Back-Channel Wireless Communication Embedded in WiFi-Compliant OFDM Packets

Hun Seok Kim, *Member, IEEE,* and David D. Wentzloff, *Senior Member, IEEE*

***Abstract*—This paper presents innovative *back-channel* wireless communication techniques for ultra-low power (ULP) devices. The concept of embedded back-channel communication is proposed to enable a variety of new applications by interconnecting heterogeneous ULP devices through existing Orthogonal Frequency Division Multiplexing (OFDM) based WiFi (IEEE 802.11a/g/n/ac) networks. The proposed back-channel communication allows ULP devices to decode messages embedded in WiFi OFDM packets even if these ULP devices are incapable of demodulating OFDM. The proposed back-channel signaling has unique properties that are easily detectable by non-WiFi ULP receivers consuming sub-mW of active power. The proposed scheme eliminates the need for specialized transmitter hardware or dedicated channel resources for embedded back-channel signal transmission. Instead, carefully sequenced data bit streams will generate back-channel messages from already-deployed WiFi infrastructure without any hardware modification. This paper demonstrates that WiFi OFDM back-channel communication is feasible in various modulation formats such as pulse position modulation (PPM), pulse phase shift keying (PPSK), or frequency shift keying (FSK). Systematic algorithms are unveiled to create back-channel messages in various modulation formats from a WiFi standard compliant datapath. Comprehensive bit error rate (BER) performance analysis of various WiFi back-channel communication schemes is derived and validated in realistic multi-path frequency selective fading channels.**

***Index Terms*—WiFi, OFDM, back-channel communication, ultra-low power wireless receiver.**

I. Introduction

In modern ultra-low power (ULP) wireless Internet-of-Things (IoT) applications, wireless communication is typically the dominant factor in overall power consumption [1] - [3]. Realizing energy-efficient wireless communication, therefore, is the most critical issue to prolong the lifespan of extremely energy- / power-constrained ULP IoT devices.

This paper presents a new concept of back-channel communication embedded in standard compliant wireless packets. We consider the Orthogonal Frequency Division Multiplexing (OFDM) [4] based WiFi (IEEE 802.11 a/g/n/ac) [5] as the primary target wireless standard although the proposed technique can be generalized for other standards as well. The proposed back-channel communication does not require specialized hardware or a dedicated wireless channel to send back-channel signals embedded in standard compliant packets. Instead, carefully crafted bit sequences in the data message would generate embedded back-channel signals. That is, back-channel signal transmission is entirely software-defined by simply using a proper data bit sequence on standard compliant packets without modifying already-deployed hardware infrastructure. The primary motivation for back-channel communication is to reduce the amount of energy used for wireless communication, while maintaining the ability to communicate with existing wireless infrastructure such as WiFi networks. This is achieved by designing an ULP receiver that can detect the back-channel signaling, where that back-channel receiver does not have to be compliant with the WiFi standard to do so.

H.S. Kim and D. Wentzloff are with the Department of Electrical Engineering and Computer Science, University of Michigan, Ann Arbor, MI, 48109, USA, e-mail: hunseok@umich.edu, wentzlof@umich.edu.

Demodulating a WiFi OFDM signal is a power demanding task (typically $\geq 120mW$ [6] - [8]) due to stringent RF / analog frontend specifications and sophisticated digital baseband processing. Although WiFi signals are ubiquitously available in urban environments, the majority of ULP IoT devices cannot utilize WiFi connectivity because of their extremely limited power and/or complexity budget [1] - [3], [9], [10]. The proposed back-channel communication technology will break this barrier to allow heterogeneous ULP IoT devices to interoperate with already existing WiFi infrastructure with minimal power consumption.

Prior works [11] [12] demonstrated a primitive back-channel communication concept in the form of packet length modulation or packet interval modulation using multiple consecutive WiFi or Bluetooth Low Energy (BLE) packets. The packet length or interval modulation utilizes an entire packet (or multiple packets) as an on-off-keying information symbol for the energy detector based receiver. Its efficiency, however, is very poor since the signaling requires many consecutive packets. Moreover, this form of back-channel signaling is particularly vulnerable to interferences as the packet length modulation [11] is susceptible to an interferer OFDM packet (or any other high power interference signal) that could appear between multiple back-channel signaling packets. The WiFi/BLE packet collision (which is common in the collision avoidance based medium access control scheme) can disrupt the packet length or interval modulation too. The other related technique is the hierarchical modulation [13] [14] [15]. In hierarchical modulation, receivers can selectively demodulate high rate (e.g., 16QAM) or low rate (e.g., 4QAM ignoring 2 LSBs out of 16QAM) information from a single packet depending on the channel quality. Unlike our proposed back-channel scheme, however, this hierarchical modulation scheme does not allow communication among heterogeneous devices using very distinct modulation schemes (e.g., coherent vs. non-coherent).

This paper demonstrates intra-packet back-channel modulation schemes and the feasibility of the embedded back-channel signal generation without modifying the existing packet struc-

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JSAC.2016.2612078, IEEE Journal on Selected Areas in Communications

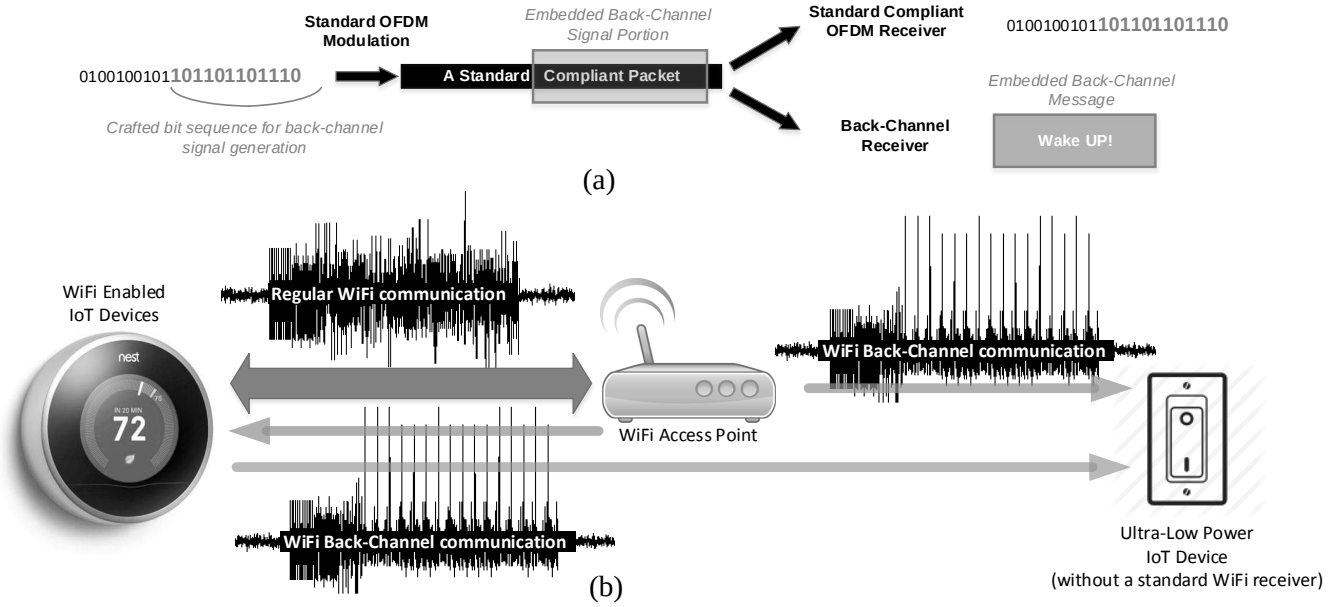

Fig. 1. Concept of WiFi back-channel communication

ture of WiFi standards. Embedded back-channel signals are all generated by a set of carefully crafted bit sequences within the boundary of standard compliant packet structure. The proposed back-channel communication concept is depicted in Fig. 1 - (a). A standard compliant data receiver can demodulate the entire bit sequence including the bits to create back-channel message. Meanwhile, at the ULP back-channel receiver, only the embedded back-channel message is decodable, not the entire bit sequence.

The back-channel signaling must be accomplished within strict constraints of the standard compliant packet structure. This paper discusses systematic methods to generate a subset of unique bit sequences that will embed desired back-channel signals in WiFi packets using pulse position modulation (PPM), pulse phase-keying keying (PPSK), and frequency shift keying (FSK) formats. This back-channel concept can be extended and generalized to other OFDM based communication systems such as the cellular 4G LTE (long-term evolution). Therefore, the proposed back-channel technique could directly impact the next wireless standardization to adopt more flexible packet structures to enrich use-cases of back-channel communication.

The comprehensive low power wireless transceiver survey [16], Fig. 2, indicates that the state-of-the-art ULP transceivers are capable of operating at $\geq$ -95 dBm received signal sensitivity level with sub-mW of active power consumption. It is worth noting that almost all sub-mW transceiver IC designs in Fig. 2 employ either FSK, single carrier PSK, or non-coherent energy detection based schemes such as on-off keying to achieve the lowest power consumption given a target sensitivity level. The state-of-the-art 2.4GHz carrier frequency ULP FSK, PSK, energy-detection receiver designs [17], [18], [19] respectively report 350μW, 2.4mW, and 415μW power consumption for $\geq$-86dBm, -92dBm, and -87dBm sensitivity with 1Mbps, 2Mbps, and 250kbps data rate. Meanwhile,

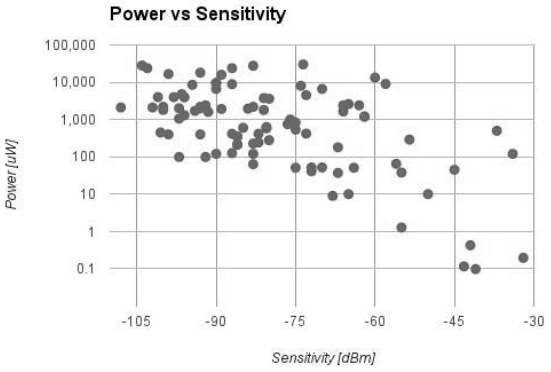

Fig. 2. ULP radio survey. Sensitivity vs Power consumption tradeoff.

commercial / academic WiFi OFDM ICs [6] - [8] aim for a very different class of applications where tens of Mbps data rates are necessary, and hundreds of mW power consumption is affordable. The proposed back-channel communication provides an unique engineering solution to bridge the power and data rate mismatch between the WiFi and ULP IoT devices. We will discuss in Section IV potential architectures to realize ULP back-channel receivers that could operate with less than a few mW of power budget to demodulate PPM, PPSK, or FSK messages embedded in WiFi OFDM packets.

We will discuss in-depth theoretical analysis on bit error rate (BER) performance for various back-channel communication modulation schemes. Realistic multi-path frequency selective fading channels are applied to derive back-channel BER expressions in Section V. The BER performance analysis reveals that back-channel modulation schemes can provide significant signal-to-noise ratio (SNR) gain over conventional WiFi OFDM by lowering the effective symbol rate and con-

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JSAC.2016.2612078, IEEE Journal on Selected Areas in Communications

centrating the OFDM symbol power on intentionally generated sparse pulses (PPM and PPSK). In other words, SNR gain is achieved by utilizing the full 20MHz WiFi bandwidth to realize much lower data rate for back-channel communication. ULP back-channel receivers can exploit this SNR gain to achieve significantly longer link distance and/or lower power consumption than what conventional WiFi OFDM communication can offer.

We envision that the proposed back-channel technique can be best utilized as a wireless paging / wakeup / interrupt channel empowered by already deployed legacy WiFi devices as depicted in Fig. 1 - (b). The back-channel signaling allows an existing WiFi device to control heterogeneous ULP devices that employ various types (e.g., PPM, PPSK, FSK, etc.) of back-channel receivers with a dramatically lower power budget than what a conventional WiFi receiver requires. The proposed back-channel technique also provides a unique solution to realize the concept of 'WiFi on-demand', in which the power-demanding OFDM receiver stays in deep-sleep, rather than continuously searching for randomly arriving packets, until it is asynchronously (and remotely) activated by the paging / wakeup message delivered to an always-on ULP back-channel receiver.

This paper is organized as follows. In section II, we discuss general procedures to create back-channel modulations embedded in OFDM packets. Section III presents systematic algorithms to general back-channel messages complying with the WiFi standard datapath. Potential ULP architectures for WiFi back-channel receivers are proposed in Section IV. Section V provides in-depth BER analysis of various WiFi back-channel modulation schemes. In section VI, we evaluate WiFi back-channel modulation schemes with BER simulations and analysis results. Section VII concludes the paper.

II. Back-Channel Modulations Realized in OFDM

In OFDM, the information bits are modulated using a linear modulation scheme such as quadrature amplitude modulation (QAM) on each subcarrier with equal average power, resulting in a white (or flat) frequency spectrum power spectral density (PSD) over the channel bandwidth. This whiteŹ PSD property makes the OFDM time domain signal appear as an uncorrelated noise-like signal with relatively high peak-to-average power ratio (PAPR). This high PAPR, in fact, is one of the major drawbacks of OFDM [20] since it requires highly linear RF circuits over a wide dynamic range to avoid unintended signal quality degradation from non-linear distortion. In this section, we discuss pulse based back-channel modulation techniques that utilize the high-PAPR OFDM property as a controlled modulation scheme for communication. In addition, a frequency domain back-channel modulation scheme that intentionally creates non-uniform PSD to emulate FSK is discussed in this section.

A. Pulse Position Modulation (PPM) Back-Channel

The pulse position modulation (PPM) back-channel uses the position of pulses (≥1 pulse per OFDM symbol) to convey back-channel messages. Since the SNR of the PPM back-channel is enhanced by maximizing the power of the intentionally created back-channel pulse, the PPM back-channel communication purposely maximizes the PAPR of the OFDM time domain signal. Fourier transform theory [21] indicates that the PAPR of an OFDM symbol is maximized by assigning linear modulation symbols on subcarriers with a constant phase rotation rate across all subcarriers as in (1).

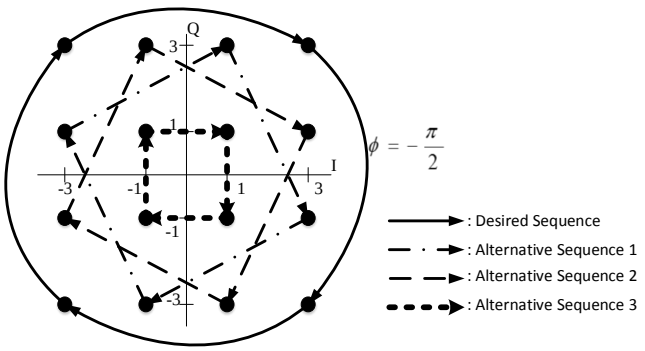

Fig. 3. Back-Channel pulse generating symbol sequence examples using 16-QAM

$$X_k = X_{k-1}e^{j\phi}, \quad Q_k = q(X_k), \quad k = 1, 2, ..., K \qquad (1)$$

In (1), ϕ is the constant phase rotation rate, k is the subcarrier index, K is the total number of subcarriers, Q_k is the linear modulation (e.g., QAM) symbol on the subcarrier k, $q(X)$ is the mapping from a complex number X to the nearest valid linear modulation symbol, and X_1 is the starting subcarrier symbol chosen from the set of valid linear modulation symbols. The inverse discrete Fourier transform (IDFT) on the set of Q_k, $k = 1, 2, ..., K$ results in a high-PAPR time domain OFDM symbol containing a pulse exemplified by Fig. 4.

By selecting a specific ϕ in (1), one can adjust the position of a pulse within a time-domain OFDM symbol. A binary PPM embedded in OFDM is realized by using two pulse positions; pulse 0 or pulse 1 resulting from phase rotation rates of ϕ_{p0} and ϕ_{p1} respectively, and by selecting one of two pulses depending on the message to be conveyed in back-channel modulation. The time difference between two possible pulse positions is given by $\frac{3.2|\phi_{p0}-\phi_{p1}|}{2\pi}\mu s$ for IEEE 802.11 a/g/n 20MHz legacy modes. Take an example of two distinct pulse positions generated by $\phi_{p0} = -\pi$ for pulse 0, and $\phi_{p1} = -\pi/2$ for pulse 1 and assigning a common starting symbol X_1 for both pulse positions. For the linear modulation on each subcarrier, we use a 16-QAM example as shown in Fig. 3 with $\{\pm 3 \pm 3j,\ \pm 1 \pm 1j,\ \pm 3 \pm 1j,\ \pm 1 \pm 3j\}$ constellation. A time domain WiFi OFDM symbol pair with this binary PPM back-channel modulation example is shown in Fig. 4 where two pulse positions were activated by using $\phi_{p0} = -\pi$, $\phi_{p1} = -\pi/2$, and $X_1 = 3 + 3j$ on the actual WiFi standard compliant datapath. It is possible to generate a longer pulse with lower peak power using a dithering phase rotation rate. Notice non-zero power, noise-like samples at non-pulse positions in Fig. 4, although the procedure given

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JSAC.2016.2612078, IEEE Journal on Selected Areas in Communications

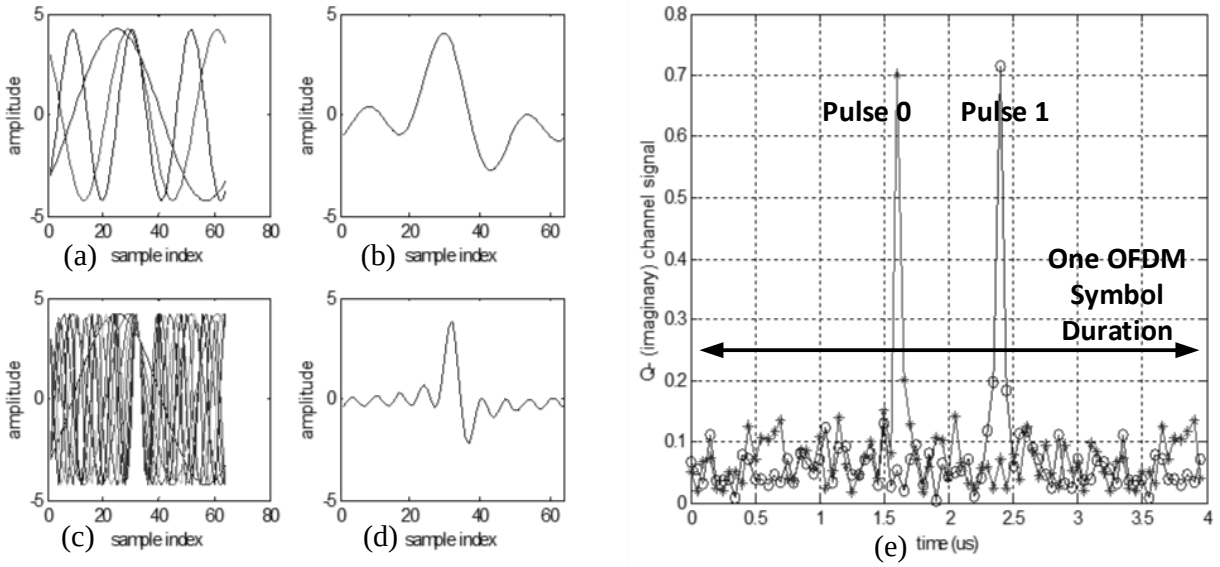

Fig. 4. Realization of binary PPM back-channel modulation. (a) $\phi = \pi$, $X_1 = 3 + 3j$, $X_i cos(2\pi ik/K)$, $i = 1, 2, 3$; (b) plot of $\sum_{i=1}^{3} X_i cos(2\pi ik/K)$; (c) $\phi = \pi$, $X_1 = 3 + 3j$, plot of $X_i cos(2\pi ik/K)$, $i = 1, 2, ..9$; (d) plot of $\sum_{i=1}^{9} X_i cos(2\pi ik/K)$; (e) plot of $|\sum_{i=0}^{K-1} X_i cos(2\pi ik/K)|$, $\phi = -\pi$ for pulse 0, $\phi = -\pi/2$ for pulse 1.

by (1) is supposed to create an ideal pulse with zero samples at all non-pulse positions. This non-ideality is originated from the fact that a WiFi compliant datapath requires mandatory convolutional coding and null / pilot subcarriers that prevent using the exact ideal sequence dictated by (1).

One of the central challenges of back-channel modulation is to identify a subset of unique bit sequences that create desired back-channel signals within strict constraints of the standard compliant packet structure. We will introduce in Section III a systematic algorithm to circumvent this issue and to create back-channel modulation from the WiFi compliant datapath with insignificant deviation from the ideal sequence given by (1).

In the binary PPM format, the back-channel message bit $b = 0$ can be transmitted by the pulse 0 while $b = 1$ is represented by the pulse 1. Extension to M-ary PPM back-channel modulation is straightforward. The back-channel PPM pulse rate is the same as the OFDM symbol rate. That is, 250k pulses per second for 20MHz bandwidth IEEE 802.11a/g/n WiFi operation. The primary advantage of this scheme is that even an ULP, non-coherent receiver can detect and demodulate these PPM modulated symbols, thus it allows communication between an OFDM transmitter and an non-OFDM (e.g., envelope detector based) ULP receiver on the energy- / power-constrained device.

B. Pulse Phase Shift Keying (PPSK) Back-Channel

By controlling the starting symbol X_1 in the subcarrier modulation assignment rule in (1), one can adjust the phase of a pulse in an OFDM time domain symbol. An M-ary pulse phase shift keying (PPSK) back-channel is realized by employing M pulses; pulse 0, ..., pulse $M - 1$ that have the same pulse position (i.e., a common phase rotation rate ϕ) but distinct pulse phases dictated by a non-overlapping starting symbols $X_1^{(m)}$ for each pulse m. For example, $\phi = -\pi/2$ with different initial phases; $X_1 = 3+3j$ for pulse 0 and $X_1 = -3-3j$ for pulse 1 create a binary PPSK modulated back-channel where the phase of a pulse conveys a binary back-channel message bit. The corresponding binary PPSK back-channel example of a time domain WiFi OFDM symbol pair (showing imaginary part only) is shown in Fig. 5. The non-zero, noise-like samples at non-pulse positions in Fig. 5 are because of the restrictions on a WiFi standard compliant datapath preventing arbitrary sequence mapping. Fig. 5 is a realization of the

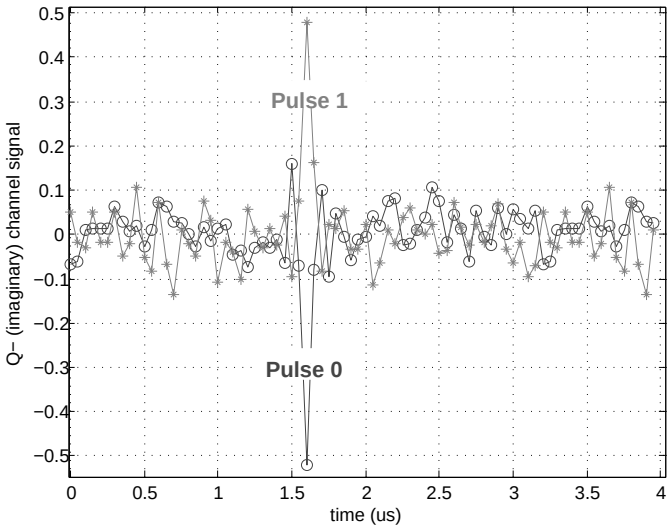

Fig. 5. Realization of binary PPSK back-channel modulation.

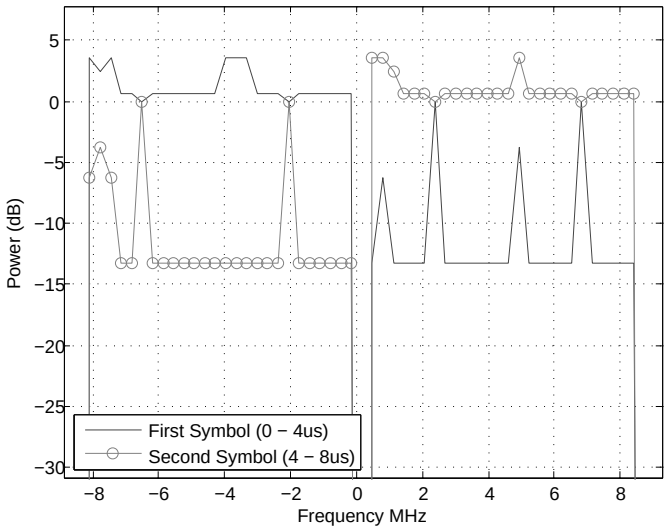

Fig. 6. Realization of binary FSK back-channel modulation.

systematic Algorithm 1 in Section III, which is designed to mitigate restrictions of a WiFi compliant datapath.

C. Frequency Shift Keying (FSK) Back-Channel

The OFDM back-channel can also be realized in a frequency shift keying (FSK) modulation format. We propose intentional, non-uniform linear modulation symbol power allocation across OFDM subcarriers to generate the FSK modulated back-channel. For an M-ary FSK modulation, we define M non-overlapping subsets of subcarrier indices $\mathcal{S}_{SC}^{(0)}$, $\mathcal{S}_{SC}^{(1)}$, ..., $\mathcal{S}_{SC}^{(M-1)}$ satisfying that cardinality of $\mathcal{S}_{SC}^{(m)}$ is $\frac{M}{K}$ for all m, $\mathcal{S}_{SC}^{(m)} \cap \mathcal{S}_{SC}^{(n)} = \emptyset$ for $m \neq n$, and $\mathcal{S}_{SC}^{(0)} \cup \mathcal{S}_{SC}^{(1)} \cup \ldots \cup \mathcal{S}_{SC}^{(M-1)} = \{1, 2, , \ldots K\}$. A back-channel M-ary FSK symbol m is conveyed by allocating higher power symbols to subcarriers in the subset $S_{SC}^{(m)}$ while lower power is assigned to all other subcarriers. For a binary FSK example, one can use $\mathcal{S}_{SC}^{(0)} = \{1, 2, \ldots, \frac{K}{2}\}$ and $\mathcal{S}_{SC}^{(1)} = \{\frac{K}{2}+1, \frac{K}{2}+2, \ldots, K\}$.

Fig. 6 shows a realization of an FSK back-channel OFDM symbol pair in the frequency domain, where two back-channel data bits are modulated by allocating higher power to $\mathcal{S}_{SC}^{(0)}$ for the first OFDM symbol, and higher power to $\mathcal{S}_{SC}^{(1)}$ for the second OFDM symbol. The 64-QAM subcarrier symbol constellation was used to realize the example shown in Fig. 6. Non-ideal power allocation within the set $\mathcal{S}_{SC}^{(0)}$ or $\mathcal{S}_{SC}^{(1)}$ is because of the restrictions on a WiFi compliant datapath that include mandatory convolutional coding and null/pilot subcarriers. Fig. 6 is the result of Algorithm 2 in Section III, that is proposed to minimize the impact of WiFi compliant datapath restrictions. The data rate of the binary FSK modulated back-channel is 250kbps when the WiFi bandwidth is 20MHz and each OFDM symbol is $4\mu s$ long in time (IEEE 802.11a/g/n legacy mode).

III. Back-Channel Modulations in Standard-Compliant WiFi Packets

Thus far, it was assumed that an arbitrary sequence of linear modulation symbols satisfying (1) and/or intentional non-uniform power could be allocated to OFDM subcarriers to generate the desired back-channel modulated signals embedded in OFDM packets. The IEEE 802.11 a/g/n WiFi standard datapath shown in Fig. 7, however, does not allow an arbitrary sequence of linear modulation symbols. The input data bit stream is scrambled, and encoded with a convolutional code. The coded bit sequence is then punctured, interleaved, and finally mapped to linear modulation symbols in the WiFi standard datapath. The linear modulation on each subcarrier is either BPSK, QPSK (4-QAM), 16-QAM, or 64-QAM. Some subcarriers are assigned as pilot and null subcarriers with predefined modulation symbols. Therefore, only a subset of all possible QAM symbol sequences is WiFi standard compliant. The proposed method circumvents this issue using the fact that the scrambler, interleaver and QAM mapper in WiFi standards are all one-to-one mapping invertible functions. The puncturing operation can be disabled in some WiFi modes without affecting the bit sequence. Even if the puncturing is enabled, the back-channel modulation process can simply allocate arbitrary bits on punctured bits as they will be eventually removed before the QAM mapping. In fact, it is only the convolutional encoder and the deterministic null/pilot subcarrier mapping that prevent creating an arbitrary sequence of QAM symbols. The convolutional encoder output has to be a valid codeword, which is a subset of all possible bit sequences.

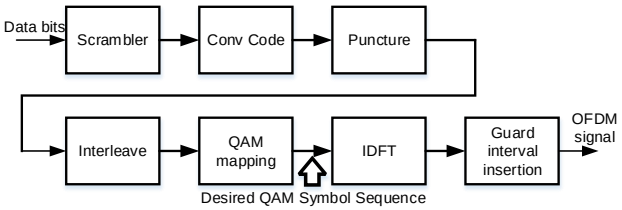

Fig. 7. IEEE 802.11 a/g/n WiFi modulation datapath

A. Pulse Based Back-Channel Modulation Using WiFi Datapath

The property of a back-channel modulated pulse within an OFDM symbol is determined by the constant phase rotation rate ϕ and the initial symbol X_1 in (1). Once an OFDM symbol is assigned with a specific ϕ and X_1 for pulse-based back-channel modulation, the *desired* QAM symbol sequence for all subcarriers within an OFDM symbol; Q_1, Q_2, ..., Q_K are obtained by (1). In general, this *desired* QAM symbol sequence is infeasible to be realized in a WiFi compliant datapath. We propose a systematic procedure specified in Algorithm 1 that utilizes multiple (R) alternative QAM symbol sequences with the same ϕ but with different starting symbols $X_1^{(r)}$ as depicted in Fig. 3. R alternative sequences are generated with the rule of $|X_1^{(1)} - X_1| \leq |X_1^{(2)} - X_1| \leq \ldots \leq |X_1^{(R)} - X_1|$. Algorithm 1 allows deviation from the *desired* QAM symbol sequence and temporary switching to one of alternative sequences if that is necessary to enforce the resulting sequence is standard compliant. The alternative sequences are sorted in the order of

minimizing the impact of deviation from the desired sequence. Algorithm 1 specifies the detailed procedure to produce pulse-based (PPM or PPSK) back-channel modulation complying with WiFi standards.

Algorithm 1 WiFi Data Bit Assignment for Pulse Based Back-Channel Modulation

1. A WiFi packet must start with mandatory header bits and service bits. The first OFDM data symbol is encoded using header bits. The second OFDM data symbol consists of service bits and arbitrary padding bits. The exact state of the scrambler and convolutional encoder after the second OFDM data symbol modulation is recorded for back-channel modulation starting from the third OFDM data symbol.
2. For a back-channel modulated OFDM symbol, the *desired* sequence of QAM symbols is generated using (1).
3. Generate multiple (R) alternative QAM symbol sequences with the same ϕ but with a different starting symbols $X_1^{(r)}$ satisfying $|X_1^{(1)} - X_1| \leq |X_1^{(2)} - X_1| \leq \ ... \ \leq |X_1^{(R)} - X_1|$.
4. For both desired and alternative sequences, QAM symbols that belong to pilot or null subcarriers are replaced by WiFi standard defined pilot and null symbols.
5. Desired and alternative sequences are converted to corresponding bit sequences at the convolutional encoder output (Fig. 7) using inverse operations of QAM mapping, interleaving, and puncturing. These bit sequences are denoted by the desired coded-bit sequence and alternative coded-bit sequences.
6. N_{SI} bits at the scrambler input are required to create an OFDM symbol. These data bits, b_j, $j = 0, 1, ... N_{SI} - 1$, are sequentially determined from the lowest index $j = 0$. Each b_j has two possible values; 0 or 1.
while $j < N_{SI}$ **do**
  if $b_j = b^*$, $b^* \in \{0, 1\}$ maps to the desired coded bit sequence after scrambling and convolutional encoding **then**
    7-a. $b_j \leftarrow b^*$.
  else {neither $b_j = 0$ nor 1 maps to the desired coded bit sequence}
    7-b. b_j is assigned with the value that provides an alternative coded bit sequence with smallest index r. If all alternative coded bit sequences are infeasible, b_j is assigned with a random value.
  end if
  8. Update the state of the scrambler and convolutional encoder according to b_j.
  9. $j = j + 1$
end while
10. Repeat from the step **2** if there are more back-channel symbols to be modulated. If not, quit.

We validated the effectiveness of Algorithm 1 not only with MATLAB simulations but also using a commercial off-the-shelf WiFi transceiver chipset, Texas Instruments CC3100 [6]. The data bit sequence obtained from Algorithm 1 is applied after the WiFi mandatory short training fields (STF), long training fields (LTF), physical layer header, and mandatory service bits of a WiFi packet. Thus, back-channel pulses appear from the seventh (after two STF symbols, two LTF, one OFDM symbol for header bits, and the other OFDM symbol for mandatory service bits) OFDM symbol as shown in Fig. 8. The last two OFDM symbols are excluded from back-channel modulation since they contain mandatory padding and frame check sequence (FCS) bits automatically appended by the transmitter. A pair of MATLAB simulated back-channel pulses within an OFDM symbol are shown in Fig. 4 and Fig. 5 in more details.

The proposed Algorithm 1 is based on a heuristic method. We observed that $R = 4$ alternatives are sufficient when underlying modulation is 16-QAM to generate a pulse $\approx 16dB$ stronger than the average symbol power. Increasing this peak power further would be unnecessary since the maximum peak-to-average power ratio of the WiFi transmitter power amplifier (typically $\leq 15dB$) would be the limiting factor, not the proposed algorithm.

It is worth noting that all non-idealities introduced by Algorithm 1 are incorporated in the BER performance analysis discussed in Section V. The data rate of the binary PPM/PPSK modulated back-channel shown in Fig. 4, Fig. 5, and Fig. 8 is 250k bits/s. The maximum number of back-channel modulated data bits per packet is the same as the maximum number of OFDM symbols within a packet (e.g., up to 340 bits for 16-QAM modulated IEEE 802.11g WiFi).

B. FSK Based Back-Channel Modulation using WiFi Datapath

The ideal M-ary FSK back-channel modulation on OFDM requires controlling symbol power on M non-overlapping subsets of subcarrier indices $\mathcal{S}_{SC}^{(0)}$, $\mathcal{S}_{SC}^{(1)}$, ..., $\mathcal{S}_{SC}^{(M-1)}$ as described in Section II. Although ideal M-ary FSK modulation is infeasible due to WiFi datapath restrictions, a systematic method described in Algorithm 2 circumvents this issue to generate approximated FSK back-channel modulation that is compliant with WiFi standards.

We denote $\mathcal{Q}_k$ as the set of all possible QAM symbols that can be assigned to the subcarrier k. High order QAM constellations such as 64-QAM are recommended to maximize the power difference between the high and low power subcarriers. The $\mathcal{Q}_k$ contains all valid QAM symbols initially. The number of entries in $\mathcal{Q}_k$ decreases as a result of sequentially specifying QAM mapping input bits following procedures in Algorithm 2. Each QAM mapping input bit assignment for the subcarrier k reduces the size of $\mathcal{Q}_k$ by the factor of $\frac{1}{2}$. The size of $\mathcal{Q}_k$ becomes 1 once all QAM mapping input bits for the subcarrier k are specified.

The back-channel modulation is the process of determining N_{SI} scrambler input bits, $b_0, ..., b_{N_{SI}-1}$, for each OFDM symbol. In Algorithm 2, each scrambler input bits are evaluated with a cost function that returns higher value when the input bit results in further deviation from the desired QAM symbol power allocation. Algorithm 2 assumes the binary FSK modulation assigning higher power to $\mathcal{S}_{SC}^{(high)}$ and lower power to $\mathcal{S}_{SC}^{(low)}$ while $\mathcal{S}_{SC}^{(high)} \cup \mathcal{S}_{SC}^{(low)} = \{1, 2, ..., K\}$ and $\mathcal{S}_{SC}^{(high)} \cap \mathcal{S}_{SC}^{(low)} = \emptyset$. Fig. 6 shows binary FSK back-channel modulated OFDM symbols in frequency domain generated

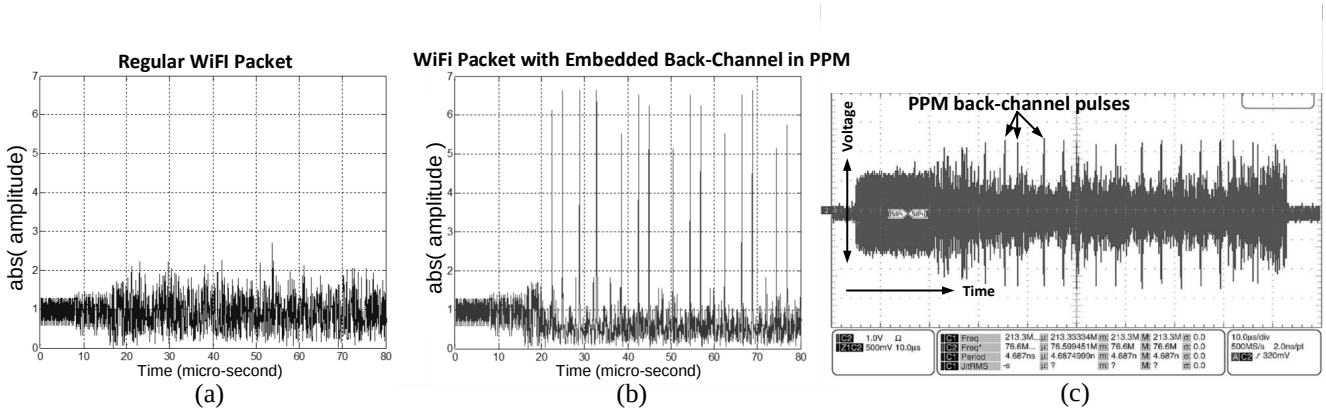

Fig. 8. Pulse-based back-channel modulation on WiFi packets using Algorithm1. (a) a conventional WiFi packet; (b) a MATLAB simulated WiFi packet with PPM back-channel modulation; (c) a WiFi packet from a commercial transceiver chipset with embedded PPM back-channel modulation.

using Algorithm 2. The presence of pilot and null subcarriers is clearly noticeable in Fig. 6. The impact of non-ideal FSK power allocation is included in the BER performance evaluation discussed in Section V. The extension of Algorithm 2 to M-ary FSK back-channel is straightforward.

Algorithm 2 WiFi data bit assignment for FSK back-channel modulation. A binary-FSK example assigning higher power to $\mathcal{S}_{SC}^{(high)}$ and lower power to $\mathcal{S}_{SC}^{(low)}$.

1. A WiFi packet must start with mandatory header bits and service bits. The back-channel modulation starts from the third OFDM data symbol.

2. For a back-channel modulated OFDM symbol, the scrambler input bits b_j are determined sequentially from $j = 0$ to $j = N_{SI} - 1$. The index j is initialized to 0. Q_k for all k is initialized to the set of all possible QAM symbols.

for $(j = 0;\ j < N_{SI};\ j = j + 1)$ **do**

3. Construct $Q_k^{b_j=0\ |\mathbf{b_{j-1}}}$ and $Q_k^{b_j=1\ |\mathbf{b_{j-1}}}$; the set of all possible QAM symbols that can be assigned to the subcarrier k when $b_j = 0$ and $b_j = 1$ respectively, given $\mathbf{b_{j-1}} = [b_0, \ \dots, b_{j-1}]$ from the result of previous steps.

4. Evaluate C_0 and C_1 where $C_b = \sum_{\forall k \in \mathcal{S}_{SC}^{(high)}} (P_{MAX} - max\{|Q_k^{b_j=b\ |\mathbf{b_{j-1}}}|^2\}) + \sum_{\forall k \in \mathcal{S}_{SC}^{(low)}} (min\{|Q_k^{b_j=b\ |\mathbf{b_{j-1}}}|^2\} - P_{MIN})$, P_{MAX} (or P_{MIN}) is the maximum (or minimum) QAM symbol power among all valid QAM symbols, $|Q|^2$ is element-wise QAM symbol power on a set Q and $max\{Q\}$ (or $min\{Q\}$) is the operation to select the maximum (or minimum) in a set Q.

if $C_0 < C_1$ **then**

5. $b_j \leftarrow 0$

else

6. $b_j \leftarrow 1$

end if

7. Update the state of the scrambler and convolutional encoder states according to b_j.

end for

8. Repeat from step **2** if there are more back-channel symbols to be modulated. If not, quit.

IV. Low Power, WiFi Back-Channel Receiver Architectures

One of main motivations of the back-channel modulation is to realize ULP receivers with dramatically reduced power consumption compared to a conventional OFDM receiver. Power demanding quadrature demodulation, a high accuracy RF local oscillator (LO) phase-lock loop (PLL), and DFT/FFT baseband processing are all unnecessary for PPM based back-channel demodulation. In this section, we propose receiver architectures that are suitable for extremely power-limited, non-WiFi compliant ULP devices to demodulate back-channel signals embedded in OFDM packets.

Fig. 9 depicts potential ULP receiver architectures for various types of back-channel modulations. The architectures shown in Fig. 9 (a) and (b) are designed for PPM back-channel signals. They are based on non-coherent signal envelope detection which does not require costly RF frequency synthesizers or mixers. The envelope of the signal is converted to digitally quantized levels to be processed in the digital baseband. Envelope detection is typically implemented with a rectifier or by self-mixing (squaring operation) followed by a low pass filter. The RF bandpass filter (BPF) and the amplifier are employed at the beginning of the datapath for interference rejection and out-of-band noise filtering. For further power consumption reduction, signal envelope detection and analog-to-digital converter (ADC) in Fig. 9 (a) can be replaced by a rectifier followed by a binary signal level comparator as shown in Fig. 9 (b) where pulse detection is performed entirely in analog circuits using a predefined pulse voltage bias (V_{bias}). Since the amplitude information is lost during analog one-bit comparator quantization, its bit error rate performance is expected to be significantly worse than that of the architecture employing an ADC (Fig. 9 (a)). Nonetheless, for applications that operate only in short distances, the architecture given in Fig. 9 (b) could be a compelling, energy-efficient solution. A ULP receiver design [22] that employs a similar rectifier based architecture reports $116nW$ power consumption.

Meanwhile, the PPSK back-channel receiver architecture proposed in Fig. 9 (c) utilizes the same RF / analog fron-

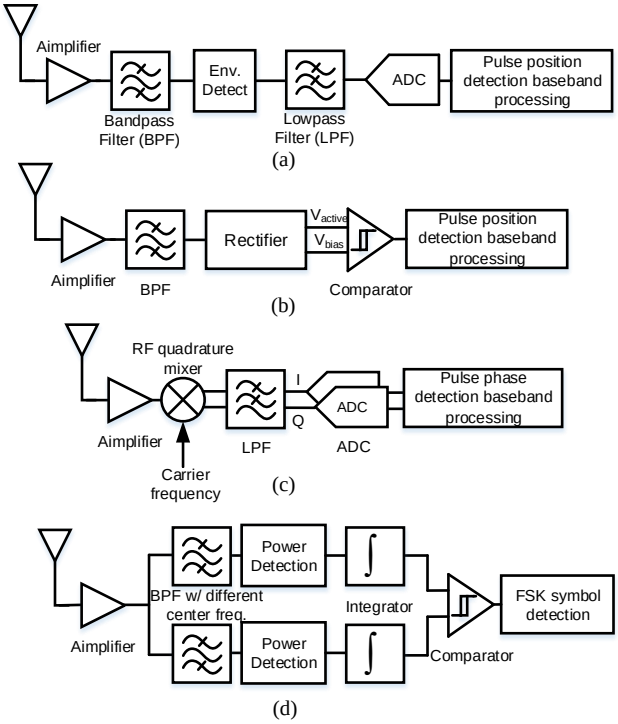

Fig. 9. OFDM back-channel receiver architectures. (a) Non-coherent PPM back-channel receiver; (b) Simplified, non-coherent PPM back-channel receiver; (c) coherent PPSK back-channel receiver; (d) Non-coherent FSK back-channel receiver.

tend for coherent quadrature demodulation that is required for conventional single-carrier PSK or OFDM demodulation. Unlike OFDM demodulation, the baseband signal processing for PPSK back-channel does not involve costly DFT/FFT computation and its symbol rate is at least 1/64 times lower than the OFDM signal bandwidth. Thus, its complexity (and power consumption) is significantly lower than that of a conventional WiFi OFDM receiver. Although its complexity is higher than that of non-coherent architectures designed for PPM back-channel, analysis in Section V and VI reveals that the PPSK back-channel has superior bit-error rate performance compared to PPM based back-channel modulation.

Fig. 9 (d) depicts the proposed ULP receiver architecture to demodulate the FSK modulated back-channel. This non-coherent receiver architecture consists of bandpass filters, power detectors, integrators (lowpass filters), and a comparator to detect power difference between two outputs from non-overlapping bandpass filters. The digital baseband processing produces the final demodulated bits by sampling the comparison output at the Nyquist rate. Note that this proposed architecture is also greatly simplified compared to a conventional OFDM receiver since it does not require RF LO frequency PLL, RF quadrature mixers, and DFT/FFT baseband processing for demodulation.

V. Back-Channel Communication Error Rate Performance Analysis

In this section, we analyze the error rate performance of the back-channel receivers discussed in Section IV. We assume non-coherent energy detector based architectures; Fig. 9 (a) and (d) with ideal circuits and filters for PPM and FSK back-channel BER evaluation respectively. The architecture Fig. 9 (c) with ideal components is assumed for PPSK back-channel performance analysis.

We use a multi-path (frequency selective) quasi-static Rayleigh fading channel model with exponentially decaying power profile, whereby the channel is static within the duration of a single packet but is independent from one packet to the next [23]. Discrete signal model with Nyquist sampling period $T_s = 50ns$ for 20MHz bandwidth operation is used throughout this section. The channel impulse response has the form of (2), where h_l is an i.i.d. zero-mean complex Gaussian random variable with variance $\sigma^2_{h_l}$ (3), l is the sample index, L is the channel length, and τ_{RMS} is the root-mean-squared (RMS) delay spread of the multi-path channel. Note that the average multi-path channel power is normalized so that $\sum_{l=0}^{L-1} \sigma^2_{h_l} = 1$.

$$h[n] = \sum_{l=0}^{L-1} h_l \delta[n-l], \quad \delta[n] = \begin{cases} 1, & n = 0 \\ 0, & n \neq 0 \end{cases} \tag{2}$$

$$\sigma^2_{h_l} = \frac{e^{\frac{-lT_S}{\tau_{RMS}}}}{\sum_{i=0}^{L-1} e^{\frac{-iT_S}{\tau_{RMS}}}} \tag{3}$$

We first derive the conventional uncoded OFDM bit error rate (BER) for BPSK modulation on each subcarrier to make a comparison with various back-channel modulation schemes. The DFT operation on the multi-path Rayleigh fading channel model (2) results in *statistically identical but correlated* Rayleigh fading channel for each subcarrier. The average unit power of the channel (3) indicates that the frequency domain channel coefficient for each subcarrier is a complex Gaussian random variable with unit variance. Uncoded system BER is dictated by the distribution of each individual subcarrier channel, and it is independent of correlation among subcarriers because bit errors on a certain subcarrier do not affect bit decisions on the other subcarriers. Although subcarrier channels are correlated, each individual subcarrier experiences the *statistically identical* Rayleigh flat fading channel [24]. Therefore, the BER of BPSK modulated OFDM subcarriers in our multi-path Rayleigh fading channel model (2) - (3) can be obtained by (4) [24] where $\sigma^2_N = 10^{-SNR/10}$ for a given SNR.

$$P^b_{e,OFDM-BPSK} = \int_0^\infty e^{-x} Q\left(\sqrt{\frac{2x}{\sigma^2_N}}\right) dx = \frac{1}{2}\left(1 - \sqrt{\frac{1}{\sigma^2_N + 1}}\right) \tag{4}$$

A. PPM Based Back-Channel Error Rate Performance

The average OFDM symbol power is assumed to be 1 without loss of generality. Binary back-channel PPM modulation creates a pulse that consists of a single complex sample, s,

located at one of two possible pulse positions within a time-domain OFDM symbol sampled at Nyquist rate. The pulse power is 16dB higher than the average OFDM symbol power (i.e., $10log_{10}|s|^2 = 16dB$) when the back-channel pulse is generated by the procedure described in Algorithm 1 for IEEE 802.11 a/g/n using 16-QAM subcarrier modulation. The WiFi datapath requirement and non-idealities involved in Algorithm 1 result in undesired noise-like samples, n^{TX} with an average power of $(\sigma_N^{TX})^2 = 1 - \frac{|s|^2}{K}$ at non-pulse sample positions. Thus, the PPM modulated back-channel transmit signal is represented by (5) assuming the pulse position is at the sample index 0. The received signal, $r_1[n]$, oriented at the correct pulse position, and $r_0[n]$ centered at the other incorrect pulse positions are represented by (6) where $\bar{n}_l^{TX} = \sum_{j=0}^{L} h_j n_{l-j}^{TX}$ is the transmitter generated noise arrived at the receiver through the channel and n_l^{RX} is the complex additive white Gaussian random noise added at the receiver with variance $(\sigma_N^{RX})^2 = 10^{-SNR/10}$ for a given SNR.

$$t_{PPM}[n] = \sum_{l=-L}^{L} \left(s\delta[n] + n_l^{TX}\delta[n-l] \right) \tag{5}$$

$$\begin{aligned} r_1[n] &= \sum_{l=0}^{L-1} \left(sh_l + \bar{n}_l^{TX} + n_l^{RX} \right) \delta[n-l], \\ r_0[n] &= \sum_{l'=0}^{L-1} \left(\bar{n}_l^{TX} + n_{l'}^{RX} \right) \delta[n-l'] \end{aligned} \tag{6}$$

In the non-coherent energy detector based receiver (i.e., Fig. 9 (a)), symbol detection error occurs when $R_1 = \sum_{l=0}^{L-1} |sh_l + \bar{n}_l^{TX} + n_l^{RX}|^2 < R_0 = \sum_{l'=0}^{L-1} |\bar{n}_l^{TX} + n_{l'}^{RX}|^2$. To make analysis simpler, we assume $\bar{n}_l^{TX}$ is an i.i.d. complex Gaussian random variable given a channel power instance $h_{PWR} = \sum_{l=0}^{L-1} |h_l|^2$. This assumption turns out to be reasonable as the simulation vs. analysis results are well matched (shown in Section VI). Now, we define an *effective* i.i.d. complex Gaussian noise $n_l = \bar{n}_l^{TX} + n_l^{RX}$ whose variance is $\sigma_N^2 = (\sigma_N^{TX})^2 h_{PWR} + (\sigma_N^{RX})^2$ given channel power h_{PWR}. Since h_l and n_l are both i.i.d. complex Gaussian random variables, the probability density function (pdf) of R_1 given h_{PWR} has a conditional non-central chi-square distribution, $p_{R_1}(x|h_{PWR})$, (7) [24] [25] where $I_a(b)$ is the modified Bessel function of the first kind. Whereas, R_0 is a chi-square distributed random variable, whose pdf, $p_{R_0}(x)$, is given by (8) [24][25] where $\Gamma(x)$ is the Gamma function.

$$\begin{aligned} p_{R_1}(x|h_{PWR}) = &\frac{1}{\sigma_N^2} \left(\frac{x}{|s|^2 h_{PWR}} \right)^{\frac{L-1}{2}} \cdot \\ &e^{-\frac{x+|s|^2 h_{PWR}}{\sigma_N^2}} I_{L-1}\left(\frac{2\sqrt{x|s|^2 h_{PWR}}}{\sigma_N^2} \right) \end{aligned} \tag{7}$$

$$p_{R_0}(x) = \frac{1}{\sigma_N^{2L}\Gamma(L)} x^{L-1} e^{-\frac{x}{\sigma_N^2}} \tag{8}$$

The h_{PWR} is a linear combination of chi-square random variables with non-equal variances conditioned by a given channel power delay spread profile (3). An analytical expression of its pdf, $p_{h_{PWR}}(x)$, can be obtained by using expressions in [26]. An alternative, more concise expression of $p_{h_{PWR}}(x)$ is (9) where $*$ stands for convolution. Applying (7), (8) and $p_{h_{PWR}}(x)$, the back-channel binary PPM bit error probability, $p_{e,PPM}^b$, is obtained by (10).

$$p_{h_{PWR}}(x) = \frac{1}{\sigma_{h_0}^2} e^{-\frac{x}{\sigma_{h_0}^2}} * \frac{1}{\sigma_{h_1}^2} e^{-\frac{x}{\sigma_{h_1}^2}} * \ldots * \frac{1}{\sigma_{h_{L-1}}^2} e^{-\frac{x}{\sigma_{h_{L-1}}^2}} \tag{9}$$

$$p_{e,PPM}^b = \int_0^\infty p_{h_{PWR}}(x) \int_0^\infty p_{R_1}(y|x) \int_y^\infty p_{R_0}(z) dz\, dy\, dx \tag{10}$$

B. Pulse PSK Based Back-Channel Error Rate Performance

M-ary PPSK modulated WiFi back-channel creates a pulse signal per OFDM symbol represented by (5). M-distinct possible phases for s, $\angle s \in \{\Phi_0, \Phi_1, ..., \Phi_{M-1}\}$, satisfy the relationship (11). We only consider binary PPSK back-channel modulation in this paper; $\Phi_0 = -\Phi_1$. Extension to M-ary PPSK back-channel is straightforward.

$$\Phi_j = \Phi_i 2\pi(j-i)/M \tag{11}$$

We assume perfect synchronization and a coherent detection architecture shown in Fig. 9 (c) to analyze the BER of the binary PPSK back-channel modulation. Applying the multi-path delay spread channel model given by (2), the received signal oriented at the correct pulse position is represented by $r[n] = \sum_{l=0}^{L-1} \left(sh_l + \bar{n}_l^{TX} + n_l^{RX} \right) \delta[n-l]$. We use the ideal matched filter, $r_{MF}[n] = \sum_{l=0}^{L-1} h_{L-l-1}^* \delta[n-l]$, that is obtained by estimating the channel response from multiple back-channel training symbols with predefined pulse phases. The average OFDM symbol power is assumed to be 1 without loss of generality, while $10log_{10}|s|^2 = 16dB$ and $(\sigma_N^{TX})^2 = 1 - \frac{|s|^2}{K}$ hold when the back-channel pulse is generated by Algorithm 1 for IEEE 802.11 a/g/n using 16-QAM subcarrier modulation. As we did for PPM error performance analysis, the *effective* noise $n_l = \bar{n}_l^{TX} + n_l^{RX}$ is modeled as an i.i.d. Gaussian complex random variable with variance $\sigma_N^2 = (\sigma_N^{TX})^2 h_{PWR} + (\sigma_N^{RX})^2$ given channel power h_{PWR}.

The PPSK back-channel symbol detection is performed on the matched filter output, $r[n] * r_{MF}[n]$, sampled at the correct back-channel pulse position. The binary PPSK detection error rate, $p_{e,PPSK}^b$, is equal to the probability of $|s|^2 \sum_{l=0}^{L-1} |h_l|^2 < \Re\left(\sum_{l=0}^{L-1} h_l^* n_l \right)$. Since $h_l^* n_l$ are i.i.d. complex Gaussian random variables with variance $\sigma_{h_l}^2 \sigma_N^2$, their sum, $\sum_{l=0}^{L-1} h_l^* n_l$ is also a complex Gaussian random variable with variance $\sum_{l=0}^{L-1} \sigma_{h_l}^2 \sigma_N^2 = \sigma_N^2$. Therefore, $p_{e,PPSK}^b$ can be represented by (12) using the expression of h_{PWR} pdf (9).

$$P_{e,PPSK}^b = \int_0^\infty p_{h_{PWR}}(x) Q\left(\sqrt{\frac{2|s|^2 x}{\sigma_N^2}} \right) dx \tag{12}$$

C. FSK Based Back-Channel Error Rate Performance

We use a frequency domain discrete signal model sampled at Nyquist rate (13) to derive binary FSK modulated WiFi back-channel error rate performance. In (13), k is the subcarrier index, Y_k is the frequency domain received signal, Q_k is

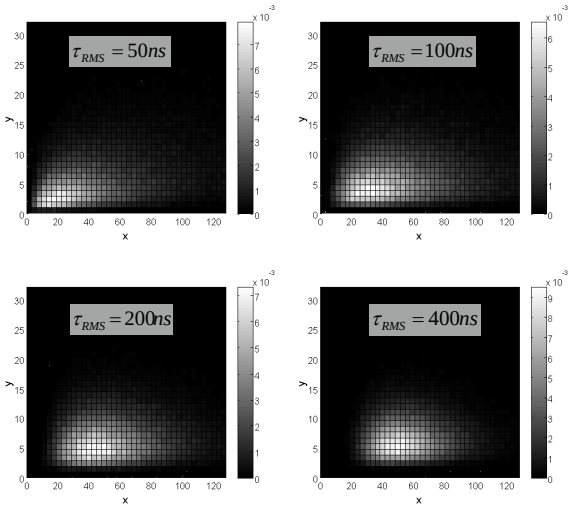

Fig. 10. Numerically evaluated pdf $p_{H_{PWR}^{(high)},H_{PWR}^{(low)}}(x,y)$ for $\tau_{RMS} = 50ns, 100ns, 200ns$, and $400ns$ using Algorithm 2 with IEEE 802.11a/g/n 54Mbps 64-QAM legacy mode (MCS 7)

the subcarrier symbol allocated as a result of FSK back-channel modulation, N_k is the frequency domain complex Gaussian noise whose variance is $(\sigma_N^{RX})^2$, and H_k is the frequency domain channel response obtained by performing K-point DFT (with $K-L$ zero-padding samples assuming $L \leq K$) on the channel impulse response (2). Note that noise samples N_k on different subcarriers are uncorrelated while H_k's are correlated according to the frequency selective multi-path channel model (2).

$$Y_k = H_k Q_k + N_k, \quad k = 1, ..., K \tag{13}$$

Consider binary FSK back-channel modulation that assigns higher power symbols to the subcarrier set $\mathcal{S}_{SC}^{(high)} = \{1, \ldots, \frac{K}{2}\}$ and lower power to $\mathcal{S}_{SC}^{(low)} = \{\frac{K}{2}+1, \ldots, K\}$. For a non-coherent energy detection based receiver (Fig. 9 (d)), demodulation error occurs when $Y_{PWR}^{(high)} = \sum_{k\in\mathcal{S}_{SC}^{(high)}} |Y_k|^2 < Y_{PWR}^{(low)} = \sum_{k\in\mathcal{S}_{SC}^{(low)}} |Y_k|^2$. Given $H_{PWR}^{(high/low)} = \sum_{k\in\mathcal{S}_{SC}^{(high/low)}} |H_k Q_k|^2$, $Y_{PWR}^{(high/low)}$ has a conditional non-central chi-square distribution, $p_{Y_{PWR}^{(high/low)}}(x|H_{PWR}^{(high/low)})$, (14).

$$p_{Y_{PWR}^{(high/low)}}\left(x|H_{PWR}^{(high/low)}\right) = \frac{1}{(\sigma_N^{RX})^2}\left(\frac{x}{H_{PWR}^{(high/low)}}\right)^{\frac{K/2-1}{2}} \cdot e^{-\frac{x+H_{PWR}^{(high/low)}}{(\sigma_N^{RX})^2}} I_{K/2-1}\left(\frac{2\sqrt{xH_{PWR}^{(high/low)}}}{(\sigma_N^{RX})^2}\right) \tag{14}$$

To obtain a detection error probability expression, we need a joint probability density function of $H_{PWR}^{(high)}$ and $H_{PWR}^{(low)}$ denoted by $p_{H_{PWR}^{(high)},H_{PWR}^{(low)}}(x,y)$. Note that $H_{PWR}^{(high)}$ and $H_{PWR}^{(low)}$ are correlated as a result of DFT operation on multi-path channel impulse response (2). Since it is difficult to obtain an analytical expression of $p_{H_{PWR}^{(high)},H_{PWR}^{(low)}}(x,y)$ when the channel delay spread $\tau_{RMS} > 0$ and subcarrier symbols, Q_k, are allocated by the non-ideal, WiFi compliant procedure in Algorithm 2, we evaluate $p_{H_{PWR}^{(high)},H_{PWR}^{(low)}}(x,y)$ from numerical simulations with various τ_{RMS}. Fig. 10 shows numerically obtained $p_{H_{PWR}^{(high)},H_{PWR}^{(low)}}(x,y)$ for various $\tau_{RMS} > 0$ using Algorithm 2 with the IEEE 802.11a/g/n 54Mbps 64-QAM legacy mode (MCS 7). Fig. 10 clearly indicates FSK back-channel modulation satisfies $H_{PWR}^{(high)} \gg H_{PWR}^{(low)}$ condition with high probability, especially in large τ_{RMS} channels where frequency diversity is more evident. Applying numerically obtained $p_{H_{PWR}^{(high)},H_{PWR}^{(low)}}(x,y)$ and (14), the bit error probability of binary FSK modulated back-channel, p_{FSK}^b is obtained by (15).

$$p_{FSK}^b = \int_0^\infty \int_0^\infty \int_0^\infty p_{H_{PWR}^{(high)},H_{PWR}^{(low)}}(x,y) p_{Y_{PWR}^{(high)}}\left(z|H_{PWR}^{(high)} = x\right) \int_z^\infty p_{Y_{PWR}^{(low)}}\left(w|H_{PWR}^{(low)} = y\right) dw\ dz\ dx\ dy \tag{15}$$

VI. Evaluation Results

A. Evaluation Packet Structure

The proposed back-channel scheme enables the packet-in-packet structure as depicted in Fig. 11. This packet structure allows sending messages to both a regular WiFi receiver and a back-channel receiver using a single WiFi packet. The message targeting a regular WiFi receiver is encoded in WiFi symbols in Fig. 11. One WiFi OFDM symbol contains numerous (at least 48) information bits, and its uncoded BER performance is governed by (4) for BPSK. These information bits contained in regular WiFi symbols are ignored by back-channel receivers. Meanwhile, each back-channel symbol in Fig. 11 contains only one information bit (assuming binary PPM, PPSK, or FSK back-channel) per OFDM symbol. These back-channel symbols are intended for back-channel receivers. The uncoded BER of these back-channel symbols can be obtained by (10), (12), and (15). It is worth noting that a regular WiFi receiver can demodulate OFDM symbol input bits (not back-channel information bits) contained in back-channel symbols as they are also valid OFDM symbols. Its BER would be the same as the conventional WiFi OFDM system. However, the decoded bits will be meaningless to regular WiFi receivers because the sole purpose of these bits is to modulate back-channel symbols, not to convey meaningful information for regular WiFi receivers. In order to ensure interoperability, it is desired to assign extra information bits in the WiFi symbol to indicate the presence of back-channel symbols in the packet so that a regular receiver can ignore back-channel modulated symbols for decoding. The pack-in-packet structure in Fig. 11 ends with a regular WiFi symbol which contains the cyclic redundancy check (CRC) bits for the entire packet. In this way, the entire packet is regarded as a valid WiFi packet by regular WiFi receivers without a CRC error.

B. Performance Evaluation

To validate the back-channel BER analysis, we compared Monte-Carlo MATLAB simulations with the analytical ex-

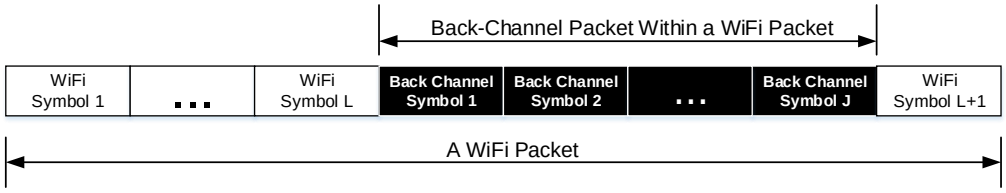

Fig. 11. Evaluated packet structure. A back-channel packet is embedded in a WiFi packet.

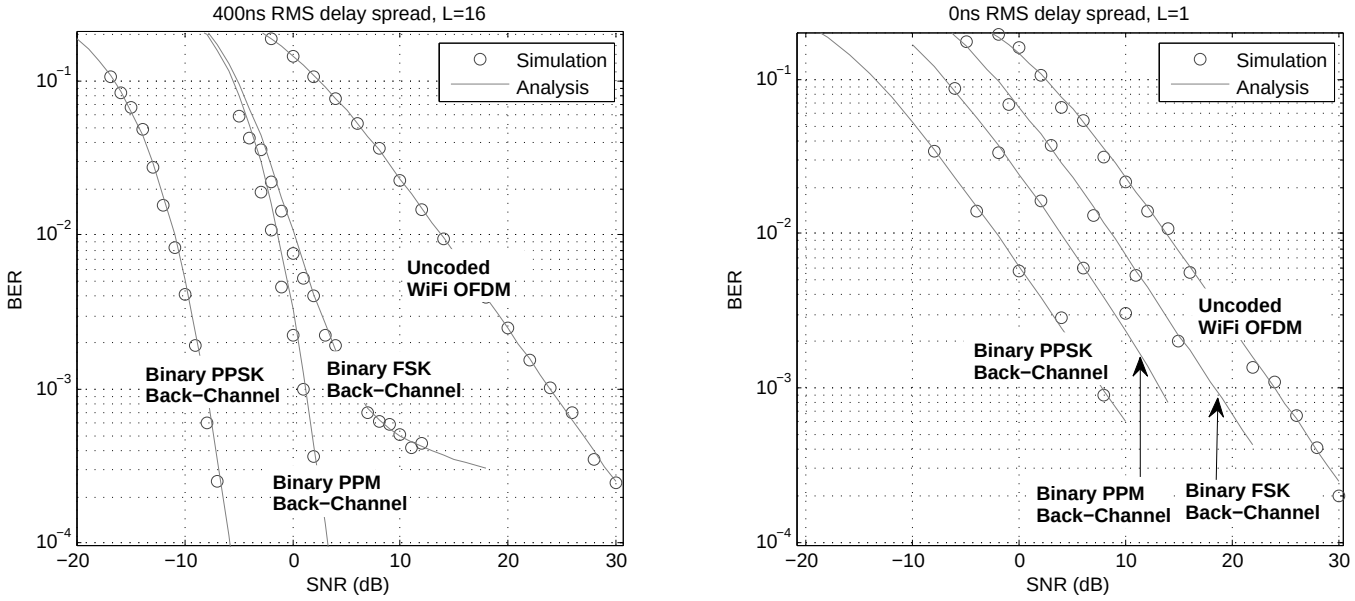

Fig. 12. Uncoded OFDM and back-channel BER performance, MATLAB simulations vs. analysis results. (a) in 400ns RMS delay spread channel; (b) in 0ns RMS delay spread channel.

pressions given by (4), (10), (12), and (15). Fig. 12 shows a side by side comparison of the BER performance, and it confirms that analysis results are well matched to the actual BER for various back-channel modulation schemes. The WiFi standards are designed to operate with up to 800ns (OFDM symbol guard interval length) of channel delay spread. We evaluated τ_{RMS} =0 (Rayleigh flat fading channel), 100, 200 and 400ns RMS delay spread channels with L =1, 5, 8 12, and 16 respectively.

Fig. 12 shows τ_{RMS} = 0 and 400ns results revealing that proposed back-channel modulation schemes can operate with lower SNR than what conventional WiFi OFDM requires. It is because the effective back-channel symbol rate is much lower than the OFDM bandwidth, and back-channel schemes aggregate OFDM symbol energy from 64 subcarriers to create a single back-channel symbol at lower symbol rate. This can be considered as de-spreading gain that is available in spreading spectrum modulation schemes. The back-channel signal bandwidth is 20MHz but the symbol rate is only 250kHz. The SNR gain from this energy concentration or de-spreading is approximately (not exactly because of WiFi compliant datapath requirements) $10log_{10}64 = 18dB$ which can be observed by comparing the BER performance between PPSK back-channel and conventional WiFi OFDM (uncoded) in the Rayleigh flat fading channel (Fig. 12 (b)). The BER performance gap is smaller for PPM and FSK back-channel schemes because they use sub-optimal non-coherent demodulation architectures. The BER performance gap increases for a non-zero delay spread channel (Fig. 12 (a)) because back-channel modulation schemes can exploit diversity gain from the multi-path channel with independent taps (2) while the uncoded OFDM does not. This significant SNR gain of back-channel schemes can be utilized to lower power consumption of the ULP back-channel receiver or to extend link distance beyond the conventional WiFi range.

Fig. 13 and Fig. 14 show the impact of channel delay spread on PPM and PPSK back-channel schemes respectively. Note that the conventional uncoded OFDM BER performance is independent of channel delay spread since all subcarriers experience statistically identical Rayleigh fading channels although they are correlated in frequency domain. On the other hand, PPM and PPSK back-channel schemes gain from multi-path diversity because each channel tap of (2) in the time domain has independent distribution. That is, a low power fading channel tap can be compensated by other high power channel taps with high probability when there are multiple independent fading channel taps in the channel impulse response. It is worth noting that the gain from longer channel response (larger L)

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JSAC.2016.2612078, IEEE Journal on Selected Areas in Communications

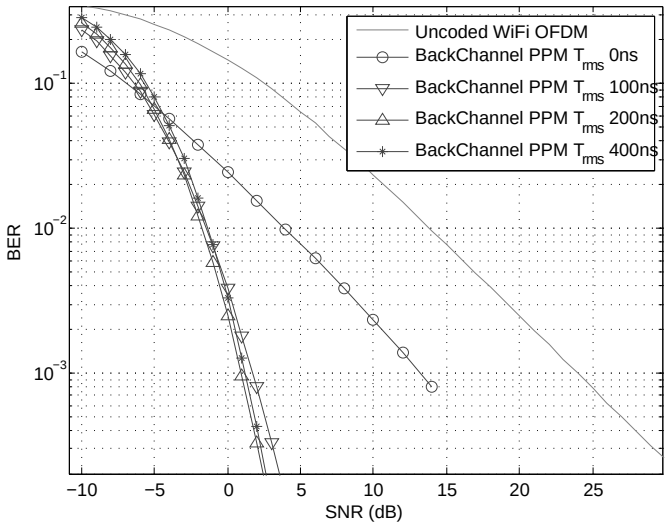

Fig. 13. PPM back-Channel BER performance in 0, 100, 200, and 400ns delay spread channels.

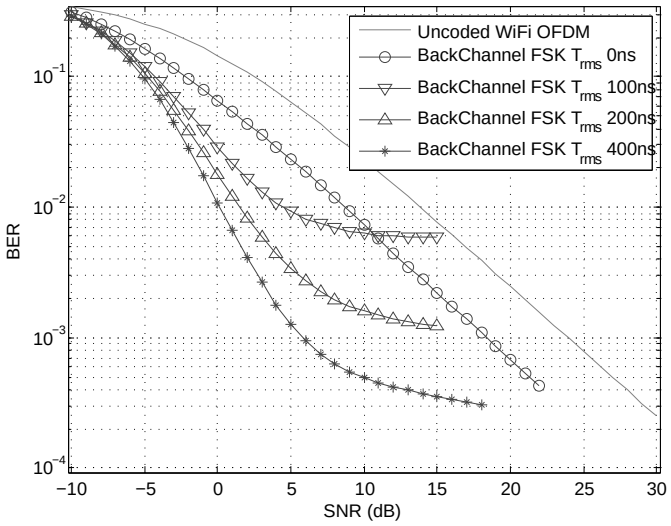

Fig. 15. FSK back-Channel BER performance in 0, 100, 200, and 400ns delay spread channels.

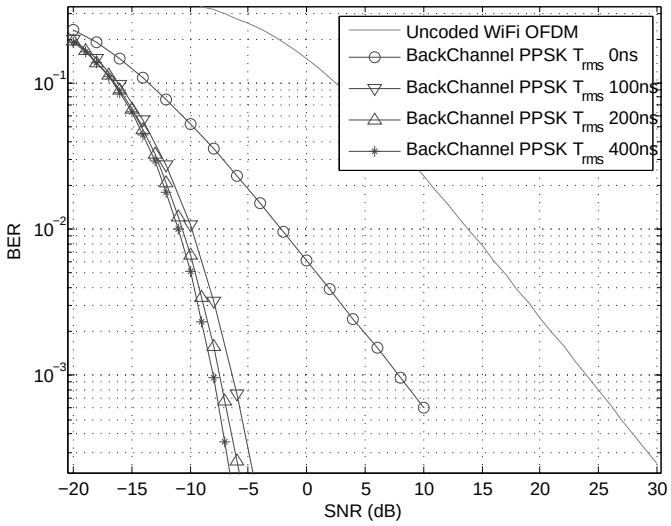

Fig. 14. PPSK back-Channel BER performance in 0, 100, 200, and 400ns delay spread channels.

is not necessarily monotonic. For instance, the 200ns delay spread channel has slightly better performance than the 400ns channel for PPM as shown in Fig. 13. The diversity gain diminishes for a large L because the average signal energy remains constant regardless of channel delay spread length in our channel model (2) - (3) while the noise energy observed for symbol detection linearly increases as a function of L.

Fig. 15 shows the BER performance of FSK back-channel modulation. Notice channel RMS delay spread dependent error floors (i.e. not improving BER for higher SNR) on the FSK back-channel BER plots. These error floors are because of frequency selectivity of the channel. When high power subcarriers encounter destructive fading, the FSK back-channel error probability increases. The shorter channel delay spread results in a wider channel coherence bandwidth, and consequently, the probability of many high power subcarriers suffering from destructive channel fading at the same time (whereas low power subcarriers see constructive channel fading) increases. In such a condition, the BER performance is limited by the statistical distribution of the frequency selective channel fading, not by SNR, resulting in error floors. The frequency flat fading channel does not create an error floor since both high and low power subcarriers experience the same fading, and back-channel symbol detection is performed by measuring the power difference. As channel delay spread increases, channel coherence bandwidth decreases with reduced correlation among subcarriers. Frequency diversity from longer channel delay spread, therefore, lowers the BER error floor for the FSK back-channel. It is whatorth noting that short length (e.g., 48-bit) back-channel messages for wakeup, paging, or control commands could be successfully communicated with a reasonable frame error rate when the BER is around 10^{-3}. In general, FSK back-channel communication will provide more robust performance in the additive white Gaussian channel (no fading) or in non-line-of-sight indoor channels with > 100ns RMS delay spread. In fact, IEEE 802.11n provides options to employ multiple transmit antennas with intentional cyclic time shift to create artificial channel delay spread and enhance frequency diversity [5]. Using multiple transmit antennas will improve robustness of FSK back-channel. For a single WiFi TX antenna system, PPM or PPSK back-channel modulation is recommended to operate in < 100ns RMS delay spread fading channels.

C. Proof of Concept Prototype

A micro-controller (MCU) based PPM back-channel receiver prototype was built and validated. For a proof-of-concept prototype, the RF frontend was assembled with discrete components from Mini-Circuits and a low power TI MSP430 MCU evaluation board [27] that is programmed to receive and decode PPM WiFi back-channel messages in real time. Fig. 16 shows the prototype receiver system architecture.

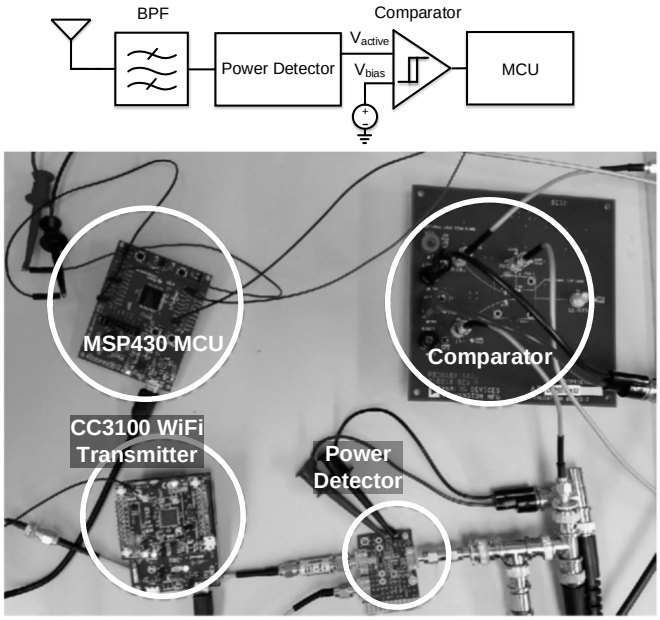

Fig. 16. Proof-of-Concept Prototype System for PPM WiFi Backchannel Reception.

An off-the-shelf power detector [28] outputs the instantaneous power of the 2.4 GHz WiFi signal and the comparator produces a digital pulse for the MCU whenever the power of the Wi-Fi signal exceeds a predefined threshold. The MSP430 MCU clock frequency of the prototype system is set to 25MHz clock, which is far insufficient to perform regular 20MHz WiFi OFDM demodulation. In the prototype system, the MCU only processes the timing information of the pulse detected by the power comparator, thus it is able to decode WiFi back-channel messages in real time using constrained resources available on the MSP430 MCU with low power consumption (7.5mW for the MSP430). Sensitivity measurement of the prototype system was conducted with a wired setup, where the WiFi transmitter CC3100 [6] is connected to the prototype receiver system via attenuators to test various levels of received signal power in a flat fading channel. For 32-bit back-channel messages, packet error rate $\leq 1\%$ was reported at the received signal power level of -55dBm for this primitive (sub-optimal) prototype system. This prototype system is sub-optimal in power consumption and sensitivity but it successfully validate the low cost and low power back-channel receiver concept. Designing a dedicated back-channel receiver with improved sensitivity and power efficiency is left as a future work.

VII. Conclusions

We presented innovative back-channel communication techniques for ultra-low power wireless devices, which could not afford standard WiFi wireless communication due to their extremely limited power budget. The concept of back-channel communication enables interconnecting heterogeneous ULP devices through existing ubiquitous WiFi networks even if these ULP devices are incapable of decoding regular WiFi messages. The back-channel signaling embedded in WiFi messages has unique properties that are easily detectable by ULP receivers operating with sub mW power budget.

The proposed back-channel scheme eliminates the need for specialized transmitter hardware or dedicated channel resources for embedded back-channel signal transmission. Instead, we have demonstrated that carefully sequenced data bit streams can generate back-channel messages from already-deployed WiFi infrastructure without any hardware modification. Various back-channel modulation formats such as PPM, PPSK or FSK were discussed in this paper.

Theoretical BER analysis revealed that back-channel modulation schemes provide significant SNR gains over the conventional uncoded WiFi OFDM modulation. The impact of various channel delay spread parameters were analyzed for each back-channel modulation type. Significant SNR gain of back-channel schemes over conventional OFDM can be utilized to lower power consumption of the ULP back-channel receiver or to extend link distance beyond the conventional WiFi range.

The proposed back-channel technique could make direct impact on the next wireless standardization to adopt more flexible packet structures to enrich use-cases of back-channel communication. WiFi standard compliant nodes could potentially benefit from the back-channel technique to significantly enhance their power efficiency without employing a proprietary wakeup signal transmitter and/or dedicated channel resources. Novel concepts such as WiFi-on-demand, replacing conventional always-on WiFi Access Points, can be realized by the outcomes of the proposed technique.

Acknowledgment

The authors would like to thank Huajun Zhang and Michael Kines for their contribution in testing back-channel using commercial WiFi chipsets. This work was funded in part by NSF Career Award 1253172 and NSF ECCS 1507192.

References

[1] I. Demirkol, C. Ersoy, E. Onur, "Wake-up receivers for wireless sensor networks: benefits and challenges," *Wireless Communications, IEEE*, vol.16, no.4, pp.88,96, Aug. 2009.

[2] L. Gu, J.A. Stankovic, "Radio-triggered wake-up capability for sensor networks," *Real-Time and Embedded Technology and Applications Symposium, 2004. Proceedings. RTAS 2004. 10th IEEE*, vol., no., pp.27,36, 25-28 May 2004.

[3] J. Ansari, D. Pankin, P. Mahonen, "Radio-Triggered Wake-ups with Addressing Capabilities for extremely low power sensor network applications," *Personal, Indoor and Mobile Radio Communications, 2008. PIMRC 2008. IEEE 19th International Symposium on*, vol., no., pp.1,5, 15-18 Sept. 2008.

[4] W. Yiyan, W.Y. Zou, "Orthogonal frequency division multiplexing: a multi-carrier modulation scheme," *IEEE Transactions on Consumer Electronics*, vol.41, no.3, pp.392-399, Aug 1995

[5] IEEE standards association, 802.11n specification, Available at: https://standards.ieee.org/findstds/standard/802.11n-2009.html

[6] Texas Instruments, CC3100 online datasheet, Available at: http://www.ti.com/product/CC3100/datasheet

[7] T.-M. Chen, Y.-M. Chiu, C.-C. Wang, K.-U. Chan, Y.-H. Lin, M.-C. Huang, C.-H. Lu, W.-S. Wang, C.-S. Hu, C.-C., Lee, J.-Z. Huang, B.-I Chang, S.-C. Yen, Y.-Y. Lin, "A Low-Power Fullband 802.11a/b/g WLAN Transceiver With On-Chip PA," *IEEE Journal of Solid-State Circuits*, vol.42, no.5, pp.983 - 991, May 2007

[8] M. Zargari, S. Jen, B. Kaczynski, M. Lee, M. Mack, S. Mehta, S. Mendis, K. Onodera, H. Samavati, W. Si, K. Singh, A. Tabatabaei, M. Terrovitis, D. Weber, D. Su, B. Wooley, "A single-chip dual-band tri-mode CMOS transceiver for IEEE 802.11a/b/g WLAN," *IEEE International Solid-State Circuits Conference, 2004. Digest of Technical Papers. ISSCC*, Vol.1, 15-19. Feb. 2004

[9] G. Chen, H. Ghaed, R. Haque, M. Wieckowski, Y. Kim, G. Kim, D. Fick, D. Kim, M. Seok, K. Wise, D. Blaauw, D. Sylvester, "A cubic-millimeter energy-autonomous wireless intraocular pressure monitor," *IEEE International Solid-State Circuits Conference, 2011. Digest of Technical Papers. ISSCC*, pp.310 - 312, 20-24 Feb. 2011.

[10] Y. Lee, G. Kim, S. Bang, Y. Kim, I. Lee, P. Dutta, D. Sylvester, D. Blaauw, "A modular 1mm3 die-stacked sensing platform with optical communication and multi-modal energy harvesting," *IEEE International Solid-State Circuits Conference, 2012. Digest of Technical Papers. ISSCC*, pp.402 - 404, 19-23 Feb. 2012.

[11] S. Tang, H. Yomo, Y. Takeuchi, "Optimization of Frame Length Modulation-Based Wake-up Control for Green WLANs," *IEEE Transactions on Vehicular Technology*, vol.PP, no.99, pp.1,1.

[12] N. E. Roberts et al., "26.8 A 236nW -56.5dBm-sensitivity bluetooth low-energy wakeup receiver with energy harvesting in 65nm CMOS," *2016 IEEE International Solid-State Circuits Conference (ISSCC)*, San Francisco, CA, 2016, pp. 450-451.

[13] H. Jiang and P. Wilford, "A hierarchical modulation for upgrading digital broadcast systems," *IEEE Transactions on broadcasting*, Vol. 51, No. 2 (2005), pp 223-229.

[14] S. Wang, S. Kwon and B.K. Yi, "On enhancing hierarchical modulation," *IEEE International Symposium on Broadband Multimedia Systems and Broadcasting*, March 31 2008-April 2 2008, Las Vegas, NV, (2008), pp. 1-6.

[15] H. Meric, J. Lacan, F. Arnal, G. Lesthievent, M.-L. Boucheret, "Combining Adaptive Coding and Modulation With Hierarchical Modulation in Satcom Systems," *IEEE Transactions on Broadcasting*, Vol. 59, No. 4 (2013), pp 627-637.

[16] D. D. Wentzloff, "Low Power Radio Survey," Available at: http://www.eecs.umich.edu/wics/wp-content/low_power_radio_survey.html

[17] J. Ayers, N. Panitantum, K. Mayaram, T.S. Fiez, "A 2.4GHz wireless transceiver with 0.95nJ/b link energy for multi-hop battery-freewireless sensor networks," *IEEE Symposium on VLSI Circuits (VLSIC) 2010*, pp.29 - 30, 16-18 June 2010

[18] Y.-H. Liu, A. Ba, J.H.C. van den Heuvel, K. Philips, G. Dolmans, H. de Groot, "9.5 A 1.2nJ/b 2.4GHz receiver with a sliding-IF phase-to-digital converter for wireless personal/body-area networks," *IEEE International Solid-State Circuits Conference, 2014*, pp.166 - 167, 9-13 Feb. 2014

[19] S. Drago, D.M.W. Leenaerts, F. Sebastiano, L.J. Breems, K.A.A. Makinwa, B. Nauta, "A 2.4GHz 830pJ/bit duty-cycled wake-up receiver with ?82dBm sensitivity for crystal-less wireless sensor nodes," *IEEE International Solid-State Circuits Conference, 2010*, pp.224 - 225, 7-11 Feb. 2010

[20] S.H. Muller, J.B. Huber, "OFDM with reduced peak-to-average power ratio by optimum combination of partial transmit sequences," *Electronics Letters*, vol.33, no.5, pp.368-369, 27 Feb 1997

[21] A. V. Oppenheim, A. S. Willsky, S. Hamid, *Signals and Systems*, Prentice Hall, 2nd Edition.

[22] S. Oh, N. E. Roberts, D. D. Wentzloff, "A 116nW multi-band wake-up receiver with 31-bit correlator and interference rejection," *IEEE Custom Integrated Circuits Conference (CICC)*, Sept. 2013, pp 1-4.

[23] I. Lee, A. M. Chan, and C.-E. W. Sundberg, "Space-Time Bit-Interleaved Coded Modulation for OFDM Systems," *IEEE Transactions on Signal Processing*, vol. 52, issue 3, pp. 820 - 825, Mar. 2004.

[24] J. Proakis, *Digital Communications*, New York: McGraw-Hill, 2001.

[25] S. Gishkori, G. Leus, H. Deliç, "Energy Detection of Wideband and Ultra-Wideband PPM," *IEEE Global Telecommunications Conference (GLOBECOM), 2010*, pp.1 - 5, 6-10 Dec. 2010.

[26] P.G. Moschopoulos, W.B. Canada, "The distribution function of a linear combination of chi-squares," *Computers and Mathematics with Applications*, Vol. 10, Issues 4 - 5, pp. 383-386, 1984.

[27] Texas Instruments, MSP430F5529 online datasheet, Available at: http://www.ti.com/product/MSP430F5529

[28] Analog Devices, AD8361 LF to 2.5 GHz TruPwr Detector, Available at: http://www.analog.com/en/products/rf-microwave/rf-power-detectors/rms-responding-detector/ad8361.html

Hun Seok Kim is an assistant professor at the University of Michigan, Ann Arbor. His research focuses on system novel algorithms and efficient VLSI architectures for low-power/high-performance signal processing, wireless communication, computer vision, and machine learning systems. He received his B.S. degree from the Seoul National University (South Korea), and M.S. & Ph.D. degrees from the University of California, Los Angeles (UCLA), all in Electrical Engineering. He is a recipient of multiple fellowships from the Ministry of Information and Telecommunication (South Korea), Seoul National University, and UCLA. Before joining the University of Michigan, He worked as a technical staff member at Texas Instruments Inc. (2010 – 2014), while serving as an industry liaison for multiple university projects funded by the semiconductor research cooperation and Texas Instruments Inc. He currently holds 9 granted patents and has 10+ pending applications in the areas of digital communication, signal processing, and low power integrated circuits.

David D. Wentzloff (S'02 – M'07) received the B.S.E. degree in electrical engineering from the University of Michigan, Ann Arbor, MI, USA, in 1999, and the S.M. and Ph.D. degrees from the Massachusetts Institute of Technology, Cambridge, MA, USA, in 2002 and 2007, respectively. Since August 2007, he has been with the University of Michigan, where he is currently an Associate Professor of Electrical Engineering and Computer Science. His research focuses on RF integrated circuits, with an emphasis on ultra-low power design. In 2012, he co-founded PsiKick, a fabless semiconductor company developing ultra-low power wireless SoCs.

Dr. Wentzloff was the recipient of the 2009 DARPA Young Faculty Award, 2009 – 2010 Eta Kappa Nu Professor of the Year Award, 2011 DAC/ISSCC Student Design Contest Award, 2012 IEEE Subthreshold Microelectronics Conference Best Paper Award, the 2012 NSF CAREER Award, the 2014 ISSCC Outstanding Forum Presenter Award, the 2014 – 2015 Eta Kappa Nu ECE Professor of the Year Award, the 2014 – 2015 EECS Outstanding Achievement Award, and the 2015 Joel and Ruth Spira Excellence in Teaching Award. He has served on the technical program committee for ICUWB 2008 – 2010, ISLPED 2011 – 2015, S3S 2013 – 2015, and RFIC 2013 – 2015, and as a guest editor for the *IEEE Transactions on Microwave Theory and Techniques*, the *IEEE Communications Magazine, and Signal Processing: Image Communication*. He is a member of the IEEE Circuits and Systems Society, IEEE Microwave Theory and Techniques Society, IEEE Solid-State Circuits Society, and Tau Beta Pi.