(t)$ look like blue-line segments in the below subplot of Fig. 1(d). The Fourier transform of the BD symbol is given by

$$X_k(f) = \frac{T_{BC}}{2}\sum_{l=-\infty}^{\infty}\text{sinc}\left(\frac{1}{2}l\right)\text{sinc}\left[\left(f - \frac{l}{T_k}\right)T_{BC}\right],$$

where $\text{sinc}(x) = \sin(\pi x)/(\pi x)$. The harmonics of the rectangular wave nominal frequency $l\frac{1}{T_k}$, $l = 3, 5, \ldots$ attenuate slowly implying that the square wave has a wide bandwidth.

It is worth noting that the BD switching frequency is lower than 1 kHz, that is, the duration of one state of the BD reflection coefficient is the same or longer than the duration of one LTE subframe. In this scenario, during one LTE subframe, the BD signal adds an additional multipath component to the UE. The effect of this multipath component is included in the channel estimate as shown in Eq. (1).

IV. Using LTE Channel Estimator as Receiver for the Backscattered Signal

In this section, we describe how the UE channel estimator can be utilized as a receiver for the BD-modualted signal. We start by describing the impact of the BD on the channel and how that channel is seen by the UE after sampling. We then proceed describing how a receiver could be constructed using the obtained channel estimates.

A. Channel Sampling Using CRS

From the transmitted CRS, we obtain frequency-domain channel estimates $\hat{H}[n; t]$ for the time instants $t \in \{0, T_{slot}/2 + \Delta T, T_{slot}, 3/2T_{slot} + \Delta T, \ldots\}$ during which the pilots were sent. This is done by applying equation (1).

Assuming that the channel stays approximately constant during the transmission of a single OFDM symbol, the inverse Fast Fourier Transform of $H[n; t]$ at the time instants t yields the following channel taps

$$\hat{h}[l; t] = x(t)\sum_{\ell\in\mathcal{L}_0} a_\ell^b(t)\text{sinc}(l - \tau_\ell(t)W) + \sum_{\ell\in\mathcal{L}_1} a_\ell^b(t)\text{sinc}(l - \tau_\ell(t)W) + z_l(t),$$

where $W = \frac{1}{T_s}$ denotes the utilized bandwidth, $a_\ell^b(t) = e^{-i2\pi f_c\tau_\ell(t)}a_\ell(t)$ denotes the baseband equivalent channel tap of the ℓ^{th} multi-path component, f_c is the carrier frequency, and $z_l(t)$ denotes the estimation noise, the AmBC signal $x(t)$ could be $x_0(t)$ or $x_1(t)$. The LTE system is synchronized to the shortest path which appears in the first channel tap. The backscattered signal component is likely to be much smaller than the direct path component leading to very small SNR. As a consequence, the distance between the BD and the receiver is short in most practical deployments and thus most of the BD scattered power would be in the first channel tap. Hence, in the receiver it is sufficient to merely find

$$\hat{h}[0; t] = x(t)h_0(t) + h_1(t),$$

where $h_0(t)$ and $h_1(t)$ contain the scattered and direct-path components that appear in the first channel tap after sampling.

Let $T_{slot} = 0.5$ ms denote the slot length and let $\Delta T = 4T_s - \frac{T_{slot}}{2} = 35.6\ \mu$s denote the offset of the second channel sampling instant compared to a regular sampling interval $T_r = T_{slot}/2$ that would correspond to a 4-kHz sampling rate.

Let $s(t) = \delta(t)+\delta(t-T_{slot}/2-\Delta T)$ be the periodic sampling signal $s(t + T_{slot}) = s(t)$ where T_{slot} denotes the slot length and ΔT denotes the time offset of the second pilot in the slot compared to half of the slot time $T_{slot}/2$. Since $s(t)$ is periodic, we can express it in terms of the Fourier series as

$$s(t) = \sum_{l=\infty}^{\infty} s_l e^{i2\pi\frac{t}{T_{slot}}l},$$

where the Fourier-series coefficients are given by

$$\begin{aligned} s_l &= \frac{1}{T_{slot}}\int_0^{T_{slot}} s(t)e^{-i2\pi\frac{t}{T_{slot}}l}dt \\ &= \frac{1}{T_{slot}}\left(1 + e^{-i\pi\left(1+2\frac{\Delta T}{T_{slot}}\right)l}\right) \\ &= \frac{1}{T_{slot}}\left(1 + (-1)^l e^{-i2\pi\frac{\Delta T}{T_{slot}}l}\right) \\ &= \frac{2}{T_{slot}}\frac{1+(-1)^l}{2} + \frac{1}{T_{slot}}(-1)^l\left(e^{-i2\pi\frac{\Delta T}{T_{slot}}l} - 1\right). \end{aligned}$$

The sampled channel is $h_s(t) = \hat{h}[0; t]s(t)$. Now using the Fourier series representation of $s(t)$ and taking the Fourier transform of $h_s(t)$, we obtain the Discrete Time Fourier Transform (DTFT) of the sampled channel response:

$$H_s(f) = \frac{2}{T_{slot}}\sum_{l=-\infty}^{\infty} H\left(f - \frac{2l}{T_{slot}}\right) + \frac{1}{T_{slot}}\sum_{l=-\infty}^{\infty}\varepsilon_l H\left(f - \frac{l}{T_{slot}}\right),$$

where $\varepsilon_l = (-1)^l(e^{-i2\pi\frac{\Delta T}{T_{slot}}l} - 1)$.

The first (upper) sum corresponds to the spectrum of the channel sampled at rate $\frac{2}{T_{slot}} = 4$ kHz and the second (lower) sum contains additional aliased components due to the irregularity of the sampling ΔT. Fig. 3 shows that after sampling, the spectrum contains the desired FSK signal, its harmonic components as well as aliased harmonics.

Even with 4-kHz sampling frequency, we would experience severe aliasing of the harmonic components of the square waves. Due to irregular sampling, we will see additional aliased components, but they are attenuated by the factor $|\varepsilon_l|$. To be on the safe side, we select the square-wave nominal frequencies to be in the range $f_k \in [200, 1000]$ Hz. The lower limit is selected to be larger than the natural Doppler in the channel such that the direct path $h_1(t)$ can be filtered away using a high-pass filter. The upper frequency is selected to be small enough to avoid additional aliasing due to the irregular sampling.

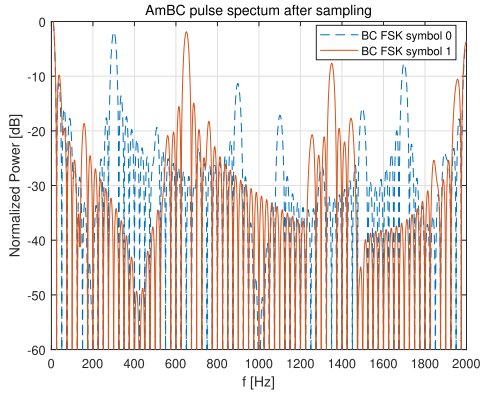


Fig. 3. Discrete Time Fourier Transform of the sampled FSK signal.

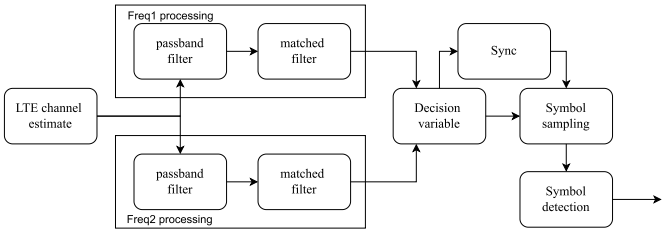


Fig. 4. Flow chart of the proposed backscatter receiver.

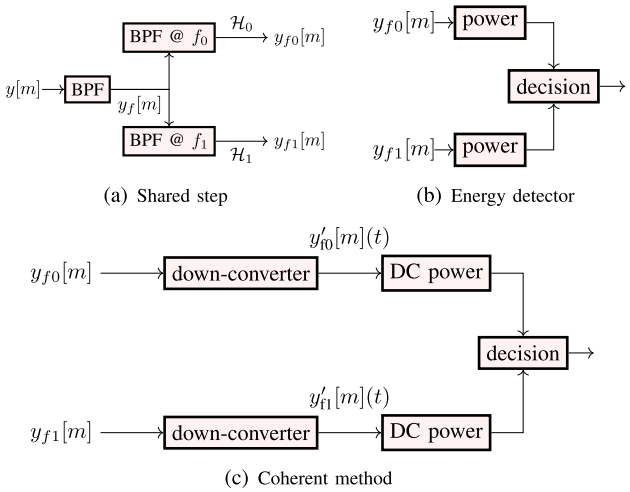


Fig. 5. Flowchart of the FSK demodulator. We proposed both coherent and noncoherent detectors. Flow chart (a) is shared step of both detectors. Flow charts (b) and (c) are the energy detector and coherent method separately. The complete energy detector is composed of (a) and (b). Also, the total coherent method consists of (a) and (c).

Even if the two backscatter symbols $x_0(t)$ and $x_1(t)$ would have been selected to be orthogonal, it turns out that the orthogonal choices after sampling will interfere with each other. Due to aliasing, it turns out that orthogonal choices $f_1 = Kf_0$ for the integer K leads to high interference from aliased harmonics hitting the other symbol. It thus seems advantageous to not take K as an integer.

B. Receiver Structure for BD

The flow chart in Fig. 4 shows the algorithm steps of the proposed backscatter receiver. In this section, the purposes of some steps in the receiver are elaborated on.

1) Band-Pass Filter: It is easy to assume that the BD symbol keeps frame synchronicity when it is received and demodulated by a UE. Let $m \in \mathbb{N}$ denote the m-th symbol backscatter sending at time $t = mT_{BC}$.

The channel phase of the scatter path $\arg\{h_0(mT_{BC})\}$ is ambiguous due to synchronization. The power of the first channel tap $l = 0$ does not contain the phase uncertainty. The receiver only operates with channel tap power $y[m] = |\hat{h}[0; m]|^2$.

The noise-free channel power satisfies the following approximation

$$y[m] \approx x[m]\beta[m] + \alpha[m],$$

where $x[m]$ is the BD signal, $\alpha[m] = |h_1(mT_{BC})|^2$, and $\beta[m] = |h_0(mT_{BC})|^2 + 2\mathrm{Re}\{h_1^*(mT_{BC})h_0(mT_{BC})\}$, considering the fact that $x^2[m] = x[m]$.

To separate the two channels, a high-pass filter and a low-pass filter is required. The high-pass filter is designed to block $\alpha[m]$. And the low-pass filter aims to constrain the harmonic frequency and other interference. In practice, these two separate filters can be combined as a band-pass filter (BPF). Considering that the frequency keys of FSK modulation are only several hundreds Hz, the Doppler effect is the principle threat of propose backscatter receiver. The Doppler effect and the frequency drift of the BS and UE contribute to the channel change of $\alpha[m]$ and $\beta[m]$ on a small time scale. By switching the BD at a higher frequency than the maximum Doppler in the channel, the Doppler frequency is restrained by the filter. With the help of a high-pass filter on $y[m]$ to remove the DPI $\alpha[m]$, the BD-modulated path component $\beta[m]$ is distinguished in the frequency domain. Thus, two frequency keys of the BD FSK symbols remain. In the base band, the FSK symbol is designed having two frequency keys, namely f_0 and f_1, where $f_k = 1/T_k, k = 0, 1$.

2) FSK Demodulator: After passing a high-pass filter and low-pass filter, the received 2-FSK signal $y_f[m]$ is demodulated. We propose a coherent detector and a noncoherent energy detector for the task in Fig. 5.

Both the coherent detector and the energy detector share a single step, that is, initially filtering $y_f[m]$ at f_0 and f_1. There is an aliasing effect of the two FSK as illustrated in Fig. 3. The harmonic components of one FSK key could unfortunately hit another FSK key. A BPF is applied to exclude the frequency leakage of other components and to constrain the interference frequency. Denote the signal filtered by a BPF at center frequency f_0 of $y_f[m]$ as $y_{f0}[m]$, and that at center frequency f_1, as $y_{f1}[m]$.

The energy detector compares the power of spectrum $f_0 \pm \Delta f$ and the power of spectrum $f_1 \pm \Delta f$. An FSK symbol is decided based on the frequency spectrum which contains higher power. For the FSK symbol $x[m]$, hypothesis testing $\mathcal{H}_0$ denotes that the BD sends $x[m]$ symbol 0. Similarly, hypothesis testing $\mathcal{H}_1$ refers that $x[m]$ is symbol 1. Thus, for the energy detector,

$$E\Big[|y_{f1}[m](t)|^2\Big] \underset{\mathcal{H}_1}{\overset{\mathcal{H}_0}{\lessgtr}} E\Big[|y_{f0}[m](t)|^2\Big].$$

TABLE I
MEASUREMENT SETUP PARAMETERS

	Parameter	Value
Tx	Baseband signal generator	R&S SMBV100A Vector Signal Generator
	Antenna	R&S HK033 VHF/UHF coaxial dipole
	Carrier frequency	486MHz
	Bandwidth	7.68 MHz
	Tx power level	15 dBm
	Peak envelop power	29.09 dBm
BD	Baseband signal generator	Tektronix AFG 31000 Arbitrary Function Generator
	Antenna	RaTLSnake M6 telescopic antenna
	Symbol duration	40 ms
	Synchronization	7-bit Braker code (three times, twice positive codes and once negative codes)
	Modulation scheme	FSK (300 Hz and 650 Hz)
Rx	Device	NI USRP-B210
	Antenna	RaTLSnake M6 telescopic antenna
	AD converter	12 bits
	Spectrum analyzer	Tektronix RSA6114A

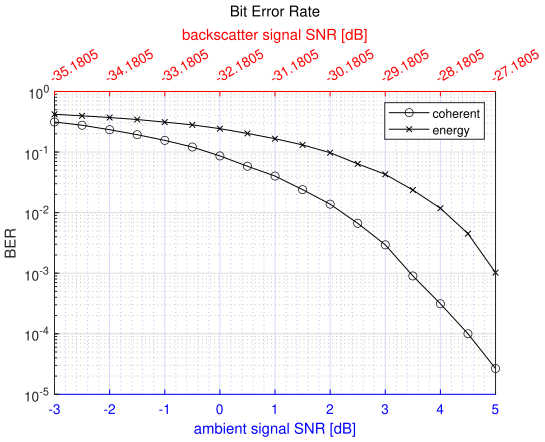


Fig. 6. Theoretical BER performance of the coherent detector and the energy detector.

The coherent method down-converts the signal to the base band by multiplying the signal with $\exp(-j2\pi f_c t)$.

$$y'_{\mathrm{f0}}[m](t) = y_{\mathrm{f0}}[m](t)e^{-j2\pi f_0 t},$$
$$y'_{\mathrm{f1}}[m](t) = y_{\mathrm{f1}}[m](t)e^{-j2\pi f_1 t}.$$

The decision is made by comparing the base band power of $y'_{\mathrm{f0}}[m](t)$ and $y'_{\mathrm{f1}}[m](t)$. The base band power is, in fact, the power of an average signal. And then, the FSK symbol decision is make based on the power comparison:

$$\left|E\left[y'_{\mathrm{f1}}[m](t)\right]\right|^2 \underset{\mathcal{H}_1}{\overset{\mathcal{H}_0}{\lessgtr}} \left|E\left[y'_{\mathrm{f0}}[m](t)\right]\right|^2.$$

V. SIMULATION AND VALIDATION

A. Parameters

We propose to select FSK $f_0 = 300$ Hz and $f_1 = 650$ Hz, and $T_{BC} = 40$ ms which corresponds to six periods of the symbol "0" wave, and 13 periods of the symbol "1" wave. A BPF with a bandwidth of 200 Hz is applied in the FSK demodulator with a different center frequency. $y_{\mathrm{f0}}[m]$ is filtered by a BPF with a bandwidth of 200 Hz at a center frequency of 300 Hz and $y_{\mathrm{f1}}[m]$ is filtered by a BPF with a bandwidth 200 Hz at a center frequency at 650 Hz.

The ambient signal is an LTE CRS signal, whose parameters are given in Table I. Frequency Division Duplex (FDD) operation is assumed. The BS and the UE are assume to be equipped with only a single antenna. The BS uses only antenna port 0. The utilized downlink carrier frequency is 486 MHz with a bandwidth 7.68 MHz which accommodates 21 resource blocks.

B. Simulations

The free-space path loss (FSPL) model is applied to different propagation paths with additive white Gaussian noise (AWGN) added to the channel. For the backscattered channel, the path loss is the product of the two links: from transmitter to BD and from BD to receiver [26]. The channel impulse response $h(t)$ and FSPL is supposed to obey

$$L = \left(\frac{4\pi D}{\lambda}\right)^2 = E\left[|h(t)|^2\right], \tag{3}$$

where D is distance between the Tx and Rx, $\lambda = c/f_c$ is the wave length of the carrier frequency f_c. The path loss L here is in linear scale. In this simulation, the distance from the Tx to Rx is 125 m, the distance from the Tx to BD is 130 m and the distance from the BD to Rx is 10 m. In the simulation, we consider that the two propagation paths are both non-line-of-sight (NLOS) and obey Rayleigh distribution. The received sample at the time instant t at the Rx is represented as

$$y(t) = h_0(t)s(t) + R_{\mathrm{on}}h_1(t)s(t)x(t) + z(t), \tag{4}$$

where R_{on} is the reflection coefficients of the BD under 'on' status, $h_0(t)$ and $h_1(t)$ are the channel impulse response of the scattered path and direct path, $s(t)$ is the LTE CRS ambient signal and $z(t)$ is AWGN. Depending on the symbols BD sent, $x(t)$ can be either $x_0(t)$ or $x_1(t)$. Footnote 0 refers to the direct path between the Tx and Rx, and footnote 1 refers to the backscatter communication path between the Tx and Rx via the BD. In an ideal BD, the reflection coefficient is $\Gamma = -1$ when the BD is in "on" state and $\Gamma = 0$ in the "off" state, but in practice these values tend to be closer to each other. To model the non-ideality, we assume that the BD attenuates the reflected signal power by $-20\log_{10}(R_{\mathrm{on}}) = 6$ dB.

In Fig. 6, two SNR are defined in the dB scale, as shown on the top and the bottom x-axis. For the received signal, the noise is $z(t) \sim \mathcal{CN}(0, \sigma_z^2)$, and hence the power of the noise is $P_z = \sigma_z^2$. The difference is the definition of signal power in the SNR. The blue x-axis on the bottom is based on CRS power and the red axis at the top is for the received BD-modulated signal power. The power of the CRS is

$$P_{s1} = E\left[|h_0(t)s(t) + R_{\mathrm{on}}h_1(t)s(t)x(t)|^2\right],$$

which corresponds to the LTE Reference Signal Received Power (RSRP) in the absence of noise.

Hence for the blue x-axis, we have

$$\mathrm{SNR}_1 = \frac{P_{s1}}{P_z} = \frac{E\left[|h_0(t)s(t) + R_{\mathrm{on}}h_1(t)s(t)x(t)|^2\right]}{\sigma_z^2}.$$

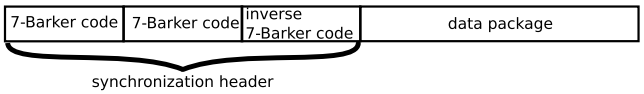


Fig. 7. Backscatter frame format of the proposed backscatter.

The red x-axis on the top treats the backscatter FSK signal from the backscatter as the signal of interest. The backscatter signal SNR of AmBC is defined as

$$\mathrm{SNR}_2 = \frac{E\left[|R_{\mathrm{on}} h_1(t) s(t) x(t)|^2\right]}{\sigma_z^2}.$$

As Eq. (4) illustrated, the power of the two path difference is given by

$$\begin{aligned} 10\log(\Delta L) &= 10\log E\left[|h_0(t)|^2\right] - 10\log E\left[|h_1(t)|^2 R_{\mathrm{on}}^2\right] \\ &= 10\log L_0 - 10\log L_1 - 20\log R_{\mathrm{on}}. \end{aligned}$$

Using the MATLAB LTE toolbox, the Rayleigh fading channel model is applied. The oppler frequency shift is not considered in this simulation, although the Doppler effect influences a lot in practice. MIMO channel propagation is also not setup, because the transmitter and receiver antenna is assumed to be SISO. The LTE downlink channel estimator estimates the channel based on that CRS signal. No OFDM symbol is interpolated between the CRS pilots.

The coherent detector algorithm and energy detector algorithm are discussed in Section IV-B2 FSK demodulator. To smooth the simulation BER curve, we simulate various times of experiments. High BER points (BER $>$ 0.01) simulate 10000 times Monte Carlo experiments. Low BER points (BER $\leq$ 0.01) simulate 100000 times Monte Carlo experiments.

The simulation uses backscatter communication parameters as mentioned in Section V-A Parameters. Fig. 6 shows the BER performance of the two AmBC receivers. The energy detector is always worse than the coherent detector. In the low SNR region, such as -3 dB, the two methods have similar performance. The BER difference of the two FSK demodulators is small. The gap of BER performance between the two detectors widens, such as, SNR $=$ 5 dB.

C. Backscatter Signal Synchronization

A special backscatter frame structure is designed to find out the beginning of a backscatter signal. The backscatter signal is synchronized by three sequences of 7-Barker code. As shown in Fig. 7, there are two parts in one backscatter frame, the synchronization header and the data packet. At the beginning of one packet, two continuous sequences of 7-bit Barker code (“0000110”) followed by an inverse 7-bit Barker code (“1111001”) composes the synchronization header. Then the data packet attaches the synchronization header.

Between the two backscatter frames, there is a short period that no FSK symbol is sent, called the sleep period. During sleep period, the BD kept in the “off” state and the ambient signal is not shifted.

Compared to previous work [6], the need for a clock signal for synchronization is eliminated from the proposed method.

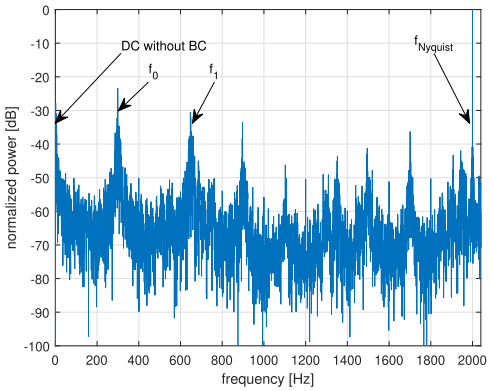


Fig. 8. An FSK-modulated backscatter signal in spectrum.

Sometimes, backscatter packets would be synchronized incorrectly. In that case, the data bit error could be incredibly high (more than one third). The synchronization header bits are already known, as a part of the backscatter communication protocol. By comparing the known synchronization bits with the demodulated bits, we can evaluate the quality of the data received at the Rx and decide whether synchronization was successful or not. If the measurement indicates that the synchronization failed, we discard the whole packet.

D. Measurements

This measurement is a validation of the aforementioned coherent detector simulation. The measurement parameters are described in Section V-A.

The transmitter is a Rhode&Schwarz (R&D) SMBV100 signal generator with LTE signal packets. The generator emits a standard LTE signal with 50 resource block (7.68 MHz bandwidth) at 486 MHz carrier frequency and the transmission power is 15 dBm. The frame structure is for a SISO system with a corresponding synchronization signal and pilots for cell ID 3.

The BD node is an in-house design as shown in Fig. 1(c). The control signal from the MCU is driven by a RaspberryPi nano, an RP2040-based MCU board.

The receiver is a universal software radio peripheral (USRP), connected to a laptop. Some post-signal processing is executed on that laptop, using MATLAB.

1) System Validation: We validate the system with measurements over cables. The impacts of the DPI is attenuated by a circulator. In this case, the backscatter frequency-shifting phenomenon can be emphasized in the spectrum analyzer, as shown in Fig. 9. This experiment measures over the cables in the absence of the direct path component $h_1(t)$. A circulator routes signal from the LTE signal generator to the BD and then from the BD to USRP. Fig. 8 and 9 simply give the spectrum and spectrogram of the USRP receiver, respectively.

The two symbols are clearly visible in the spectrum as well as their aliased harmonic components. In addition, there is a strong DC component and a component at 2 kHz corresponding to the uniform sampling frequency $1/T_{slot}$, which the arrow f_{Nyquist} points to in Fig. 8. The spectrum was obtained using a Fast Fourier Transform directly on the measured channel

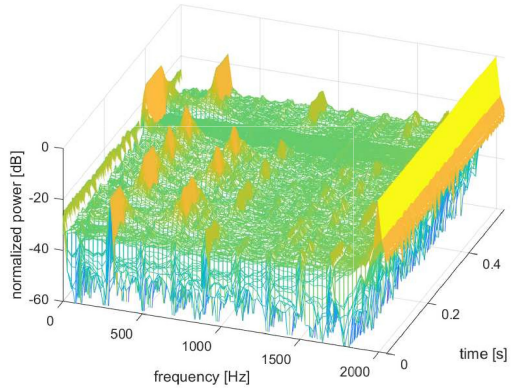


Fig. 9. A validation of a FSK-modulated BD signal in spectrogram.

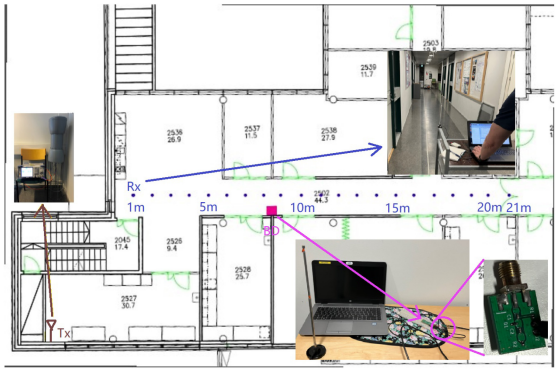


Fig. 10. Over-the-air measurement devices setup and site floor plan.

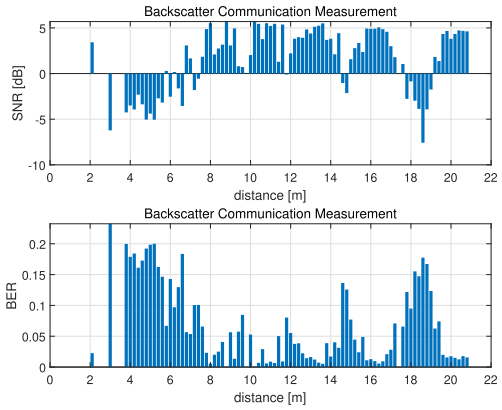


Fig. 11. Over-the-air measurement performance of AmBC in SNR and BER.

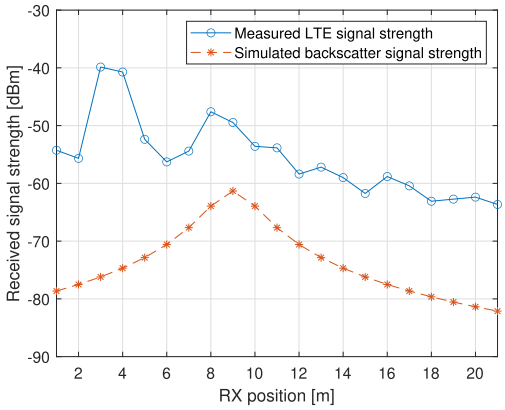


Fig. 12. Variation in the measured received LTE signal power and the simulated backscatter signal power at the 21 Rx positions. The backscatter signal power is calculated using the FSPL with an exponent of 2.

samples $\hat{h}[0, t_s]$ without compensating for the irregularity of the underlying sampling process. From the spectrogram that illustrates how the spectrum changes in time, we can clearly see the transmitted symbol sequence '11001010' by observing the power at the frequencies f_0 and f_1. As illustrated in Fig. 8 around 0.5 s, there is a 100 ms sleep period, presenting a peak at direct current (DC) component.

The spectrogram of the square-wave FSK is illustrated in Fig 9. There are two frequency keys f_0 (300 Hz) and f_1 (650 Hz) the appear alternately. The peak of 2 kHz is caused by uniform sampling frequency $1/T_{slot}$, as shown in Fig. 8. Other peaks in the spectrum, such as 900 Hz, are caused by the alias from other components on the spectrum or harmonic frequency.

2) Over-the-Air Measurement: This over-the-air measurement is a proof-of-concept of the proposed AmBC system. The experiment environment is setup as Fig. 10. The AmBC communication experimental results are recorded as in Fig. 11. The experimental BER and simulation prediction BER are compared in Section VI.

Fig. 10 presents the measurement environment at Maarintie 8 on Aalto University campus. The transmitter antenna R&S HK300 is located in the lower lefthand corner in the Figure. The BD node is in the middle of the corridor next to the measurement point 9 (at 9 m from the wall). The receiver is a USRP B205 unit and a laptop running in-house created C++ implementation of a LTE receiver, connected to a UDP port with a MATLAB implementation of the AmBC signal detection. The receiver implements real time decoding of received AmBC signal.

Different from our previous work [6], no external synchronization clock is distributed between the transmitter, BD, and receiver.

In Fig. 11, the SNR and BER are measured on the positions marked in the corridor shown in Fig. 10, with step 0.2 m, from 2 m to 21 m. The x-axis refers to the position of receiver, indicating the distance to the corridor wall in Fig. 10. At most positions, receiver can receive the signal from the BD and demodulate the symbols. When the AmBC system works, the BER and SNR describe the AmBC communication system performance.

In particular, the measurement system cannot detect a weak signal which is lower than an analog digital converter (ADC) in the environment. In Fig. 12, a simulation is given for the received power of the weak backscatter signal as a supplement. The simulation is based on the backscatter path-loss mode [26] and completely ignores the impact of the walls. Thus, it can be treated as an upper bound for the actual backscattered power.

The data at some positions are lost, due to the high BER. If the BER is too high, a possible explanation is that the backscatter frame is not correctly synchronized by three 7-barker bits header. As Section V-C stated, that data sequence is useless if the packet is asynchronized. In our measurement,

if the BER is higher than one over three, then that backscatter data packet is omitted. I think the BER looks not far from FSK theoretical BER curve. But I just don't under stand its Monte-Carlo curve. Why it does not converge to a smooth exponential asymptote.

In the over-the-air measurement shown in Fig. 11, the relationship between the BER and SNR roughly satisfies the following relationship: low BER positions are usually under high SNR environments. A sinusoidal tendency appears in the SNR via distance. That periodic phenomena in the tunnel corridor (6 m to 16 m) is distinct from other positions. The BER shows the same periodic regular pattern with the SNR. In the room 2536 (distance less than 6 m), the SNR starts to deteriorate. Then, at the fork road corner (between 16 m and 18 m), the SNR decreases steeply.

The received ambient signal power at each measurement position is estimated based on the received LTE signal power. The step length of the LTE ambient signal power measurement is 1 m, which is the blue curve in Fig. 12. Backscatter signal power is calculated based on Friis transmission equation, which is red line in Fig. 12. We assume position propagation paths from the transmitter to BD and from the BD to each measurement position, are all line of sight. The FSPL module is applied in the estimation of the backscatter signal power, as Eq. (3). But this FSPL module is higher than that of the real backscatter signal power received at the measurement positions. In practice, the difference between the ambient LTE signal power and the backscatter signal power is even larger than that in Fig. 12.

The measured LTE signal power (blue line in Fig. 12) for 8 m to 21 m approximately obeys the FSPL. Because the BD is set at 9 m, the simulated backscatter signal power (orange line in Fig. 12) peaks at 9 m, showing a typical FSPL pattern as a function of distance. Comparing the two plots, Fig. 11 and Fig. 12, some noteworthy contrasts are given in the following. Around 6 m the LTE signal deteriorates. That ambient signal attenuation also can be observed in Fig. 11. Around 6 m, the SNR decreases dramatically with the BER jumping to a high level. A steep drop of LTE signal power from 1 m to 2 m is believed to be caused by a metal door between room 2045 and room 2536, which lies exactly between the transmitter and the measurement receiver.

VI. Discussion

Comparison of the simulation result and the over-the-air measurements are illustrated in Fig. 13. The results indicate that there is approximately 3 - 4 dB loss between the measured performance compared to the simulated one. The trend of the coherent detector simulation curve does not perfectly fit over-the-air measurements. This is due to the simulation conditions and measurements not being completely consistent. The simulations were done assuming line-of-sight conditions and a fixed transmitter, receiver and BD locations and varying only the received power level. The measurements, in turn, were taken in a real office environment impacted by multipath propagation. In the measurements, the transmitter and BD location were fixed while the receiver location was varied.

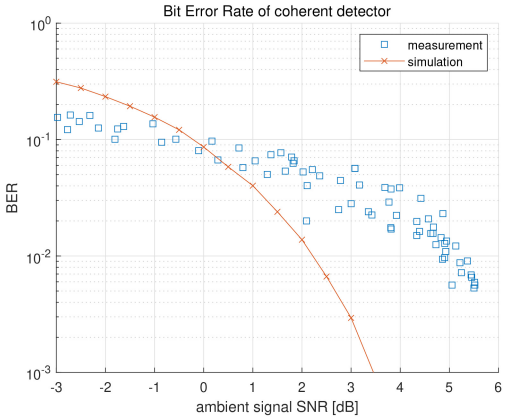


Fig. 13. Compare coherent detector simulation and practice performance, in SNR VS BER.

Also the measurements were performed using a 12-bit ADC while the simulations assumed ideal sampling. The power difference between the direct and scattered path varied (see Fig. 12) causing changes in the quantization noise in the actual measurements which too were omitted in the simulations.

The reason why in Fig. 13 some of the measured points have a lower BER than that suggested by the simulations is due to the fact that we were able to measure the BER only for those packets that the receiver was able to synchronize to.

The performance of the proposed AmBC system is drastically different to LScatter proposed in [18]. LScatter achieved over 10 Mbps data rates whereas the FSK method proposed in this paper has a data rate of only 3.125 bps. It should be noted, however, that our method enable the BD to share the bandwidth with the LTE while LScatter shifted the BD-modulated signal to an adjacent band which was required to be empty. This is a strict requirement that goes against the aim of mobile operators to maximize spectrum utilization. Even though the data rate of our FSK backscatter is quite low, it is still sufficient for the foreseen CD-ZED application. Also it is worth noting, that the BD symbol duration was selected to be relatively long to ensure uncoded operation even in low SNR conditions. By shortening the BD symbol, the data rate could be increased.

Our proposed system does not require the BD to be synchronized with the LTE signal, giving a simpler BD structure. Even though the system indeed requires the synchronization between the LTE and the UE (AmBC receiver), it can be easily done by LTE UEs. The analysis and the measurement suggest that any receiver that can synchronize with LTE signal can be utilized as the AmBC receiver. This facilitates the implementation of AmBC receivers.

We argued that the impact of the BD on the LTE receiver is likely to be small since the BD-modulated signal path is much weaker than the direct path. The fact that the UE (AmBC receiver) channel estimator is able to track the BD signal in order to demodulate it, indicates also that the other irrelevant UE channel equalizers could track the channel. The actual impact thus depends on the implementation of the UE channel equalizer and could vary from one modem to another.

In this paper, we only considered a single BD device, but in order to build a CD-ZED application, the system needs to be extended to support multiple access. This is left as a further study.

VII. Conclusion

In this paper, we proposed a system that uses the LTE CRS and channel estimator for receiving backscatter modulated signals. The BD utilized two square waves having different nominal frequencies to perform frequency shift modulation. The proposed receiver was validated using over-the-air measurements in an indoor environment. Based on our experimental results, we can conclude that the LTE channel estimator offers a great potential to be utilized for receiving backscattered signals in Ambient Internet of Things applications.

References

[1] V. Liu, A. Parks, V. Talla, S. Gollakota, D. Wetherall, and J. R. Smith, "Ambient backscatter: Wireless communication out of thin air," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 43, no. 4, pp. 39–50, 2013.

[2] R. Fara, "Ambient backscatter communications in future mobile networks," Ph.D. dissertation, Dept. Inf. Sci. Technol. Commun., Université Paris-Saclay, Paris, France, Oct. 2021. [Online]. Available: https://theses.hal.science/tel-03434254

[3] D.-T. Phan-Huy, D. Barthel, P. Ratajczak, R. Fara, M. Di Renzo, and J. De Rosny, "Ambient backscatter communications in mobile networks: Crowd-detectable zero-energy-devices," *IEEE J. Radio Freq. Identif.*, vol. 6, pp. 660–670, 2022.

[4] H. Stockman, "Communication by means of reflected power," *Proc. IRE*, vol. 36, no. 10, pp. 1196–1204, Oct. 1948.

[5] K. Finkenzeller, *Rfid Handbook: Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication*. New York, NY, USA: Wiley, 2010.

[6] K. Ruttik, X. Wang, J. Liao, R. Jäntti, and P.-H. Dinh-Thuy, "Ambient backscatter communications using LTE cell specific reference signals," in *Proc. IEEE 12th Int. Conf. RFID Technol. Appl. (RFID-TA)*, 2022, pp. 67–70.

[7] R. Biswas, M. U. Sheikh, H. Yiğitler, J. Lempiäinen, and R. Jäntti, "Direct path interference suppression requirements for bistatic backscatter communication system," in *Proc. IEEE 93rd Veh. Technol. Conf. (VTC-Spring)*, 2021, pp. 1–5.

[8] K. Ruttik, R. Duan, R. Jäntti, and Z. Han, "Does ambient backscatter communication need additional regulations?" in *Proc. IEEE Int. Symp. Dyn. Spectr. Access Netw. (DySPAN)*, 2018, pp. 1–6.

[9] A. N. Parks, A. Liu, S. Gollakota, and J. R. Smith, "Turbocharging ambient backscatter communication," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 44, no. 4, pp. 619–630, 2014.

[10] H. Yiğitler, X. Wang, and R. Jäntti, "Optimum multiantenna ambient backscatter receiver for binary-modulated tag signals," *IEEE Trans. Wireless Commun.*, vol. 22, no. 2, pp. 808–823, Feb. 2023.

[11] J. Lietzén, A. Liljemark, R. Duan, R. Jäntti, and V. Viikari, "Polarization conversion-based ambient backscatter system," *IEEE Access*, vol. 8, pp. 216793–216804, 2020.

[12] R. Fara, D.-T. Phan-Huy, A. Ourir, M. Di Renzo, and J. de Rosny, "Robust ambient backscatter communications with polarization reconfigurable tags," in *Proc. IEEE 31st Annu. Int. Symp. Pers. Indoor Mobile Radio Commun.*, 2020, pp. 1–7.

[13] G. Vougioukas and A. Bletsas, "Switching frequency techniques for universal ambient backscatter networking," *IEEE J. Sel. Areas Commun.*, vol. 37, no. 2, pp. 464–477, Feb. 2019.

[14] P. Zhang, D. Bharadia, K. Joshi, and S. Katti, "HitchHike: Practical backscatter using commodity WiFi," in *Proc. 14th ACM Conf. Embedded Netw. Sens. Syst. CD-ROM*, 2016, pp. 259–271.

[15] J. Qian, A. N. Parks, J. R. Smith, F. Gao, and S. Jin, "IoT communications with M-PSK modulated ambient backscatter: Algorithm, analysis, and implementation," *IEEE Internet Things J.*, vol. 6, no. 1, pp. 844–855, Feb. 2019.

[16] J. E. Palmer, H. A. Harms, S. J. Searle, and L. Davis, "DVB-T passive radar signal processing," *IEEE Trans. Signal Process.*, vol. 61, no. 8, pp. 2116–2126, Apr. 2013.

[17] P. Zhang, M. Rostami, P. Hu, and D. Ganesan, "Enabling practical backscatter communication for on-body sensors," in *Proc. ACM SIGCOMM Conf.*, 2016, pp. 370–383.

[18] Z. Chi, X. Liu, W. Wang, Y. Yao, and T. Zhu, "Leveraging ambient LTE traffic for ubiquitous passive communication," in *Proc. Annu. Conf. ACM Spec. Interest Group Data Commun. Appl. Technol. Archit. Protocols Comput. Commun.*, 2020, pp. 172–185.

[19] "3rd generation partnership project (3GPP); technical specification group radio access network, physical channels and modulation, evolved universal terrestrial radio access (E-UTRA)," 3GPP, Sophia Antipolis, France, Rep. TR 36.211, 2010.

[20] G. Wikström et al., "Challenges and technologies for 6G," in *Proc. 2nd 6G Wireless Summit (6G SUMMIT)*, 2020, pp. 1–5.

[21] "3rd generation partnership project (3GPP); technical specification group radio access network, ambient IoT device characteristics and categorization," 3GPP, Sophia Antipolis, France, 3GPP document TSG RAN Meeting #98e, RP-223400, 2022.

[22] M. A. Uusitalo et al., "6G vision, value, use cases and technologies from European 6G flagship project Hexa-X," *IEEE Access*, vol. 9, pp. 160004–160020, 2021.

[23] G. Madhugiri, C. Koutsimanis, and P. Skillermark, "Impact of CSI optimization and CRS selection on performance of LTE release 8 networks," in *Proc. IEEE 79th Veh. Technol. Conf. (VTC Spring)*, 2014, pp. 1–5.

[24] R. Behzad, *RF Microelectronics*, 2nd ed. New York, NY, USA: Prentice-Hall, 2012.

[25] B. Badihi, A. Liljemark, M. U. Sheikh, J. Lietzén, and R. Jäntti, "Link budget validation for backscatter-radio system in sub-1GHz," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, 2019, pp. 1–6.

[26] J. D. Griffin and G. D. Durgin, "Complete link budgets for backscatter-radio and RFID systems," *IEEE Antennas Propag. Mag.*, vol. 51, no. 2, pp. 11–25, Apr. 2009.