Wi(deband)-Fi: A Proposal for an Opportunistic Wideband Architecture based on Wi-Fi

Guevara Noubir
Northeastern University
Boston, MA, USA
noubir@ccs.neu.edu

Muriel Médard
MIT
Cambridge, MA, USA
medard@mit.edu

Peter Chin
Boston University
Boston, MA, USA
spchin@cs.bu.edu

ABSTRACT

We propose a system, Wideband-Fi, that is motivated by the information theoretic optimality of impulsive frequency shift keying (I-FSK) in wideband systems, and by the availability of orthogonal frequencies in current Wi-Fi systems. Using orthogonal frequencies to approximate I-FSK, Wideband-Fi is able to use non-contiguous spectrum bands in an agile manner, thus allowing aggressive spectrum scavenging. We present the main principles of our proposal, preliminary demonstration of its feasibility, and discuss challenges, and its connection to cognate problems such as transport-layer use of multiple wireless interfaces, and detection of white spaces.

1. INTRODUCTION

Within the wireless ecosystem, Wi-Fi (IEEE 802.11) emerged as the defacto primary technology for connecting devices to the Internet. This manifests itself first in the increasing Wi-Fi offloading of mobile traffic, caused by the limited ability of cellular ISPs to scale to applications demands, and second in the integration of Wi-Fi in a variety of low-cost Internet of Things (IoT) and Machine to Machine (M2M) devices. We are interesting in broadening the scope of capabilities of Wi-Fi to support a wide variety of radio spectrum constraints including fragmentation over a the 2.4GHz bands (80MHz ISM), 5GHz UNII-1, UNII-2, UNII-2 ext, UNII-3, and ISM bands (over 600MHz of bandwidth), as well as the non contiguous TV white space in 54–698 MHz. While traditionally Wi-Fi focused on the high SNR regime, we aim at extending it to low SNR regime, as well. A key design goal is to enable smooth co-existence with existing Wi-Fi PHY/MAC schemes and whenever possible compatibility.

Towards this goal, we propose an architecture to create a wideband system, Wideband-Fi using currently available terrestrial Wi-Fi networks. Our main inspiration is to combine information theoretic understanding of the wideband regime with practical considerations of current Wi-Fi systems, that rely upon sub-carrier transmission methods. On the one hand, impulsive frequency-shift keying (FSK) transmits by coding **across bands** by using frequency and timing of transmission for conveying information. This sparse use of time and frequency is capacity achieving in the wide band limit (low J/s/Hz), and is robust to channel fading. On the other hand, current commercial systems such as Wi-Fi and 4G cellular systems, use multiple frequencies, but use modulation and coding **within** each band. This approach, which makes dense use of time and frequency, is optimal in the high J/s/Hz and requires robust channel tracking. We therefore propose a method to bridge the two approaches, creating a continuum from low J/s/Hz to high J/s/Hz regimes, enabled especially by the ideas from the theory of compressive sensing. Current systems generally assume contiguous frequency bands, which limits the ability to aggressively scavenge bandwidth.

The main components of our proposed architecture is to instantiate in Wi-Fi networks information-theoretic principles from wideband systems by leveraging the types of sub-carrier based signalling used in modern 802.11 systems. The main principle is to use different carriers in a bursty fashion. This portion of the work has a theoretical component, that considers signal design through the adaptation of time and frequency bursty schemes suggested by information theory to Wi-Fi channels. Such schemes are capacity achieving in the limit of high bandwidths, they are impervious to even unknown channel fading and posses strong robustness to noise, even exhibiting anti-jamming (AJ) properties. The second component is experimental, in which we propose to instantiate, within the constraints of sub-carrier transmission in orthogonal frequency division multiplexing (OFDM), bursty schemes.

The main motivator in this context is that modern wireless systems, from Wi-Fi to fourth generation long-term evolution cellular systems (4G LTE) all rely on orthogonal frequency division modulation (OFDM), sometimes refered to as sub-carrier modulation (SCM). Such modulation can be used in a way similar to frequency-shift keying (FSK). True FSK transmission and its OFDM approximation are shown schematically in Figure 1.

2. THEORETICAL MOTIVATION

Traditional approaches to obtain robustness to only

MobiWac'16, November 13-17, 2016, Malta, Malta

DOI: http://dx.doi.org/10.1145/2989250.2989256

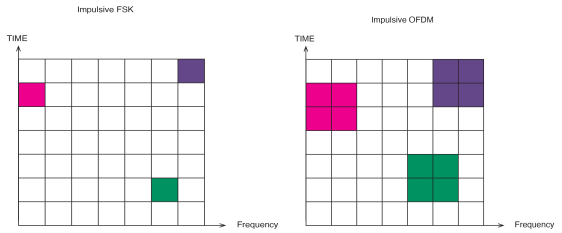


Figure 1: Impulsive FSK and using OFDM to transmit in a FSK fashion

noise, even active noise such as jamming, have been through the use of noise-like signals. The efficacy of such methods are strongly predicated on having a continuously used channel whose changes are sufficiently slow to allow measurement of the channel at the receiver. Such models do not hold in networks of mobile nodes, particularly as we consider wideband transmissions. The effect of both channel variations and interference preclude, even in the absence of jammers, the use of noise-like signals. Instead, one must use impulsive signals, which have the added advantage of being robust to channel variations and to interference in the wideband regime.

Traditional approaches to wideband robustness to noise consider time-invariant channels. In such settings, wideband robustness to noise can be obtained through spread-spectrum techniques. The jammer's best strategy is to behave as noise and the signaller's best strategy is to mimic noise. In the wideband limit, a signaller is thus in effect able to hide in the noise, as long as his signature is not known to an eavesdropper. This approach is also capacity-achieving even in the absence of a jammer. Such noise-like characteristics can be obtained by schemes such as direct-sequence code-division multiple access (DS-CDMA). The time-invariance of the channel is not crucial, rather, it is the ability of the receiver to measure the channel characteristics that is important. Even under some level of error in the channel measurement at the receiver, the capacity of a wireless link remains close to that obtained under conditions where there is no error in channel measurement [1].

The assumption of a time-invariant channel does not hold, however, when we consider mobile networks. Mobility entails changes in the channel, at a rate commensurate with the Doppler shift associated with the movement of nodes. Bursty transmissions lead to time-varying interference. Such variability in time and frequency leads to significant changes in the design of AJ and LPI systems. When the channel is time-varying, DS-CDMA suffers from poor capacity, which, in frequency-selective fading channels, decreases to 0 as the bandwidth increases [2, 3, 4]. The main reason for this poor performance is that there is insufficient energy to measure the channel's realizations across time and frequency. In the absence of such measurements, capturing a noise-like signal becomes provably infeasible. Thus, a noise-like LPI system is not practical in wideband regimes. Even other proposed wide-band approaches are not inure to effects arising from channel variations. For instance, pulse-position modulation (PPM), which has low narrowband interference but is not LPI if we consider a receiver integrating over a wide band, also suffers from deleterious effects when the number of paths increases with bandwidth (Porrat). Previous results show that what is needed is a signal which is peaky, as defined by certain properties of the scaling of the kurtosis [2] or other similar properties [3, 5]. Prime examples of such signalling are peaky frequency-shift keying (FSK) and variants thereof, such as multitone FSK, which can be effective even with limited peakiness [6]. Note that there is no absolute value of energy per degree of freedom, or rate of change of the channels, which determines when we are in a wideband regime that requires peaky transmission. Instead, we must consider the effective coherence of the channel, which takes into account the interaction among energy, bandwidth and channel variability in time and frequency [7] and, in the case of multiple-input, multiple-output systems, the number of antennas [8].

Our above discussion establishes that, even in the absence of jamming, wideband, time-varying channels require the use of peaky signals. We showed that such peaky signals also have, in the wide-band limit, very strong AJ properties [9, 10]. In particular, we showed that, through the use of peaky signals, energy-limited jammers do not affect capacity in the wideband regime. A corollary to this fact is that a node may transmit and jam simultaneously, without concern for affecting its own throughput, as long as it is allowed sufficient bandwidth over which to transmit. Moreover, a Gaussian jammer cannot even affect the error exponents, which indicate the length of the code needed to approach capacity within a certain allowed probability of code error. Impulsive FSK can also co-exist with existing pre-assigned narrowband signals, since there is no requirement that frequencies be contiguous. It is thus simple to avoid certain frequency bands in the signalling. Figures 2 and 3 show impulsive FSK and its OFDM approximation over non-contiguous frequency bands.

Our above discussion establishes that, even in the absence of jamming, wideband, time-varying channels require the use of peaky signals. We have shown that such peaky signals also have, in the wide-band limit, very strong AJ properties [9, 10]. In particular, we have shown that, through the use of peaky signals, energy-limited jammers do not affect capacity in the wideband regime. A corollary to this fact is that a node may transmit and jam simultaneously, without concern for affecting its own throughput, as long as it is allowed sufficient bandwidth over which to transmit. Moreover, a Gaussian jammer cannot even affect the error exponents, which indicate the length of the code needed to approach capacity within a certain allowed probability of code error. Impulsive FSK can also co-exist with

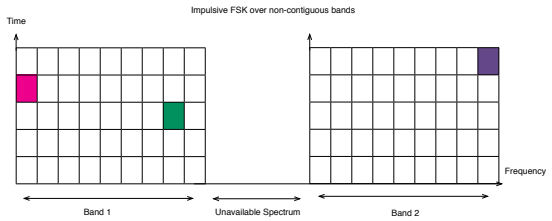


Figure 2: Impulsive FSK fashion over non-contiguous frequency bands.

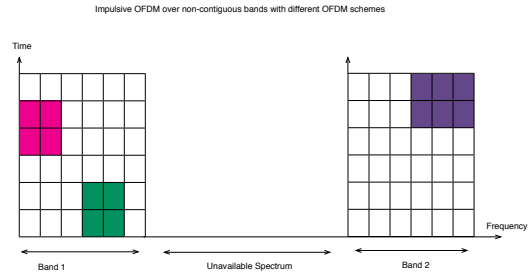


Figure 3: Using OFDM to transmit in a FSK fashion over non-contiguous frequency bands.

existing pre-assigned narrowband signals, since there is no requirement that frequencies be contiguous. It is thus simple to avoid certain frequency bands in the signalling.

Note that the use of multiple-input multiple-output (MIMO) schemes does not appreciably change the behavior in the low J/s/Hz regime. Unless a channel is entirely static, then the gain from having MIMO in the low J/s/Hz is, to a first order approximation, only useful in terms of being able to capture more energy at the receiver [8]. The benefit of MIMO is captured in a first order term, where the number of receive antennas provides a proportional gain in received energy, and the number of transmit antennas is seen only in second order terms, or in coding error exponents.

3. RETROFITTING FSK INTO WI-FI

A key aspect of Wideband-Fi, motivated by the discussion above, is an extension of current OFDM-based Wi-Fi standards to support Impulsive FSK, and retrofitting Impulsive FSK into current OFDM-based Wi-Fi standards.

While the transmitter of an Impulsive FSK communi-

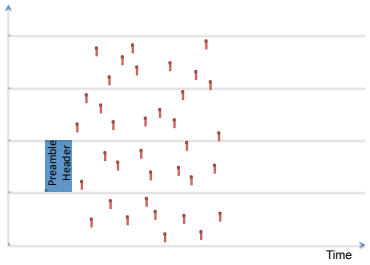


Figure 4: Illustration of Impulsive FSK with OFDM preamble header (20MHz) and 80MHz payload.

cation does not result in much complexity, the receiver requires special attention in order to detect impulses across a wideband of spectrum. An OFDM-based receiver satisfies the desired requirement providing simplicity at the receiver and support for not only a single tone Impulsive FSK but multi-tone as well. Furthermore, it integrates very well with the IEEE 802.11a/ g/ n/ ac/ ad OFDM physical layers (making future augmentation of current standards easy). In order to satisfy the need for synchronization as for a practical system, one design proposal that we consider is to use a relatively wideband preamble/header followed by the payload encoded using Impulsive FSK across the whole considered band. For example, on the 80MHz ISM band at 2.4GHz, the preamble/header is sent on one of the 20MHz channels of 802.11g, while the payload is sent over the whole 80MHz. Our proposal to simplify both the transmitter and receiver is to use OFDM combined with On-Off activation of sub-carriers. An OFDM transmitter can use an IFFT to transmit the Impulses on selected tones (sub-carriers). Single or multiple tones can easily be supported. The receiver uses the preamble/header to synchronize and an FFT operation to detect the single/multi-tone impulses. Given the low duty-cycle in frequency and time of Impulsive FSK, it is worth investigating the relevance, accuracy, and robustness of compressive sensing and sparse FFT techniques, for an efficient decoding. Compressive sensing and sparse FFT techniques have the potential to significantly reduce the complexity of the receiver, although one has to address intrinsic issues of co-existence with other communications altering the overall spectrum energy sparsity.

Our proposed system operates on multiple bands including the 2.4GHz bands (80MHz ISM), 5GHz UNII-1, UNII-2, UNII-2 ext, UNII-3, and ISM bands (over 600MHz of bandwidth), as well as the non contiguous TV white space in 54–698 MHz. These bands already have Wi-Fi systems operating on them for high SNR regime, namely IEEE 802.1a/b/g/n/ac/af. A possible instantiation is to use a SDR implementation of IEEE 802.11abg (SWiFi) to support the proposed designs, such as SWiFi [11]. SWiFi runs on popular SDR platforms (e.g., Ettus N210, X300) and even the low-cost HackRF. It is fully compatible with IEEE802.11abg physical layer and has been demonstrated to provide a performance at least as good as the best commercial Wi-Fi cards [11]. It has the advantage of running on regular PCs and therefore providing high flexibility for modifications and experimentation. The GNU Radio block di-

agrams of the SWiFi transmitter and receiver are shown in Figures 5 and 6. Extending SWiFi involves modifying the *Chunks to Symbols* block, the *OFDM Carrier Attenuator* block, and the *FFT* block. For the single-tone Impulsive FSK, a chunk of bits are mapped to the index of the carrier selected, while all other carriers are nulled. For instance, a 6-bits chunk uniquely identifies one of the 64 carriers of the 20MHz IEEE 802.11agn channel, while an 8 bits chunk would identify a unique carrier in the 80MHz band. For multi-tone Impulsive FSK, each chunk will be mapped to a unique pair of carriers. The OFDM Carrier Allocator and FFT blocks is extended to support wider bands e.g., 80MHz at 2.4GHz or 100-200MHz in the 5.2GHz UNII bands. Note that SWiFi can maintain compatibility with legacy Wi-Fi systems and smoothly adjust the mode depending on the SNR regime. The existing Wi-Fi OFDM physical layers can be viewed as a modulated version of the Impulsive FSK with all carriers being used. Similar modifications are applied to the SWiFi receiver. Potential deployment platforms of the IFSK-SWiFi are the USRP X300 which can operate over 120MHz but will also use the much lower cost LimeSDR (promising a bandwidth of 160MHz) as soon as it becomes available.

We demonstrated the main premise of our architecture, the modification of an OFDM system to implement Impulsive-FSK. We have already implemented a simple version of our scheme. In the preliminary work, we use a modified version of SWiFi for transmitting a regular packet but only on some sub-carriers (See Figure 7 for a screenshot from a spectrum analyzer). We used a regular Wi-Fi card in monitor mode (here a regular Apple MacBook with Wireshark packets sniffing tool) and were able to capture the transmitted packets despite that only the preamble/header are fully formed. As expected such packets have an incorrect CRC. For instance, we modified the OFDM Carrier Allocator block of our SWiFi implementation to use a subset of four carriers (See Figure 7). However, using a dynamic sub-carriers spacing value and a variable number of tones would require more significant modifications and additional chip resources (e.g., to implement different FFT sizes).

To illustrate what is achievable, Table 1 summarizes for various plausible configurations of spectrum (20-160Mhz) and number of tones, the resulting bitrate. Such configurations can be implemented without significant modifications to an existing IEEE 802.11 chipset baseband. The widest bands are only implemented in IEEE 802.11ac. The specific mapping between bits and multiple tones needs to be explicitly defined and standardised.

A next step of investigation is to develop a reduced version of the proposed Impulsive FSK, by embedding it in current Wi-Fi cards with only software/driver modifications. The goal is to (1) map data bits into a Wi-Fi packet such that when transmitted it results in a single (or few) sub-carriers being activated (per OFDM symbol), (2) at the receiver, despite the low SNR, the packet is detected and delivered to the driver indicating an incorrect CRC. Further software processing, would determine which OFDM sub-carriers was activated.

4. IMPLEMENTATION CHALLENGES.

To develop successfully an Impulsive-FSK stack on top of a full legacy Wi-Fi chipset, several challenges need to be addressed. The Wi-Fi physical layer chain contains multiple blocks that have to be accounted for, canceled, or leveraged. These include, the *scrambling*, *interleaving*, *coding*, and *modulation*. Similarly to current Wi-Fi systems, the physical layer needs to be complemented with adequate *rate adaptation* and *power control* algorithms.

4.1 Overcoming scrambling

According to the IEEE 802.11a/g standard, a Wi-Fi transmitter shall generate a new random scrambling seed for every transmission of a Physical Layer frame. We first briefly review the scrambling processes defined in IEEE 802.11a/g/p, and then describe how we propose to cancel it in order to control which sub-carriers are deterministically activated. The binary data is scrambled by a special construction depicted in Figure 8, where a 7-bit Linear Feedback Shift Register (LFSR) produces the scrambled bit y_k at it output by computing the exclusive-or ($GF(2)$ sum) of the input bit x_k and the LFSR output value z_k. The mathematical description of the scrambler shown in Figure 8 is given by:

$$z_k = z_{k-4} \oplus z_{k-7} \quad (1)$$

$$y_k = x_k \oplus z_k \quad (2)$$

where x_k, y_k are the k-th input and output bits, while z_k represents the feedback of the shift register at that time. We represent the shift register's content by either a binary sequence $z_{k-1} \dots z_{k-7}$ or a single decimal value s:

$$s = z_{-1} \cdot 2^6 + \dots + z_{-6} \cdot 2 + z_{-7}. \quad (3)$$

Interestingly, we recently discovered that not all chipset manufacturers follow the standard. Indeed, many chip manufacturers use a constant initial seed. For instance, we found that the Belkin N150, Edimax EW-781Un TP-Link TL-WN725N, and TP-Link TL-WN821N use a constant seed of $s = 124$, and D-Link WDA-1320, TP-Link TL-WN751ND, and TP-Link TL-WN722N use an incremental seed. Knowledge of the seed and the structure of the scrambler makes it easy to cancel its effect. To cancel the effect of the scrambling sequence z_k, the input packet x_k should be pre-xored with z_k. This approach, as well as the possibility to disable the scrambling block, seem to be possible with NexMon [12], a firmware development/patching framework for the BCM4339 Wi-Fi chipsets used for instance in Google's Nexus 5 smartphones.

4.2 Interleaving

Canceling the effects of interleaving might appear trivial, however it has its own challenges. Wi-Fi interleaving consists of two permutation rounds. The first-round permutation scatters adjacent coded bits into non-adjacent sub-carriers. Given that the permutation function is known it is possible to infer to which sub-carriers a given bit is mapped. This can be accounted for when generating the packets. However, the second-round permutation shuffle adjacent coded bits within every sub-carrier

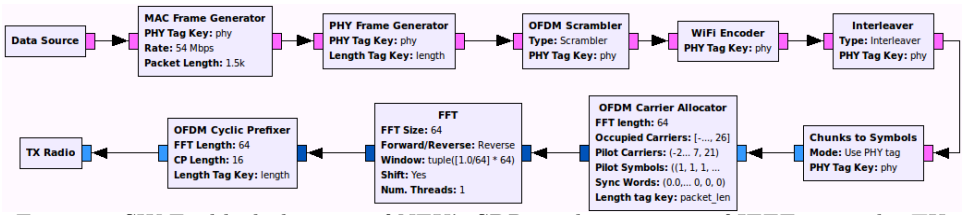


Figure 5: SWiFi: block diagram of NEU's SDR implementation of IEEE802.11abg TX

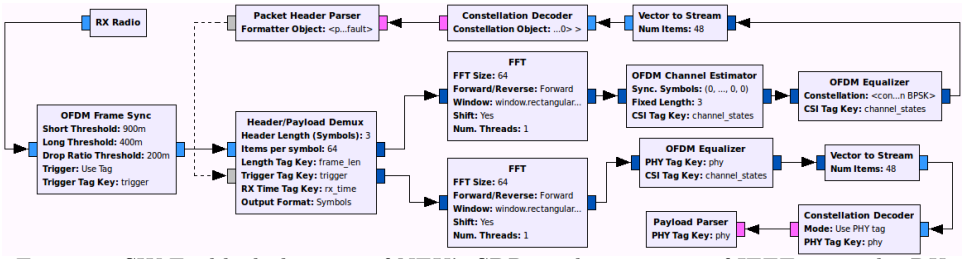
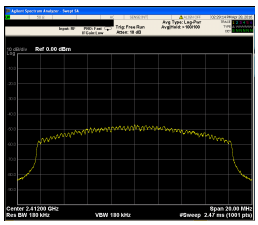
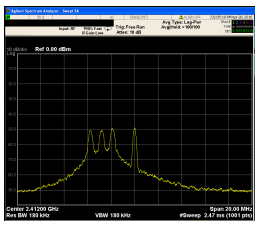


Figure 6: SWiFi: block diagram of NEU's SDR implementation of IEEE802.11abg RX



((a)) IEEE 802.11g all carriers



((b)) Restricted to 4 carriers

Figure 7: Wi-Fi transmission (20MHz OFDM) and a modified 4 carriers OFDM.

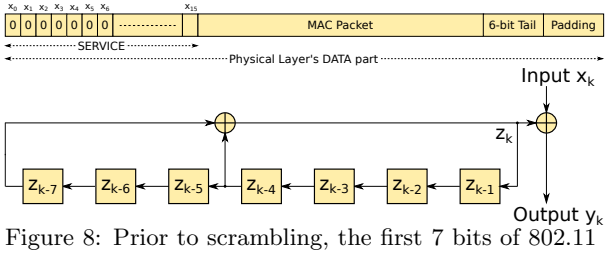


Figure 8: Prior to scrambling, the first 7 bits of 802.11 SERVICE field in the PHY header are set to zero.

which requires a more careful analysis and countering mechanism. As we will discuss in the following paragraphs, higher order modulation might be necessary to emulate Impulsive FSK but the packets would require special crafting to account for the interleaver second-round permutation.

4.3 Accounting for coding

When the effect of scrambling is canceled, the driver can introduce a single non zero bit per OFDM symbol in order to activate a single sub-carrier. However, the convolutional coding will result in multiple non-zero bits. One step towards mitigating the effect is to use a high rate Modulation Coding Scheme (MCS). For instance in IEEE802.11n/ac rate 5/6 has a low free distance. Other activated sub-carriers can be leveraged as a repetition code, which is adequate for the low S/J/Hz regime.

4.4 Approximating FSK modulation by QAM

Current Wi-Fi standards and chipsets use PSK or QAM modulation and do not support FSK modulation. They are therefore transmitting on all carriers at all times. To embed Impulsive FSK into OFDM-QAM we propose to use the highest order modulation and precompute packets that will activate a single carrier with the highest amplitude. For instance QAM-256 modulation, in 802.11ac, will give 17dB difference between the lowest and highest constellation points. This could be a valid starting point, however it has to be investigated and developed in tandem with the (second-round permutation) interleaving, the coding, and the multi-tone dimension.

4.5 Rate adaptation and power control

Our proposed system is intended to be used over a wide range of non-contiguous frequencies, aggressively scavenging available spectrum. This results in significant differences in path loss which can be as high as 50dB (for instance between the 570MHz TV White Space band and the 5.7 GHz ISM band) [13]. This is also aggravated by the co-existence with a variety of devices. Adapting to these characteristics requires agile Rate Adaptation Algorithms and Power Control.

4.6 Medium Access Control

The CSMA/CA MAC, common to all today's Wi-Fi physical layers, is a possibility for supporting our OFDM-based Impulsive FSK. The CSMA/CA MAC is possible because the preamble/header is transmitted in a similar manner to existing Wi-Fi, allowing other nodes to sense a transmission. Alternative MAC mechanisms consist of allowing parallel transmission, however this would require splitting the carriers and/or adequate coding.

Scheme\Bandwidth	20MHz	40MHz	80Mhz	160MHz
Single-Tone	1.87	3.75	7.5	15
Two-Tone	3.44	6.87	13.75	27.5
Three-Tone	4.8	9.6	19.2	38.4

Table 1: Bitrate in Mbps for various combinations of bandwidth and multi-tone OFDM-based Impulsive FSK assuming IEEE802.11a/g/n/ac subcarrier spacing of 312.5KHz.

5. DISCUSSION

5.1 Extensions beyond Wi-Fi

Since the main component of our approach is the use of OFDM signaling in a FSK-style manner, we may readily extending our approach beyond Wi-Fi, with other schemes such as cellular 4G networks, which also use OFDM. Note that, if we are to use our approach over different systems, we may need to contend with the issue of delay in multipath systems. The study of delay performance for coded schemes in multi-path environments has been somewhat limited. The delay-rate trade-off with various multi-path routing and coding approaches was investigated in [14, 15]. Multiple description coding and layered coding over multiple paths was looked at by [16]. Of primary note is the work by [17]. They propose an algorithm called Stochastic Earliest Delivery Path First (S-EDPF) that combines packet scheduling with a coding approach that assumes redundancy is only transmitted on a single path while the algorithm presented here is general enough to allow redundancy to be transmitted on multiple paths.

5.2 Compatibility with multiband systems

Our approach is compatible with existing and proposed multiband approaches, particularly for heterogeneous networks. Our approach uses disparate bands in an integrated fashion at the physical and MAC layer, but we may readily use several bands at the transport layer to make use of the inherent heterogeneity that exists among the device's wireless connections. Prime examples include the desire to offload traffic from cellular networks to Wi-Fi networks and the desire to simultaneously utilize both macro and small cells in 5G networks. Even though most devices have a significant amount of transmission rate available over different radio links, these connections operate independently and usually one at a time. They can be used together with traditional cognitive radio approaches but the fact that they operate separately may not allow the full range of application of cognitive radio techniques. While the merging of network resources has the potential to increase throughput, packet losses due to congestion, poor link quality, transient network connections, etc. can have serious consequences for meeting users' quality of service (QoS) requirements.

Approaches such as multipath TCP (MPTCP) have been recently reported to be used by Apple, but only on one network at a time [18]. Several methods to incorporate network coding with MPTCP have been proposed [19, 20, 21, 22, 23]. Gheorgiu et. al. [21] propose a protocol called CoMP that uses network coding for multipath transmission that incorporates only some aspects of TCP. References [22] and [20] propose a method incorporating TCP/NC, [24, 25], that adds a multipath scheduler below the TCP, network coding, and IP layers. Unfortunately, this scheduler negates the congestion control benefits of TCP over single paths. When network coding is applied to MPTCP, say over both LTE and Wi-Fi concurrently, we have recently shown considerable throughput and resiliency gains [26].

We can readily envisage coding across signal across different bands, using both physical layer schemes (FSK using multiple non-contiguous slices as in Wideband-Fi) and transport layer techniques (coding across paths in MPTCP with network coding).

5.3 Sensing for spectrum scavenging

Our system allows aggressive scavenging of spectrum by the use of non-contiguous bands or arbitrary sizes. In order to detect which bands can be used for signaling, spectrum use must be characterized. Compressive sensing originates from the observation that most natural signals and data streams are inherently sparse in certain bases or dictionaries where they can be approximately represented by only a few significant components carrying the most relevant information. This type of phenomenon has been widely recognized empirically recently across multiple data types and applications (sounds, images, texts, etc.), especially in RF signals, and a recently developed theory of compressive sensing attempts to exploit such a sparse structure of data in an appropriate basis. We use such an approach to receive signals without the need for onerous filter banks, but also to detect the absence thereof (i.e. white spaces).

Compressed sensing (CS) has been rigorously studied over the past few years as a signal sampling paradigm. According to CS theory, a K-sparse signal $x^\star \in^n$ is measured through a set of M linear projections $y_i =< a_i, x^\star >$, $i = 1, ..., M$, in which vectors $a_i \in^N$ form a matrix A of size $M \times N$. The intriguing CS framework advocates the collection of significantly fewer measurements than the ambient dimension of the signal. To reconstruct $x^\star$, ℓ_1-minimization is proposed to solve:

$$\text{Noiseless:} \quad \min_x x_1 \quad \text{s.t.} \quad y = Ax. \tag{4}$$

$$\text{Noisy:} \quad \min_x x_1 \quad \text{s. t.} \quad y - Ax_2 \leq \sigma. \tag{5}$$

The noisy case above deals with imperfect observations contaminated by noise, i.e., $y = Ax^\star + w$ where w is some unknown perturbation bounded by a known amount $w_2 \leq \sigma$. It has been accepted in the literature that if the sensing matrix A obeys the Restricted Isometry Property (RIP) and σ is not too large, then the solution $\hat{x}$ of (5) does not depart too far from the opti-

mal solution $x^\star$, so long as the number of measurements is on the order of $K \log N$. In particular, they proved that the reconstruction error proportionally grows with σ: $\hat{x} - x^\star{}_2 \leq C\sigma$, where C is a small numerical constant. This error bound is significant as noise is not too large. Especially when the measurement vector b is clean, the result implies perfect recovery.

Traditional Compressed Sensing is based on the assumption that the signals of interest are sparse after certain sparsifying transforms. However, it is possible to extend the theory to deal with certain problems that involve signals that are not sparse in the traditional sense, but still possess some structure, which we called Inverse Compressed Sensing problems. We propose to use Robust Inverse Compressed Sensing (RICS) for detecting white spaces.

The signal of interest x, though not sparse in transform domain, but assumed to have certain structure in that domain. The transformed coefficients are well represented using a base signal x_b and a sparse signal x_s. Mathematically,

$$\Phi x = x_s + x_b + e, \tag{6}$$

where e is an error vector that include small differences that are not covered by the model.

This signal x is obviously not sparse in its original domain and in the sparsifying domain Φ, therefore it seems impossible to recover it relying on only a few measurements captured in a regular Compressed Sensing set up $y = Ax$. However, by assuming that the signal is structured, we would expect that the "base" signal x_b is dense but not totally random. Instead, it is expected to be sparsely represented in a certain basis (or redundant dictionary), or $x_b = V\alpha_b$. The equation 6 becomes

$$\Phi x = x_s + V\alpha_b + e, \text{or} \tag{7}$$

$$\Phi(x - \Phi^T e) - V\alpha_b = x_s. \tag{8}$$

Now let us extend the original sparse coeeficient vector x_s by appending to it the α_b coefficients. The resulting vector is also expected to be sparse, and the Equation 8 changes to

$$\begin{bmatrix} x_s \\ -\alpha_b \end{bmatrix} = \begin{bmatrix} \Phi & V \\ 0 & I \end{bmatrix} \begin{bmatrix} x_e \\ -\alpha_b \end{bmatrix}, \tag{9}$$

where $x_e = x - \Phi^T e$. If we define $x_C = [x_e - \alpha_b]^T$, the original measurement vector y is representable in this notation, which is

$$y = \begin{bmatrix} A & 0 \end{bmatrix} x_C + \eta, \text{where } \eta = A\Phi^T e. \tag{10}$$

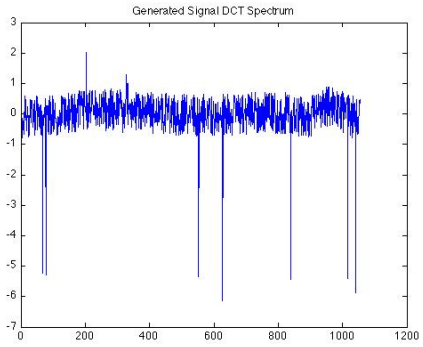
It is then possible to recover the non-sparse (but structured) signal x based only the measurements y via the following optimization problem

$$min \|Sx_C\|_1 \text{ s.t. } y = A_0 x_C + \eta, \tag{11}$$

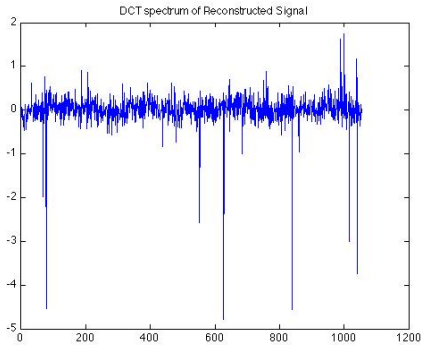
where

$$x_C = \begin{bmatrix} x_e \\ -\alpha_b \end{bmatrix}, S = \begin{bmatrix} \Phi & V \\ 0 & I \end{bmatrix}, \text{and } A_0 = \begin{bmatrix} A\ 0 \end{bmatrix}.$$

In this set up, the sparse component x_s is usually of more importance. It can be thought of as valleys in a dense spectrum, which we would like to detect. In some applications, the locations of the negative peaks are actually more important to detect or recover rather than the base signal x_b. In other words, the recovery errors in x_b are tolerable as long as the support of x_s is correct. This is reflected in our experiments with simulated data. The optimization in 11 may get error in recovering x_b but it is very robust to detecting the location of the x_s.



(a) Original Spectrum with a few Valleys



(b) Recovered Spectrum with Valleys Identified

Figure 9: Recovering white spaces (Valleys) in RF Spectrum using RICS with 10% Random Sampling

6. CONCLUSIONS AND FURTHER WORK

We propose Wideband-Fi, an approach for using OFDM over Wi-Fi in a way that mimics I-FSK, which is optimal in wideband systems. Our approach allows the aggressive, highly opportunistic use of non-contiguous spectrum bands. The use of OFDM in other widely deployed wireless systems, such as cellular systems, points to the possible extension of Wideband-Fi to channel bonding across different networks. However, our approach allows for a mixture of heterogeneous network use, allowing the simultaneous use of heterogeneous networks at the MAC layer and/or the transportation layer.

Further work in Wideband-Fi will require the demonstration and testing of simply coded I-FSK over OFDM systems. We have identified some of the main challenges, such as overcoming the scrambling and MAC

design, for which there exist several candidate possibilities. Moreover, to be of significant use, available spectrum for Wideband-Fi needs to be discovered and characterized. Compressive sensing techniques, that rely on the sparsity of spectrum use, are a promising approach.

Acknowledgements. This material is based upon work supported by Grants NSF/CNS-1409453, NSF/DMS-1222567, and AFOSR under grant FA9550-12-1-0136.

7. REFERENCES

[1] M. Médard, "The effect upon channel capacity in wireless communications of perfect and imperfect knowledge of the channe," *IEEE Transactions on Information Theory*, vol. 46, may 2000.

[2] M.Médard and R. Gallager, "Bandwidth scaling for fading multipath channels.," *IEEE Transactions on Information Theory*, vol. 48, pp. 840–852, April 2002.

[3] V. G. Subramanian and B. Hajek, "Broad-band fading channels: Signal burstiness and capacity," *Information Theory, IEEE Transactions on*, vol. 48, pp. 809 – 827, April 2002.

[4] I. Telatar and D. Tse., "Capacity and mutual information of wideband multipath fading channels," *IEEE Trans. Inform. Theory*, vol. 48, pp. 1384–1400, July 2000.

[5] S.Verdú, "Spectral efficiency in the wideband regime," *IEEE Trans. Inform. Theory*, 2002.

[6] C. Luo, M. Médard, and L. Zheng, "On achieving wideband capacity using multitone fsk," *IEEE Journal on Selected Areas in Communications (JSAC)-Special Issue on Differential and Noncoherent Wireless Communications*, vol. 23, pp. 1830–1838, September 2005.

[7] L. Zheng, D. N. C. Tse, and M. Medard, "Channel coherence in the low snr regime," *IEEE Transactions on Information Theory*, vol. 53, pp. 976–997, March 2007.

[8] S. Ray, M. Médard, and L. Zheng, "On non-coherent mimo channels in the wideband regime: Capacity and reliability," *IEEE Transactions on Information Theory*, vol. 53, pp. 1983 – 2009, June 2007.

[9] S. Ray, P. Moulin, and M. Médard, "On jamming in the wideband regime," in *ISIT*, 2006.

[10] S. Ray, P. Moulin, and M. Médard, "On optimal signaling and jamming strategies in wideband fading channels," in *IEEE Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, pp. 1–5, July 2006.

[11] T. D. Vo-Huu, T. D. Vo-Huu, and G. Noubir, "Swifi: An open source sdr for wi-fi networks high order modulation analysis," tech. rep., 2015. *Technical Report*.

[12] M. Schulz, D. Wegemer, and M. Hollick, "Demo: Using nexmon, the c-based wifi firmware modification framework," in *Proceedings of the 9th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, WiSec '16, ACM, 2016.

[13] A. B. Flores, R. E. Guerra, E. W. Knightly, P. Ecclesine, and S. Pandey, "Ieee 802.11af: a standard for tv white space spectrum sharing," *IEEE Communications Magazine*, 2013.

[14] S. Han, Z. Zhong, G. C. H. Li, E. Chan, and A. K. Mok, "Coding-aware multi-path routing in multi-hop wireless networks," in *PCCC*, pp. 93–100, Decemeber 2008.

[15] K. Ronasi, A. H. Mohsenian-Rad, V. W. S. Wong, S. Gopalakrishnan, and R. Schober, "Delay-throughput enhancement in wireless networks with multipath routing and channel coding," in *IEEE Transactions on Vehicular Technology*, vol. 60, pp. 1116–1123, March 2011.

[16] V. T. Nguyen, E. C. Chang, and W. T. Ooi, "Layered coding with good allocation outperforms multiple description coding over multiple paths," in *ICME*, vol. 2, pp. 1067–1070, June 2004.

[17] A. Garcia-Saavedra, M. Karzand, and D. J. Leith, "Low delay random linear coding and scheduling over multiple interfaces," 2015.

[18] J. Cox, "Apple iOS 7 suprises as first with new multipath TCP connections," Sept. 2013.

[19] "MPTCP IETF working group." https://datatracker.ietf.org/wg/mptcp/.

[20] Z. qun Xia, Z. gang Chen, Z. Ming, and J. qi Liu, "A multipath TCP based on network coding in wireless mesh networks," in *Proc. IEEE International Conference on Information Science and Engineering (ICISE)*, pp. 3946–3950, 2009.

[21] S. Gheorghiu, A. L. Toledo, and P. Rodriguez, "Multipath TCP with network coding for wireless mesh networks," in *Proc. IEEE International Conference on Communications (ICC)*, 2010.

[22] X. Zhuoqun, C. Zhigang, Y. Hui, and Z. Ming, "An improved MPTCP in coded wireless mesh networks," in *Proc. IEEE International Conference on Broadband Network & Multimedia Technology (IC-BNMT)*, pp. 795–799, 2009.

[23] V. Sharma, S. Kalyanaraman, K. Kar, K. K. Ramakrishnan, and V. Subramanian, "MPLOT: A Transport Protocol Exploiting Multipath Diversity Using Erasure Codes," in *INFOCOM*, pp. 121–125, 2008.

[24] J. Sundararajan, D. Shah, M. Médard, M. Mitzenmacher, and J. Barros, "Network coding meets tcp," in *INFOCOM 2009, IEEE*, pp. 280–288, April 2009.

[25] J. Sundararajan, D. Shah, M. Médard, S. Jakubczak, M. Mitzenmacher, and J. Barros, "Network coding meets tcp: Theory and implementation," *Proceedings of the IEEE*, 2011.

[26] J. Cloud, F. du Pin Calmon, W. Zeng, G. Pau, L. Zeger, and M. Médard, "Multi-path tcp with network coding for mobile devices in heterogeneous networks," in *VTC Fall*, 2013.