2017 IEEE 37th International Conference on Distributed Computing Systems

Communication through Symbol Silence: Towards Free Control Messages in Indoor WLANs

Bing Feng*†, Jianqing Liu‡, Chi Zhang*† and Yuguang Fang‡
*CAS Key Laboratory of Electromagnetic Space Information
University of Science and Technology of China, Hefei 230027, P. R. China
†State Key Laboratory of Information Security, Institute of Information Engineering
Chinese Academy of Sciences, Beijing 100093, P. R. China
‡Department of Electrical and Computer Engineering
University of Florida, Gainesville, Florida 32611, USA
Email: fengice@mail.ustc.edu.cn, jianqingliu@ufl.edu, chizhang@ustc.edu.cn, fang@ece.ufl.edu

***Abstract*—Efficient design of wireless networks benefits from the exchange of control messages. However, control message itself consumes scarce channel resources. In this paper, we propose CoS (Communication through symbol Silence), a novel communication strategy that conveys control messages for free without consuming extra channel resources. CoS inserts silence symbols in data packets and leverages the intervals between inserted silence symbols to encode information. The silence symbols can be located by energy detection at the granularity of symbols and the intervals are interpreted into transmitted control messages. Based on our key insights that the channel code is under-utilized in current wireless networks and the distribution of symbol errors within a data packet is predictable in indoor wireless transmissions, the symbols erased by silence symbols are recovered by the coding redundancy that is originally used to correct symbol errors. A rate adaptation scheme is designed to dynamically adjust the rate of free control messages according to channel conditions so that the transmission of free control messages does not harm the original data throughput. We implement CoS on our software defined radio platform to validate the feasibility of CoS. The extensive results show that the control messages are delivered with close to 100% accuracy in a large SNR range. In addition, we measure the achievable capacity of free control messages in various channel conditions.**

I. Introduction

Control messages are essential for designing efficient applications such as access coordination, resource allocation and load balancing. In current wireless local area networks (WLANs), control messages are conveyed by explicit control frames or implicit piggybacking schemes. However, with conventional mechanisms, the transmission of control messages needs to define new control frames or change existing data frame structure, which consumes extra channel resources.

On the other hand, wireless networks exhibit considerable Signal-to-Noise Ratio (SNR) gap that is potentially available for conveying extra information. The data rate adaptation scheme picks an optimal data rate to maximize channel capacity according to channel SNR. However, the current data rate adaptation scheme only provides stair-case data rate adjustment due to the limited number of data rates. As a result, when the SNR falls between adjacent data rates, there exists a SNR gap between the minimum SNR required by the selected data rate and the actual SNR supported by the current channel. Prior works [1] [2] focus on how to design seamless data rate adaptation schemes to fill the SNR gap, but these schemes are complex and cause extra hardware overhead. Instead, we will exploit, rather than fill, the existing SNR gap, which enables us to transmit lightweight control messages for free without consuming additional channel resources in WLANs.

In this paper, we propose CoS, an extension to orthogonal frequency division multiplexing (OFDM) based WLANs (e.g., 802.11a/g/n), which utilizes a novel communication strategy to convey lightweight control messages, while ensuring not to sacrifice the original data throughput. CoS embeds control messages into the intervals between inserted silence symbols. Compared to normal symbols, silence symbols are data symbols with zero transmission power. Thus, a silence symbol conveys no specific data bits except for its existence. The length of an interval can be detected by locating silence symbols that is achieved by symbol level energy detection [3].

The normal symbols are deliberately erased to be silence symbols that are treated as symbol errors at receiver, so the challenge is to exploit the SNR gap to recover those symbols damaged by intended erasures so that the data packet can be decoded correctly. Since wireless transmissions are inherently unreliable, data bits are encoded by channel code (convolutional code in 802.11 standards) to add redundant bits and the encoded bits are able to correct certain bit errors [4]. The SNR gap leads to under-utilization of channel code, i.e., the number of erroneous symbols induced by wireless fading is much less than the adopted channel code can actually handle. Therefore, CoS can take advantage of the SNR gap to obtain the correction capability of channel code to correct the inserted silence symbols and convey a reasonable amount of silence symbols. In CoS, both erroneous symbols induced by wireless fading and inserted silence symbols are symbol errors that need to be corrected by channel code. Given the correction capability of channel code, to enhance the total number of silence symbols that can be inserted in CoS, the intuition is that we insert as many silence symbols as possible but avoid introducing too much new symbol errors into the original data packet. Therefore, in addition to utilizing the existing SNR gap to design CoS, we will proactively reduce symbol

1063-6927/17 $31.00 © 2017 IEEE
DOI 10.1109/ICDCS.2017.120

errors induced by inserted silence symbols by designing the distribution of inserted silence symbols.

The feasibility behind the proactive reduction of introduced symbol errors is based on our promising insight that the distribution of erroneous symbols within a data packet is predictable in indoor environments. Our measurements reveal that the error probabilities of symbols within a data packet are highly uneven and errors are more likely to occur at certain symbol positions than others. This phenomenon is caused by frequency selective fading where different OFDM subcarriers undergo various fading. The observed symbol error patterns verify the fact that the number of erroneous symbols is dominated by those weak OFDM subcarriers. Therefore, if we can predict subcarrier conditions and design our proposed communication strategy on those weak OFDM subcarriers, a large number of inserted silence symbols will fall onto the positions of error-prone symbols. Compared with silence symbols falling onto the data symbols in reliable OFDM subcarriers, this method reduces new symbol errors introduced by inserted silence symbols because data symbols in weak OFDM subcarriers will be corrupted by wireless fading and fixed by the channel code. Moreover, in indoor environments such as offices, conference rooms and laboratories, the usage pattern of WiFi users is "static or mobile with walking-speed during communications". Our measurements show that frequency diversity is relatively stable over time and the coherence time of indoor wireless channel is big enough to predict for further data packets. Therefore, a picture of the distribution of erroneous symbols within a future data packet can be constructed.

We have implemented CoS on our software defined radio platform Sora. The experiment results show that the detection accuracy of control messages is close to 100% in practical SNR regions and the rate of free control messages provided by CoS is sufficient to support various upper layer applications.

The rest of this paper is organized as follows. Section II presents an overview of CoS and our experimental observations. Section III describes the detailed design of CoS. Section IV validates CoS and presents extensive results. Section V reviews the related work, and we conclude this paper in VI.

II. Overview and Observations

In this section, we start with an overview of CoS based on 802.11a physical layer. We then conduct experiments with software defined radios to show the existence of SNR gap and characterize symbol error patterns in a typical indoor environment.

A. Overview of CoS

The physical (PHY) layer of most modern WLANs (e.g., 802.11a/g/n) is based on OFDM. Taking 802.11a for an example, OFDM divides 20 MHz wireless channel into 64 orthogonal subcarriers, each of which has a bandwidth of 312.5 KHz. Every subcarrier carries independent symbols in parallel. The composite signal of 64 subcarriers is referred as an OFDM symbol. The duration of an OFDM symbol can be considered as a time slot that equals to 4 us in 802.11a/g. As shown in Fig. 1(a), a symbol is a 2-D time-frequency resource unit in OFDM. The basic idea of CoS is to intentionally insert silence symbols on the selected n weak subcarriers and embed information into intervals between inserted silence symbols. For simplicity, we assume $n = 6$ weak subcarriers are selected to convey control messages and are logically numbered from 1 to 6 in Fig. 1(a). Let i denote slot index, j denote subcarrier index, and $S_{i,j}$ denote a symbol with location coordinate (i, j). The $S_{1,1}$ is a silence symbol to indicate the start of control messages and the interval between silence symbols is the number of symbols. Suppose an interval carries k bits ($k = 4$ in CoS), then the maximum interval length is 15. For example, CoS divides 24 bits "001001101000001110100111" into six groups where $\{$"0010" $\rightarrow$ 2, "0110" $\rightarrow$ 6, ..., "0111" $\rightarrow$ 7$\}$. Fig. 1(a) shows the corresponding location distribution of inserted silence symbols and we can see that the interval between $S_{1,4}$ and $S_{2,5}$ is 6 corresponding to "0110". The OFDM signal for time slot 4 including 6 subcarriers in frequency domain is shown in Fig. 1(b), and silence symbols can be detected by symbol level energy detection [3] [5] in frequency domain.

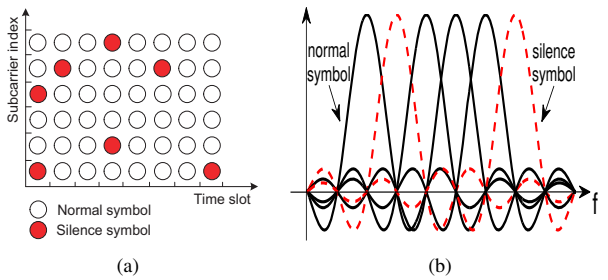


Fig. 1. (a) The control bits are encoded into intervals between silence symbols on OFDM-based PHY layer. (b) OFDM signal (time slot 4) including 6 subcarriers in frequency domain.

The key principle behind the design of CoS is to ensure the inserted silence symbols can be recovered correctly by the code redundancy in channel code existed in the physical layer. In following parts, we will present our experimental observations to demonstrate the feasibility of CoS.

B. Experimental Platform

We carry out experiments using two Sora devices deployed in our indoor laboratory. Sora provides a fully featured IEEE 802.11a implementation by a software WiFi driver. The PHY layer parameters such as channel code, modulation, and power allocation are set to 802.11a default values. Note that the 802.11a channel contains 64 subcarriers, of which there are 12 guard subcarriers, 4 pilot subcarriers, and 48 data subcarriers. There is no noticeable interference in our experiments.

C. The SNR Gap

Measure method: We vary the positions of Sora receiver to obtain various channel SNRs. The data rate adaptation scheme [6] is adopted to adjust data rate according to the receiver's measured SNR provided by network interference card (NIC). The minimum required SNRs for selected data

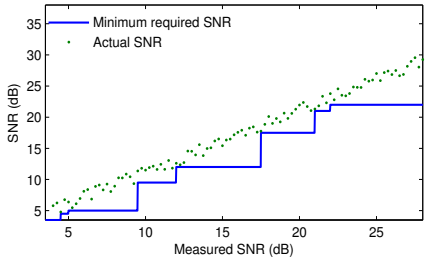


Fig. 2. The SNR gap between the minimum required SNR and the actual channel SNR in our tests using 802.11a.

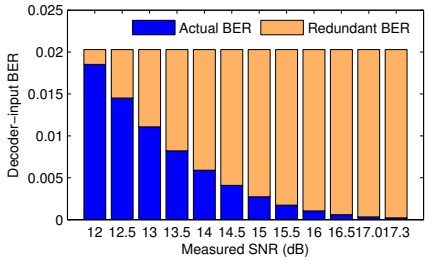


Fig. 3. The decoder-input BERs versus measured SNRs when data rate is 24 Mbps.

rates to successfully decode transmitted data packets are defined in IEEE 802.11a standard. We use channel sounder equipment to collect actual channel SNRs.

Results: Based on our experiments, the measured SNRs, actual SNRs, and minimum required SNRs are plotted in Fig. 2. We can clearly see the gap between the minimum required SNR and the actual SNR, and the actual SNR is always higher than the minimum required SNR. For example, when the measured SNR provided by receiver's NIC is 15 dB corresponding to selected data rate of 24 Mbps, the minimum required SNR for this data rate is 12 dB but the actual SNR is 16.7 dB. Thus the SNR gap is 4.7 dB. This SNR gap is mainly due to current data rate scheme. Since data rates are discrete while the metric value of SNR is continuous [1], the perfect one-to-one matching from data rates to channel SNRs is impossible. There are only eight data rates in IEEE 802.11a standard while the SNR range is large. Because of this staircase rate adjustment, the sender is forced to select a lower data rate even if its actual channel condition is at a SNR higher than the minimum required. In addition, the SNR estimation provided by NIC ignoring frequency selective fading also leads to this SNR gap, and the measured SNR is dragged to a low value by those fading subcarriers [7]. Such SNR gap means the actual number of bit errors introduced by wireless transmissions is much less than the corresponding channel code can handle, so the code redundancy in channel code is wasted. To futher understand the effect of SNR gap on the channel code, when data rate is 24 Mbps corresponding to the minimum required SNR of 12 dB, Fig. 3 plots the relationship between decoder-input bit error rates (BERs) and measured SNRs. Compared to the decoder-input BER at the minimum

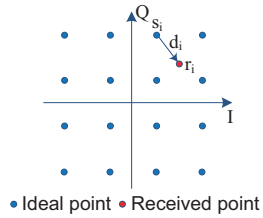


Fig. 4. The distortion of a 16QAM symbol in constellation diagram.

required SNR of 12 dB, the redundant BER is the extra BER that the decoder can tolerate. Obviously, the redundant BER increases with the increment of measured SNR.

Based on the above observations, CoS will take advantage of the existing SNR gap to correct those inserted silence symbols. However, a closer look at Fig. 2 reveals that when the measured SNR gets close to the minimum required SNR but not yet triggers a lower data rate, the SNR gap is very small. There is a limited available correction capability for CoS because the channel code is mainly consumed by wireless fading. As in Fig. 3, when the measured SNR gets close to 12 dB, the available redundant BER is small. To further enhance the capacity of free control messages, in addition to passively exploiting the existing SNR gap, we also need to proactively utilize the correction capability of channel code by carefully designing the distribution of silence symbols, which is based on our promising observations in next part.

D. The Distribution of Erroneous Symbols

Metric for subcarrier conditions: The error vector magnitude (EVM) is originally used to characterize channel conditions at symbol level [4] [8], and it represents the deviation of the received symbol position away from its idle symbol position in the constellation space. To capture the channel condition at subcarrier level, we newly define per subcarrier EVM as follows.

$$EVM = \sqrt{\frac{\frac{1}{L}\sum_{i=1}^{L}|\vec{r_i}-\vec{s_i}|^2}{\frac{1}{M}\sum_{m=1}^{M}|\vec{s_m}|^2}}, \quad (1)$$

where L is the number of transmitted symbols per data subcarrier, r_i is the received constellation point of i-th transmitted symbol, and s_i is the ideal constellation point of i-th transmitted symbol. M is the number of constellation points in the constellation diagram (for example, $M = 16$ for 16QAM) and s_m is m-th constellation point. As shown in Fig. 4, a received symbol position gets dispersed from its ideal position due to signal distortion, and the error vector for a symbol is $\vec{d_i} = \vec{r_i} - \vec{s_i}$. Thus EVM can be used to characterize subcarrier condition by symbol-level dispersions. Note that low EVM values correspond to good channel conditions.

Measure method: The Sora receiver is placed in three positions to measure frequency selective fading. Since the 802.11-based WiFi is originally designed for indoor environments and indoor mobile scenario is more challenging than indoor static

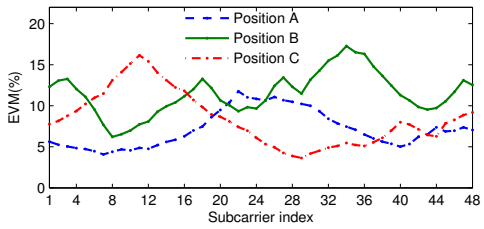


Fig. 5. Measured EVMs from 20MHz 802.11a channel with frequency selective fading in various positions.

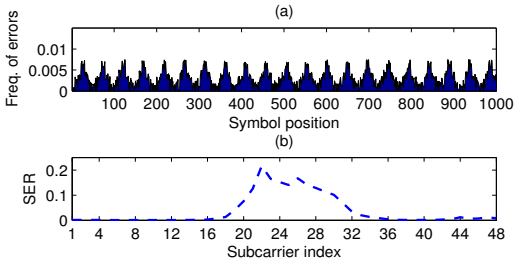
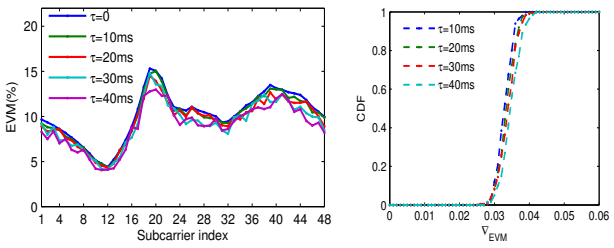


Fig. 6. Measurements in position A. (a) Frequency and distribution of symbol errors within a data packet. (b) Symbol error rate (SER) of data subcarriers.

scenario, only mobile traces are presented to demonstrate the temporal selectivity of indoor channels, and the Sora receiver moves at walking speed (about 3.4 mph) in our laboratory. A fixed data packet whose symbol values are known to both the sender and the receiver is used in our experiments.

Frequency selective fading: Fig. 5 illustrates measured EVM of 48 data subcarriers in three different positions. We can clearly see that different data subcarriers exhibit very different EVMs and the difference in EVM can be up to 13% for a single link. Moreover, three links corresponding to three positions exhibit various degrees of frequency selective fading. Frequency diversity results from multi-path propagations induced by surrounding obstacles in wireless environments [9]. Such subcarrier fading diversity impacts the distribution of erroneous symbols.

Symbol-level error pattern: Fig. 6(a) shows experimental characterization of symbol errors within a packet. As we can see, the symbol error probabilities of each symbol position are very different and certain positions of symbols have higher error probabilities than others. For clarity, only the error probabilities of the first 1000 symbols are presented. In addition, Fig. 6(a) also clearly shows that there exists a period trend of error probabilities within a packet, and the length of this period approximates the number of data subcarriers in OFDM systems (48 data subcarriers in 802.11a/g). The above phenomenons result from frequency selective fading. Specifically, since the 802.11 standard assigns the same coding rate, modulation, and power to all subcarriers [10], ignoring frequency diversity, symbols in different data subcarriers experience various signal distortions and the deep fading will be repeated for every symbol in those weak data subcarriers. The corresponding symbol error rates (SERs) for data subcarriers



(a) (b)

Fig. 7. Temporal selectivity of subcarriers in the indoor mobile scenario. (a) EVM variation of different subcarriers with time gap τ. (b) Cumulative distribution function (CDF) of ∇_{EVM}.

are plotted in Fig. 6(b). We can clearly see that quite a few of data subcarriers are more vulnerable to signal distortions than others and have higher SERs. Therefore, the distribution of erroneous symbol positions within a packet verifies the fact that those weak data subcarriers produce most of the erroneous symbols. Such deterministic property of symbol error pattern within a packet will be exploited to design CoS in those weak data subcarriers. Since the erroneous symbols in those weak data subcarriers will be corrected by the channel code to drive down BER across the data packet, inserting silence symbols onto erroneous symbols can avoid introducing too much new symbol errors into data packets. In other words, instead of being corrupted by wireless fading at the receiver, certain error-prone symbols are erased by CoS at the sender based on the prediction of error-prone symbol positions. Therefore, we will select those weak data subcarriers to design CoS according to our subcarrier selection algorithm.

Temporal stability: To accurately predict symbol error locations within a data packet, the frequency diversity should change slowly over time so that the prediction of future per subcarrier condition is possible using the current measurement feedbacks. By varying the time gap τ between transmitted data packets, we evaluate the temporal selectivity of wireless channel in indoor mobile scenarios, and Fig. 7(a) shows snapshots of the quality of all 48 data subcarriers under various time gaps τ and reveals that per subcarrier EVM is relatively stable over times.

To quantify the temporal selectivity, we define the normalized EVM change as metric:

$$\nabla_{EVM}(\tau) = \frac{\|\vec{D}(t) - \vec{D}(t+\tau)\|_2}{\|\vec{D}(t+\tau)\|_2}, \tag{2}$$

where the vector $\vec{D}(t)$ represents the magnitudes of the error vectors of all 48 data subcarriers at time t, i.e., $\vec{D}(t) = \{|\vec{d_1}(t)|, |\vec{d_2}(t)|, ..., |\vec{d_{48}}(t)|\}$, and $\|\cdot\|_2$ is the squared Euclidean norm ($\|\vec{e}\|_2 = \sqrt{\sum_k \vec{e}(k)^2}$ for the vector $\vec{e}$) [9]. Fig. 7(b) plots the cumulative distribution functions (CDF) of ∇_{EVM} with various time gap τ. As we have seen, the ∇_{EVM} difference between two consecutive time gaps is small, and ∇_{EVM} changes within 1% even if $\tau = 30ms$. The significant temporal selectivity suggests that CoS can confidently predict

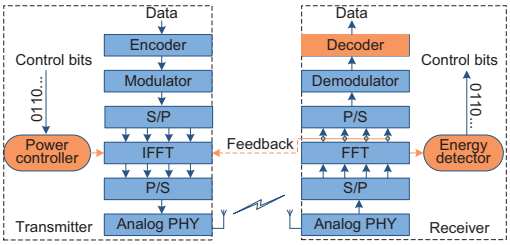


Fig. 8. Architecture of CoS system. The orange blocks are CoS extensions to OFDM-based 802.11a.

the future EVM for each data subcarrier using the current measurement feedbacks in indoor environments.

The feasibility of CoS is built up on the above observations and we argue that not only the number of inserted silence symbols but also their distribution will affect the capacity of free control messages.

III. CoS Design

In this section, we describe the detailed implementation of CoS. We first present the overall system architecture of CoS. We then describe the detailed designs including modulation/demodulation of control messages, threshold selection of energy detection, subcarrier selection feedback, erasure Viterbi decoding (EVD), and adaptive rate selection of control messages.

A. Overall System Architecture

We design and implement CoS based on the 802.11a physical layer. Fig. 8 presents the overall system architecture of CoS. The functions of each newly added component can be achieved in driver-level changes without requiring any modifications to hardware. It is easy for CoS to be integrated into existing wireless systems immediately.

At a high level, CoS works as follows. The transmission of data packets is the same as traditional procedure except the Viterbi decoder that is changed by the proposed erasure Viterbi decoding. Based on the feedback indicating the set of selected data subcarriers used to convey control messages, the power controller module at the transmitter encodes control bits by differentiating interval length. At the receiver side, the energy detector module detects and interprets control bits on those data subcarriers known to the receiver which provides the feedback of selected data subcarriers to the transmitter. Note that we adopt CoS to transmit feedback information, which is built on top of the transmission of ACK frame.

B. Modulation/Demodulation of Control Messages

To transmit control messages (or sequence of binary bits), the power controller module conducts power allocation at the granularity of symbols, which is easily achieved by Inverse Fast Fourier Transform (IFFT). In OFDM systems, the transmitter relies on IFFT to achieve OFDM modulation that transforms frequency domain data symbols into time domain OFDM symbols. By performing N-point IFFT, we can obtain an OFDM signal by

$$x[n] = \frac{1}{N}\sum_{k=0}^{N-1} X[k]e^{j2\pi\frac{kn}{N}}, \quad n = 0, 1, ..., N-1 \qquad (3)$$

where N is the total number of subcarriers, $X[k]$ is a modulated data symbol on the subcarrier k, and $x[n]$ is the time domain OFDM signal at sample time n. In normal data transmissions, the modulated symbol vector fed into IFFT is $\mathbf{X} = \{X[0], X[1], ..., X[N-1]\}$. For example, the modulated symbols $1 + 0i$ and $-1 + 0i$ are used in BPSK modulation scheme. To implement silence symbols on subcarrier k, the transmitter can simply feed 0 instead of modulated data symbols on subcarrier k when performing IFFT, leading to zero power on the corresponding position of this data symbol. Therefore, a silence symbol is a data symbol whose power is zero and is intentionally deactivated by the transmitter.

At the receiver, the Fast Fourier Transform (FFT) operation transforms received OFDM symbols $y[n]$ into frequency domain modulated symbols $Y[k]$. We can obtain the original data symbol on subcarrier k by

$$Y[k] = \sum_{n=0}^{N-1} y[n]e^{-j2\pi\frac{nk}{N}}, \quad k = 0, 1, ..., N-1. \qquad (4)$$

The result of FFT operation presents the magnitude on every subcarrier in frequency domain [3]. Based on the FFT result, the energy detector module conducts symbol-by-symbol energy detection to locate silence symbols and interpret control messages. If a symbol with zero power is transmitted, high magnitude will not be observed at the corresponding data symbol position.

C. Threshold Selection of Energy Detection

In practical implementation, the energy of those silence symbols may not be zero due to the existence of noise, so the energy detection threshold is selected based on noise floor. Because the selected data subcarriers used to convey control messages may experience different deep fading on various channel conditions, the dynamic adjustment of energy detection threshold is necessary to distinguish subcarrier with only noise from subcarrier with deep fading signal.

We propose pilot aided estimation scheme to dynamically obtain noise energy. In pilot subcarrier i, let y_i denote the received signal containing the pilot signal and the noise, then we get

$$y_i = H_i x_i + n_i, \qquad (5)$$

where the channel coefficient of pilot subcarrier i is H_i representing the channel attenuation and the phase shift, x_i is the transmitted pilot signal, and n_i is the corresponding noise. The H_i can be estimated by the training symbols contained in physical preamble [11]. In addition, the pilot signal x_i is known to the receiver. Therefore, the corresponding noise in pilot subcarrier i is estimated by

$$n_i = y_i - H_i x_i. \qquad (6)$$

Note that the noise in wireless channel is usually white noise, so the noise energy is distributed evenly across all subcarriers. Thus, n_i is the same for all OFDM subcarriers, i.e., $\eta = n_i, \forall i$. Based on the estimated noise floor η, CoS sets the energy detection threshold.

D. Subcarrier Selection Feedback

To provide channel condition at subcarrier level, the receiver calculates per subcarrier EVM. The calculation of EVM relies on the comparison between the received symbols and the corresponding ideal constellation positions (i.e., transmitted symbols) [4]. However, since the receiver dose not which symbol is transmitted, the ideal constellation positions of received symbols are unknown in practical communications. To address this challenge, CoS calculates per subcarrier EVM after the received data packet passes cyclic redundancy check (CRC), which means the entire data packet is correctly decoded and all received data bits within this data packet are correct. Then, we reconstruct the transmitted symbols by re-mapping data bits to obtain corresponding ideal constellation positions. Based on reconstructed symbols and received symbols, all the EVMs for 48 data subcarriers are calculated. Note that the silence symbols are excluded from the calculation of EVM.

The data rate selection scheme [7] is adopted at receiver. After the data rate is selected for the next data packet transmission, the receiver will select those weak data subcarriers to design CoS. For the modulation of the selected data rate, let D_m denote the minimum distance between the two nearest constellation points in the constellation diagram. Then, the receiver compares per subcarrier EVM value with $\frac{D_m}{2}$ to analyze and predict whether data subcarrier exits erroneous symbol in the next data packet transmission. If EVM value is bigger than $\frac{D_m}{2}$, the transmitted symbol can not be demodulated correctly because it falls in a far away constellation position, and this data subcarrier is selected as control subcarrier. A bit vector V is used to indicate the set of selected control subcarriers. The feedback of the set of data subcarriers selected as control subcarriers only occupies one OFDM symbol where a silence symbol represents that the corresponding subcarrier is selected as control subcarrier.

E. Erasure Viterbi Decoding

The Viterbi algorithm is widely used to decode convolutional code, but it is an error-only decoding scheme where the silence symbols are treated as symbol errors. However, previous works [12] [13] have shown that erasures are preferable to errors and erasures affect the decoding performance in forward error correction schemes.

To achieve error-and-erasure decoding in CoS, we present erasure Viterbi decoding (EVD) where erasure is incorporated into the conventional Viterbi decoding. Since the silence symbols are located by symbol-level energy detection, the decoder can conduct erasure decoding with perfect information of the distribution of erased symbols in CoS. The bit-interleaved coded modulation (BICM) is adopted in current IEEE 802.11a/g/n standards [12], so a demodulator, a deinterleaver and a Viterbi decoder are contained in the conventional BICM decoding process. Let e_k denote the erasure indicator to indicate whether the kth symbol is a silence symbol, where $e_k = 1$ is a normal symbol and $e_k = 0$ is a silence symbol. Thus, the kth received symbol y_k can be represented by the pair (y_k, e_k), and all silence symbols are marked before demodulation. If the demodulator input symbols are M-ary symbols, the bit metrics for all the $m = \log M$ bits $d_i = b(b = 0, 1; i = 1, 2, ...m)$ with regard to the kth received symbol are calculated by

$$\begin{aligned}\lambda(d_i = b) &= \log P(d_i = b|y_k, e_k) \\ &= \begin{cases} \log P(d_i = b|y_k), & \text{if } e_k = 1 \\ 0, & \text{if } e_k = 0 \end{cases}\end{aligned} \tag{7}$$

In EVD, we ignore the bit metrics that correspond to a silence symbol, i.e., $\lambda(d_i = b) = 0$ if $e_k = 0$. For each normal symbol, as in [12] [13], we can obtain the log likelihood function in (7) by

$$\begin{aligned}\log P(d_i = b|y_k) &\propto \log \sum_{x_k \in \chi_b^i} P(y_k|x_k) \\ &\approx \max_{x_k \in \chi_b^i} \log P(y_k|x_k),\end{aligned} \tag{8}$$

where $\chi_b^i = \{\mu(d_1, ..., d_i, ..., d_m)|d_i = b\}$ represents the signal subset with the ith bit being equal to $b \in \{0, 1\}$, x_k is the kth transmitted symbol, and μ is the mapping function that maps each m-tuple code bits into an M-ary symbol. The demodulated bits are then deinterleaved, which breaks the correlation between the bits in the same symbol. Therefore, the bits with $\lambda(d_i = b) = 0$ in silence symbols are spread across different positions in a codeword. Finally, the deinterleaved bits are inputted into the Viterbi decoder.

Compared to the conventional Viterbi decoding process, the proposed EVD dose not modify the existing Viterbi decoder, but only the calculation of bit metrics. In EVD, the silence symbols are treated as erasure and the bit metrics with regard to silence symbols are taken as zero during the calculation of the path metric. Therefore, the implementation of EVD is simple and it can be directly built up on the standard Viterbi decoder architecture.

F. Adaptive Rate Selection of Control Messages

The rate of control messages depends on the total number of inserted silence symbols. In practical system, the rate of control messages should be dynamically adjusted according to channel conditions, which ensures that the total number of inserted silence symbols dose not exceed the correction capability of channel code so that CoS dose not destroy the decoding of original data packets. Based on our extensive experiments that are presented in the next section, we can obtain the mapping between channel SNRs and control message rates. As with data rate selection in IEEE 802.11, a lookup table is created to dynamically select control message rate according to the receiver's channel SNR. If the transmission of data packet fails, the sender will not receive the channel condition feedback. It will select the lowest rate of control messages in next transmission.

IV. Evaluation

A. CoS Implementation

The software define radio platform Sora is used to build our current prototype of CoS using SDK version 1.5. Sora platform provides a software radio WiFi driver, SoftWiFi, and CoS's current implementation is added on top of it. As shown in the system architecture in Fig. 8, we achieve all newly added components of CoS by the Sora User-mode Extension API, which does not require costly hardware modifications.

B. Capacity of Free Control Messages

In this part, our experiments measure the capacity of free control messages under various channel conditions. In other words, we will answer the question that how many silence symbols can be inserted in CoS, while ensuring not to destroy the original data packet.

Method: We deploy two Sora nodes to conduct experiments in indoor lab. The SNR-based adaptation scheme [6] is adopted to adjust data rate. A fixed 1024 bytes data packet is transmitted repeatedly by the sender and the frame aggregation scheme is adopted. Control messages are generated randomly. To run experiments under various channel SNRs, the receiver platform is placed on different positions to measure the maximum number of silence symbols per second (denoted by R_m) CoS can insert. We conduct our measurements during daytime with normal human traffic, and there is no strong interference in our experiments. To satisfy the desired packet reception rate (PRR) of 99.3%, we adjust the rate of inserted silence symbols (denoted by R) until we can obtain the desired PPR and record the corresponding R as R_m. A data rate is a combination of modulation and code rate. The six data rates defined in IEEE 802.11a are experimented. For example, the combination (16QAM,3/4) produces data rate of 36 Mbps in IEEE 802.11a. Note that the measured SNR used in this section indicates the channel SNR reported by the rceiver's NIC.

Results: Based on our experiment results, Fig. 9 depicts the R_m as a function of measured SNR. The minimum value of R_m is 33,000 corresponding to the measured SNR of 22.4dB, i.e., 33,000 silence symbols per second can be inserted at 22.4dB. Since CoS embeds $k = 4$ bits into a interval between inserted silence symbols in our implementation, the corresponding capacity of control messages is $132Kbps$. When the measured SNR falls between 7.1dB and 9.5dB, we can obtain the maximum R_m of 148,000. Therefore, the rate of control messages should be adjusted according to channel conditions.

Analysis: Fig. 9 presents two interesting results. First, we can see that the capacity of control messages is proportional to the available code redundancy rather than the measured SNR. Within the SNR range corresponding to a given data rate, as the measured SNR increases, R_m increases significantly. However, when the measured SNR exceeds a certain threshold, we only obtain a slight increase in R_m. The main reason is that the increase of measured SNR leads to the increase of SNR gap, which means the number of erroneous symbols induced by wireless transmissions reduces and CoS can take advantages

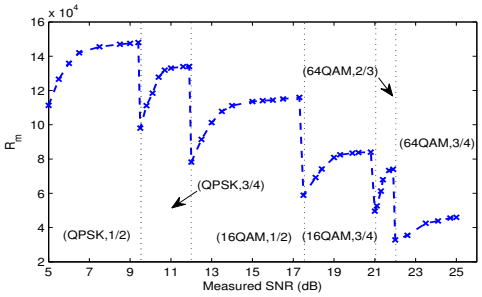
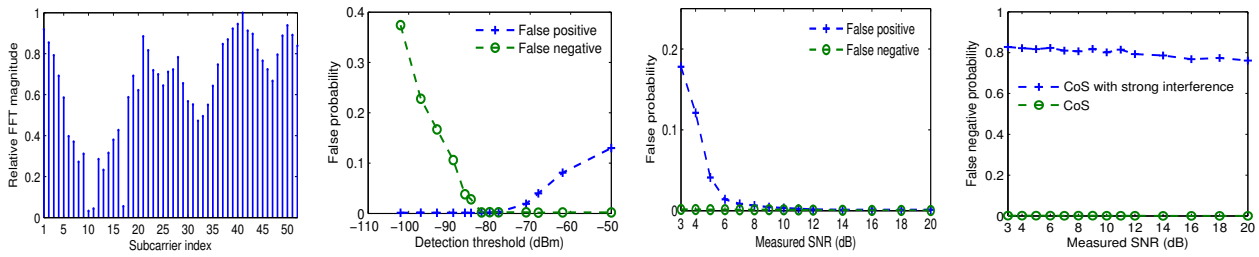


Fig. 9. The maximum number of silence symbols per second (R_m) for various channel conditions.

of more code redundancy in the channel code to recover data symbols erased by silence symbols. Since the increasing rate of available code redundancy decreases with the increase of measured SNR, R_m does not obtain significant increase with the further increase of measured SNR (or SNR gap). When the measured SNR is large enough, it has little impact on R_m. Second, the experiment results also reveal that different data rates have various upper bounds of R_m. For a same modulation scheme, various code rates produce various upper bounds of R_m. For example, (16QAM,1/2) and (16QAM,3/4) adopt the same modulation scheme, but the upper bound of R_m of (16QAM,1/2) is larger than (16QAM,3/4). When the measured SNR is far enough from the minimum required SNR, the channel code is mainly consumed by silence symbols, but 1/2 code rate has larger error correcting capability than 3/4 code rate. On the other hand, for a same code rate, a smaller upper bound of R_m is obtained when a higher modulation rate is adopted. For example, (QPSK,3/4) and (16QAM,3/4) adopt the same code rate, but the upper bound of R_m of (16QAM,3/4) is smaller than (QPSK,3/4). This is because for a larger modulation rate, more data bits are contained in a data symbol, and more code redundancy in the channel code is consumed to correct a silence symbol. The number of data bits per symbol is 2 in QPSK while the number of data bits per symbol is 4 in 16QAM. Therefore, we can also see that the upper bound of R_m shows a decreasing trend with the increase of measured SNR.

C. Detection Accuracy of Silence Symbols

In this part, we evaluate the feasibility of symbol-level energy detection in various channel conditions. The received signal is converted into a frequency domain signal by FFT and the FFT result presents different subcarrier magnitudes. Fig. 10(a) presents the relative FFT magnitudes of 52 OFDM subcarriers where 48 data subcarriers and 4 pilot subcarriers are numbered logically from 1 to 52. The 8 contiguous data subcarriers [10,11,...,17] are selected to convey control messages. If silence symbols are transmitted, we will not observe high magnitudes on the corresponding data subcarriers. In Fig. 10(a), we can observe apparent magnitude differences between active subcarriers and inactive subcarriers and the data subcarriers 10, 11, and 17 are inactive subcarriers. The



(a) (b) (c) (d)

Fig. 10. (a) Relative FFT magnitudes of 52 OFDM subcarriers and the selected control subcarriers are [10,11,...,17]. (b) The impact of detection threshold on symbol level energy detection. (c) False positive and negative probabilities under various SNRs. (d) The impact of interference on false negative probability.

length of the interval between subcarrier 11 and subcarrier 17 is 5 corresponding to control bits "0101". The inactive subcarriers are clearly discernible and can be easily located through performing simple FFT.

To quantify the accuracy of symbol-level energy detection, we adopt two metrics, i.e., false positive and false negative. A false positive indicates that a silence symbols is detected but it is actually absent while a false negative indicates that CoS misses a silence symbol that is actually present. In practical system, the threshold of energy detection is slightly higher than the estimated noise floor. A silence symbol is detected when the energy of the corresponding subcarrier is below the detection threshold. When the measured SNR is 9.2dB, Fig. 10(b) plots false negative probability and false positive probability for different detection thresholds. If the detection threshold is too high, the deep fading symbols are falsely detected as silence symbols, so the false positive probability is high. If the threshold is too low, CoS misses certain silence symbols that are considered as normal symbols, so the false negative probability is high.

Impact of adaptive estimation: The accurate estimation of noise floor is important for energy detection and the noise floor is adaptively estimated under different channel states. 1,000 data packets are transmitted for accuracy evaluation under various values of channel SNR. As shown in Fig. 10(c), the false negative probability is below 0.01, even under a very low channel SNR. Fig. 10(c) also shows that as channel SNR decreases (below 6.3dB), the false positive probability slightly increases but is still at reasonably low level. For example, when measured SNR is as low as 3.2dB, the false positive probability is about 0.143. Under low channel SNRs, deep fading reduces the energy of the received signal, which results in the energy of the corresponding active subcarrier approaching to the noise floor thus causing an incorrect detection of inactive subcarrier. Although the false positive probability is slightly high under a low channel SNR range, but we stress that the typical working SNR region of WLANs is above 10dB [14], and the false positive probability is close to zero within this SNR region.

Impact of interference: The detection of silence symbols is most vulnerable to strong interference. For weak interference, it is regarded as noise. However, strong interference seriously affects false negative probability. In our measurements, pulse signal is sent randomly. As shown in Fig. 10(d), the false negative probability is very high in presence of strong interference. If strong interference falls onto a silence symbol and results in high energy of the corresponding inactive subcarrier (above the detection threshold), CoS misses the silence symbol that is falsely regarded as a normal symbol. Specifically, WLANs do exist interference from co-channel WLAN nodes or other devices such as ZigBee. We argue that data packet can not be decoded correctly under strong interference induced by hidden node or packet collision, so the receiver fails to obtain both data packet and control messages. In our design, we do not consider strong interference and we assume strong interference can be avoided by the MAC coordination scheme. Without strong interference, the false positive probabilities are below 0.01 under various channel SNRs.

V. Related Work

The work related to our CoS design falls in the following two areas, and we only present the most closely related work in each area.

Harnessing frequency diversity: There is a large body of works attempting to harness frequency diversity. Han et al. [15] presented detailed experiments to identify the bit error pattern induced by frequency diversity in WLANs. Rahul et al. [10] presented FARA, a frequency-aware rate adaptation scheme that adopts various bit rates across different OFDM subbands. However, the system complexity of FARA limits its practical application. In addition, the frequency diversity can be used to provide unequal error protection where important bits are transmitted in more reliable OFDM subcarriers [9] [16]. Compared with above works, CoS leverages frequency diversity to embed silence symbols onto those weak data subcarriers. By this way, CoS reduces newly introduced symbol errors to enhance the total number of silence symbols that can be inserted in data packet.

Side channel design: There have been some works on designing side channel using physical layer techniques. To achieve communication between heterogeneous wireless networks, novel communication frameworks are designed in [14] [17] [18]. The proposed CoS targets quite a different scenario. Magistretti et al. [19] replaced certain control pack-

ets with control signals, which is achieved by a dictionary of correlatable symbol sequences. However, this work still consumes extra airtime to transmit 802.11 preamble at the lowest data rate. Exploiting the link margin or interference margin to convey information has emerged in [20] [21]. CoS is motivated by their works. Both [20] and [21] utilized intended inference to convey messages. However, their schemes have many limitations. First, they resolve contention in data plane by transferring it into control plane, so it is easy to corrupt the original data packet due to uncontrolled contention in control plane in practical networks. Second, since data packets and intended inference signals are transmitted by different nodes (non-synchronization), it is a challenge to ensure an intended inference signal accurately fall onto one data symbol. Third, the power of intended inference signal is 64 times the data symbol power, which consumes significant energy. In contrast, CoS utilizes silence symbols to encode information and both data packet and control message are transmitted by the same node, which avoids above limitations. Most importantly, CoS exploits frequency selective fading to obtain larger capacity of free control messages by designing the distribution of inserted silence symbols. In addition, the interference margin also has been used for power control [22] [23]. Muqattash et al. [22] leveraged interference margin to achieve concurrent transmissions in ad hoc networks. Chen et al. [23] leveraged it for spectrum access in cognitive radio networks. Different from their applications, CoS is designed for control messages transmissions in indoor WLANs.

VI. Conclusion

In this paper, our measurements show that there does exist a SNR gap due to stair-case data rate adjustment and inaccurate SNR estimation in current WLANs. We turn the wasted SNR gap into wealth by designing a novel communication strategy called CoS, which enables us to convey free control messages without consuming extra channel resources. The SNR gap is utilized to obtain correction capability of the existing channel code to correct inserted silence symbols in CoS. Moreover, based on the promising observation that the error-prone symbol positions within a data packet are non-uniform due to frequency selective fading, we design CoS on those weak data subcarriers to reduce new symbol errors introduced by CoS, which can further enhance the capacity of free control messages. If the rate of free control messages is selected according to channel conditions, CoS dose not destroy the correct decoding of data packets and does not compromise the original data throughput. We solve some practical issues in designing CoS and conduct extensive experiments to demonstrate the feasibility of CoS.

Acknowledgment

This work was supported in part by the Natural Science Foundation of China (NSFC) under Grants 61202140 and 61328208, by the Program for New Century Excellent Talents in University under Grant NCET-13-0548, and by the Fundamental Research Funds for the Central Universities under Grand WK2101020006. The work of J. Liu and Y. Fang was also partially supported by the US National Science Foundation under grants CNS-1409797 and CNS-1343356.

References

[1] H. Cui, C. Luo, K. Tan, F. Wu, and C. W. Chen, "Seamless rate adaptation for wireless networking," in *Proc. ACM MSWiM*, 2011, pp. 437–446.

[2] G. Wang, S. Zhang, K. Wu, Q. Zhang, and L. M. Ni, "Tim: Fine-grained rate adaptation in wlans," *IEEE Trans. Mobile Comput.*, vol. 15, no. 3, pp. 748–761, 2016.

[3] S. Sen, R. Roy Choudhury, and S. Nelakuditi, "No time to countdown: Migrating backoff to the frequency domain," in *Proc. ACM MobiCom*, 2011, pp. 241–252.

[4] S. Sen, N. Santhapuri, R. R. Choudhury, and S. Nelakuditi, "Accurate: Constellation based rate estimation in wireless networks." in *Proc. USENIX NSDI*, 2010, pp. 175–190.

[5] B. Roman, F. Stajano, I. Wassell, and D. Cottingham, "Multi-carrier burst contention (mcbc): Scalable medium access control for wireless networks," in *Proc. IEEE WCNC*, 2008, pp. 1667–1672.

[6] G. Holland, N. Vaidya, and P. Bahl, "A rate-adaptive mac protocol for multi-hop wireless networks," in *Proc. ACM MobiCom*, 2001, pp. 236–251.

[7] D. Halperin, W. Hu, A. Sheth, and D. Wetherall, "Predictable 802.11 packet delivery from wireless channel measurements," *ACM SIGCOMM Computer Communication Review*, vol. 41, no. 4, pp. 159–170, 2011.

[8] R. A. Shafik, M. S. Rahman, and A. Islam, "On the extended relationships among evm, ber and snr as performance metrics," in *Proc. IEEE ICECE*, 2006, pp. 408–411.

[9] A. Bhartia, Y.-C. Chen, S. Rallapalli, and L. Qiu, "Harnessing frequency diversity in wi-fi networks," in *Proc. ACM MobiCom*, 2011, pp. 253–264.

[10] H. Rahul, F. Edalat, D. Katabi, and C. G. Sodini, "Frequency-aware rate adaptation and mac protocols," in *Proc. ACM MobiCom*, 2009, pp. 193–204.

[11] M. Vutukuru, H. Balakrishnan, and K. Jamieson, "Cross-layer wireless bit rate adaptation," *ACM SIGCOMM Computer Communication Review*, vol. 39, no. 4, pp. 3–14, 2009.

[12] T. Li, W. H. Mow, V. K. Lau, M. Siu, R. S. Cheng, and R. D. Murch, "Robust joint interference detection and decoding for ofdm-based cognitive radio systems with unknown interference," *IEEE J. Sel. Areas Commun.*, vol. 25, no. 3, pp. 566–575, 2007.

[13] J. Geist and J. Cain, "Viterbi decoder performance in gaussian noise and periodic erasure bursts," *IEEE Trans. Commun.*, vol. 28, no. 8, pp. 1417–1422, 1980.

[14] X. Zhang and K. G. Shin, "Gap sense: Lightweight coordination of heterogeneous wireless devices," in *Proc. IEEE INFOCOM*, 2013, pp. 3094–3101.

[15] B. Han, L. Ji, S. Lee, B. Bhattacharjee, and R. R. Miller, "Are all bits equal?: experimental study of ieee 802.11 communication bit errors," *IEEE/ACM Trans. Netw.*, vol. 20, no. 6, pp. 1695–1706, 2012.

[16] X. L. Liu, W. Hu, Q. Pu, F. Wu, and Y. Zhang, "Parcast: soft video delivery in mimo-ofdm wlans," in *Proc. ACM MobiCom*, 2012, pp. 233–244.

[17] S. M. Kim and T. He, "Freebee: Cross-technology communication via free side-channel," in *Proc. ACM MobiCom*, 2015, pp. 317–330.

[18] K. Chebrolu and A. Dhekne, "Esense: communication through energy sensing," in *Proc. ACM MobiCom*, 2009, pp. 85–96.

[19] E. Magistretti, O. Gurewitz, and E. W. Knightly, "802.11 ec: collision avoidance without control messages," in *Proc. ACM MobiCom*, 2012, pp. 65–76.

[20] K. Wu, H. Li, L. Wang, Y. Yi, Y. Liu, D. Chen, X. Luo, Q. Zhang, and L. M. Ni, "hjam: Attachment transmission in wlans," *IEEE Trans. Mobile Comput.*, vol. 12, no. 12, pp. 2334–2345, 2013.

[21] A. Cidon, K. Nagaraj, S. Katti, and P. Viswanath, "Flashback: Decoupled lightweight wireless control," *ACM SIGCOMM Computer Communication Review*, vol. 42, no. 4, pp. 223–234, 2012.

[22] A. Muqattash and M. Krunz, "Power controlled dual channel (pcdc) medium access protocol for wireless ad hoc networks," in *Proc. IEEE INFOCOM*, vol. 1, 2003, pp. 470–480.

[23] Y. Chen, G. Yu, Z. Zhang, H.-h. Chen, and P. Qiu, "On cognitive radio networks with opportunistic power control strategies in fading channels," *IEEE Trans. Mobile Comput.*, vol. 7, no. 7, 2008.