This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2019.2924000, IEEE Transactions on Mobile Computing

Turning Waste into Wealth: Free Control Message Transmissions in Indoor WiFi Networks

Bing Feng, Chi Zhang, *Member, IEEE,* Jianqing Liu, and Yuguang Fang, *Fellow, IEEE*

Abstract—A practical WiFi system only achieves a discrete data rate adjustment due to hardware constraints while channel signal-to-noise ratio (SNR) is continuous. This mismatch leads to the SNR gaps. In this paper, we introduce a novel communication mechanism, CoS (Communication through Silent subcarriers), which turns the wasted SNR gaps into new opportunities for transmitting control messages for free. Compared with traditional piggybacking schemes, CoS is more reliable to transmit control messages from one node to many nodes. In CoS, silent subcarriers are inserted into data packets and the intervals between adjacent silent subcarriers are utilized to encode information. Since the wasted SNR gap results in under-utilization of the channel code, the data bit errors induced by silent subcarriers are corrected by the correcting capability of the existing channel code as long as we carefully design the total number of inserted silent subcarriers. Based on CoS, we design CoS-MAC to validate the effectiveness of CoS. We measure the throughput of free control messages achieved by CoS under various channel conditions and conduct simulations to show the throughput gain achieved by CoS-MAC over the existing schemes.

Index Terms—WiFi networks, control signaling, MAC, SNR gap, OFDM, frequency selective fading.

1 Introduction

Control messages are essential for improving the performance of various applications such as medium access, scheduling, and resource allocation in WiFi networks. However, with traditional piggybacking schemes adding new control fields in the medium access control (MAC) header, control message exchanges among nodes lack reliability. Specifically, a data packet's data rate is selected according to its intended receiver's channel condition, and so unintended receivers in the WiFi network may not be able to correctly decode the data packet's MAC header[1] to obtain the conveyed control messages. In addition, traditional piggybacking schemes consume extra channel resources (bandwidth or time) and modify the original data packet format defined in the IEEE 802.11 standards to add new control fields.

In this paper, we utilize the features of OFDM (Orthogonal Frequency Division Multiplexing) to design CoS (Communication through Silent subcarriers), a novel communication mechanism in OFDM-based WiFi networks (e.g., 802.11a/g/n). In CoS, we insert silent subcarriers into data packets. An inserted silent subcarrier is a subcarrier with zero transmission power within one OFDM symbol. CoS leverages the intervals between silent subcarriers to encode information. The energy detection at the granularity of subcarriers [3] [4] is utilized to locate silent subcarriers. Unlike traditional piggybacking schemes, CoS extracts the embedded control messages via physical layer energy detection instead of using conventional data packet decoding that requires higher SNR. In CoS, even if a node's neighboring nodes cannot correctly decode its transmitted data packets because they may have worse channel conditions than the data packets' intended receiver, they may still correctly obtain the embedded control messages. Therefore, compared with traditional piggybacking schemes, CoS is more reliable to transmit control messages from one node to other nodes in the network. Since CoS does not change the original 802.11 data packet structure, a legacy 802.11 node can process the data packets transmitted by a node implementing CoS but ignores the embedded control messages at the physical layer. In addition, CoS exploits the wasted SNR gaps to convey lightweight control messages without consuming additional channel resources (i.e., not sacrificing the original data throughput).

In CoS, some data bits are erased deliberately within a data packet due to inserted silent subcarriers, which results in data bit errors. The feasibility of CoS is based on the observation that a practical WiFi system exhibits considerable SNR gap. In wireless transmissions, the best data rate, a combination of modulation and channel code, is selected to fight against transmission failure according to channel condition (e.g., SNR) [5]. A practical WiFi system only achieves a discrete data rate adjustment due to the limited number of modulation types and code rates, but channel SNR is continuous [6] [7]. As a result, wireless networks exist SNR gap between the actual channel SNR and the minimum channel SNR required for the currently selected data rate. The SNR gap results in under-utilization of the channel code, which is utilized to design CoS. Thus, in our CoS, data bits erased by inserted silent subcarriers can be recovered by the correcting capability of the existing channel code as

- *B. Feng and C. Zhang are with the School of Information Science and Technology, University of Science and Technology of China, Hefei 230027, P. R. China. E-mail: fengice@mail.ustc.edu.cn, chizhang@ustc.edu.cn.*
- *J. Liu is with the Department of Electrical and Computer Engineering, University of Alabama in Huntsville, Huntsville, Alabama 35899, USA, Email: jianqing.liu@uah.edu.*
- *Y. Fang is with the Department of Electrical and Computer Engineering, University of Florida, Gainesville, Florida 32611, USA. E-mail: fang@ece.ufl.edu.*

A preliminary version of this paper appeared in IEEE ICDCS'17 [1].

1. According to Section 17.3.2 in the IEEE 802.11 standard [2], the MAC header is transmitted at the same data rate with the MAC frame body in practical WiFi communication systems.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2019.2924000, IEEE Transactions on Mobile Computing

long as we carefully design the total number of inserted silent subcarriers. Both data bits erased by inserted silent subcarriers and erroneous data bits induced by wireless transmissions are treated as data bit errors and should be corrected by the channel code to ensure correct decoding of the original data packet. Since the SNR gap results in under-utilization of the channel code, the correcting capability of the channel code is beyond the number of erroneous data bits induced by wireless transmissions, and the coding redundancy is wasted. In other words, the SNR gap expresses the extra level of data bit errors that the receiver can tolerate while meeting the minimum channel SNR required for the selected data rate. Therefore, with the wasted correcting capability of the existing channel code, CoS can correct a reasonable amount of data bit errors induced by inserted silent subcarriers. More importantly, such a communication mechanism does not consume extra channel resources.

Besides the existing SNR gap, the distribution of inserted silent subcarriers within data packets also affects the total number of silent subcarriers that can be inserted in CoS. To insert as many silent subcarriers as possible, we proactively reduce data bit errors induced by inserted silent subcarriers. Our observation is that inserting a silent subcarrier into a data packet may not bring in new data bit errors, which is built upon the insight that we can predict the distribution of erroneous data bits induced by wireless transmissions within a data packet. Due to frequency selective fading where the channel quality of each OFDM subcarrier varies, the distribution of erroneous data bits within a data packet is uneven and data bits on certain positions are more likely to be corrupted than others. The weak OFDM subcarriers produce most of the erroneous data bits. Therefore, if we select weak OFDM subcarriers to design CoS based on OFDM subcarriers' channel conditions, the positions of some data bits erased by inserted silent subcarriers overlap with the erroneous data bits induced by wireless transmissions. Such a design can reduce the number of new data bit errors introduced by inserted silent subcarriers. In fact, these erroneous data bits will be corrected by the existing channel code. Moreover, frequency selective fading is stable over time in indoor WiFi environments [8]. Therefore, we can predict the OFDM subcarriers' channel conditions within a future data packet in indoor WiFi networks.

The free control message transmissions provided by CoS can be used to improve the performances of applications such as medium access coordination and resource allocation. In this paper, we present one of the CoS-based applications to validate the effectiveness of CoS. EBA [9] was proposed to let nodes exchange backoff counters selected for their next packet transmissions to reduce packet collisions. We propose CoS-MAC to adopt the same MAC scheme with EBA but exploits the proposed communication scheme CoS to exchange backoff counters among nodes. Compared with EBA adopting the traditional piggybacking scheme, CoS-MAC not only is more reliable to transmit control messages but also avoids consuming extra channel resources. Our simulation results show that CoS-MAC achieves significant throughput gain over EBA in realistic network scenarios.

The rest of this paper is organized as follows. Section 2 presents an overview of CoS and our experimental observations. Section 3 describes the detailed design of CoS. Section 4 validates CoS and presents extensive evaluation results. Section 5 designs our CoS-MAC, a CoS-based application, and evaluates its performance. Section 6 reviews the related work, and we conclude this paper in Section 7.

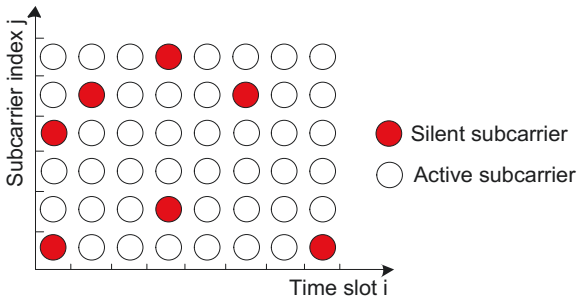


Fig. 1. The illustration of CoS where silent subcarriers are inserted into data packets.

2 Overview and Observations

This section starts with an overview of CoS that is built upon the OFDM physical layer. Then, we present our experimental studies to show the feasibility of CoS.

2.1 Overview of CoS

Modern WiFi standards (e.g., IEEE 802.11a/g/n) adopt OFDM at the physical layer. In the IEEE 802.11a, the 20 MHz wireless channel is divided into 64 orthogonal OFDM subcarriers, of which there are 4 pilot subcarriers, 12 guard subcarriers, and 48 data subcarriers. An OFDM symbol is the composite signal of 64 subcarriers. In the IEEE 802.11a, the duration of an OFDM symbol equals to 4 μs (a time slot). A data subcarrier within one OFDM symbol is denoted by $S_{i,j}$ where the location coordinate is (i, j) of which i is the time slot (or OFDM symbol) index and j is the data subcarrier index. As shown in Fig. 1, in CoS, compared with an active subcarrier, a silent (or inactive) subcarrier results in zero transmission power for an $S_{i,j}$ and erases the data bits contained in the $S_{i,j}$.

In CoS, silent subcarriers are inserted on the n selected weak data subcarriers within a data packet. For simplicity, $n = 6$ is assumed in Fig. 1. We logically number these 6 selected weak data subcarriers from 1 to 6. CoS exploits the intervals between adjacent silent subcarriers to encode information. To indicate the start of conveyed information, a silent subcarrier is inserted onto the $S_{1,1}$ (bottom left corner in Fig. 1). The length of an interval between two adjacent silent subcarriers is the number of active subcarriers. Suppose k bits ($k = 4$ in CoS) are carried by an interval, then the length of an interval ranges from 0 to 15. For example, the binary bits "0010" corresponds to 2 in decimal, so the length of the corresponding interval should be 2 to represent the sequence of bits "0010". To convey 24 bits "001001101000001110100111", we divide it into six groups where $\{$"0010", "0110", ..., "0111"$\}$. Each group includes 4 bits. The corresponding distribution of inserted silent subcarriers is shown in Fig. 1, where the number of active subcarriers between two adjacent silent subcarriers is counted from the bottom to the top of each column. For

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2019.2924000, IEEE Transactions on Mobile Computing

example, when counting the number of active subcarriers between $S_{6,5}$ and $S_{8,1}$, we observe that there are 1, 6, and 0 active subcarriers in columns 6, 7, and 8, respectively. Therefore, the length of the interval between $S_{6,5}$ and $S_{8,1}$ is 7 in decimal, and the conveyed information is "0111" in binary.

CoS aims for lightweight control messages that require broadcast nature to enable nodes in the network to exchange messages in a distributed manner. In CoS, the transmission of control messages is built upon a data packet whose transmission is unicast, but the data packet can be overheard by all nodes including the intended receiver to extract the embedded messages because of the broadcast nature of the wireless channel. In other words, CoS builds broadcast transmission of control messages on the unicast transmission of data packets. Although the data packet is transmitted at the data rate selected according to the intended receiver's channel condition, CoS extracts the embedded messages via physical layer energy detection instead of using conventional packet decoding that requires higher SNR. The reliability of transmitting control messages from one node to many nodes by CoS is slightly worse than using a dedicated control packet, but is significantly better than traditional piggybacking schemes.

Since CoS embeds (or piggybacks) control messages by inserting silent subcarriers at the physical layer, it does not change the original 802.11 data packet format. A legacy 802.11 node can correctly receive and process the data packets transmitted by a node implementing CoS even if it is not aware of the embedded control messages. In other words, the legacy 802.11 node treats the data packets transmitted by a CoS node as the original 802.11 data packets transmitted by a legacy 802.11 node.

The key idea behind CoS is that we insert a reasonable amount of silent subcarriers within a data packet while not affecting the correct decoding of the original data packet. In the subsequent development, we will show the feasibility of CoS based on experimental studies.

2.2 The SNR Gap

In this subsection, we conduct some experiments to demonstrate our fundamental idea in this paper. In our measurements, we assume that there is no strong interference. We adopt the IEEE 802.11a default values to set up the physical layer parameters such as modulation, channel code, and power allocation. The Sora platform [10] provides a software WiFi driver that implements the fully featured IEEE 802.11a standard. The IEEE 802.11a standard defines the minimum required SNR for each data rate. A data rate is selected only when the measured SNR at a receiver is higher than the minimum required SNR.

Fig. 2 plots minimum required SNRs and actual SNRs according to our experiments. The SNR gap between the actual SNR and the minimum required SNR can be observed clearly, and the minimum required SNR is always smaller than the actual SNR. For example, if the actual SNR is 16.7 dB falling between 12 dB and 17.5 dB, the data rate of 24 Mbps is selected. The minimum required SNR for this data rate is 12 dB. Thus the SNR gap is 4.7 dB. The SNR gap mainly results from the data rate adaptation scheme

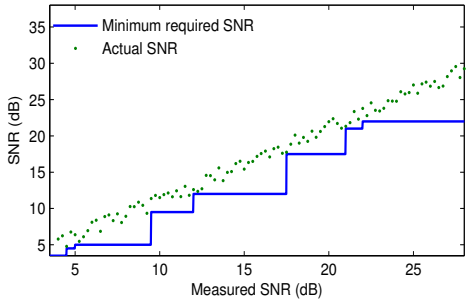


Fig. 2. The SNR gap between the actual channel SNR and the minimum required SNR.

adopted in current WiFi networks. Since channel SNRs are continuous while data rates are discrete, it is impossible to get perfect one-to-one matching from channel SNRs to data rates. Because of the stair-case adjustment for data rate in practical communication systems, when the measured SNR falls between two adjacent rates, the lower rate is selected even if the measured SNR is much higher than the minimum required SNR for that lower rate. In addition, inaccurate SNR estimation provided by the IEEE 802.11a NIC also results in the SNR gap [11]. Such an SNR gap means the number of data bit errors that can be handled by a receiver is more than the number of data bit errors induced by wireless transmissions, and so the code redundancy in channel code is not fully utilized.

The feasibility of CoS is based on the SNR gap. However, as shown in Fig. 2, when the measured SNR gets close to the minimum required SNR but not yet triggers a lower data rate, the available correcting capability of the channel code for CoS is small because the correcting capability is mainly used to correct erroneous data bits induced by wireless transmissions (fading or interference). Therefore, to further enhance the total number of silent subcarriers that can be inserted, especially in the case that the SNR gap is small, we proactively reduce data bit errors induced by inserted silent subcarriers by controlling the distribution of inserted silent subcarriers within a data packet, which is based on our observations presented in the next subsection.

2.3 The Distribution of Erroneous Data Bits

Metric for subcarrier condition: The error vector magnitude (EVM) [5] [12] can capture the deviation between the received and transmitted modulation signal positions in a constellation diagram. We use EVM to accurately characterize channel condition at subcarrier level. Notice that small EVM values represent slight deviations and good subcarrier conditions.

Frequency selective fading: Fig. 3 plots the EVM values of 48 data subcarriers measured on three positions. It can be observed that different data subcarriers exhibit very different EVM values. In a single measurement position, the difference in EVM can be up to 13%. Moreover, the frequency selective fading magnitude in each measurement position varies. In wireless transmissions, such frequency selective fading (or frequency diversity) is mainly due to multi-path propagations induced by surrounding obstacles [8].

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2019.2924000, IEEE Transactions on Mobile Computing

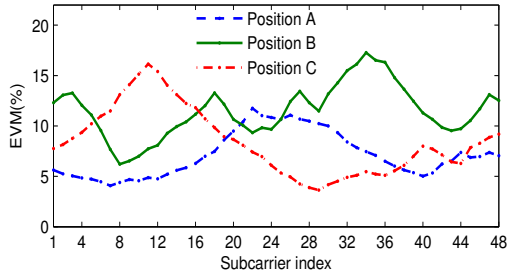


Fig. 3. Measured EVM values from frequency selective fading channels on three positions.

The pattern of data bit errors: The distribution of erroneous data bits induced by wireless transmissions is affected by frequency selective fading. Within a data packet, certain data bit positions have higher error probabilities than others. Specifically, since the IEEE 802.11 standards ignore frequency diversity and allocate the same transmission power and data rate to all data subcarriers, the data bits on the data subcarriers with deep fading experience more severe signal distortion. Thus, quite a few data subcarriers have higher data bit error rates than others and are more vulnerable to signal distortions. The error-prone data bit positions within a data packet are on the weak data subcarriers. Based on such a deterministic pattern of data bit errors, we can explicitly select weak data subcarriers to design CoS. If inserted silent subcarriers fall onto the data subcarriers that have no data bit errors in wireless transmissions, the data bits erased by inserted silent subcarriers are new data bit errors at the receiver. However, inserting silent subcarriers onto the data subcarriers that have data bit errors in wireless transmissions does not introduce new data bit errors into a data packet. In other words, CoS intentionally erases certain data bits that are more likely to be corrupted by wireless transmissions according to the prediction of the pattern of data bit errors. Therefore, we select weak data subcarriers to design CoS according to subcarrier conditions, which increases the probability that the data bits erased by inserted silent subcarriers are error-prone data bits.

Temporal stability: To predict erroneous data bit distribution within a future data packet using the current measurement feedbacks of subcarrier conditions, the frequency diversity should change slowly over time. The measurements in previous work [8] have shown that the indoor WiFi scenarios remain temporal stability over the wireless channel.

3 CoS Design

In this section, we first describe the overall system architecture for CoS. We then present the detailed design.

3.1 Overall System Architecture

Fig. 4 presents the overall system architecture of CoS built upon the IEEE 802.11a physical layer. We achieve the functionality of each newly added component by driver-level modifications without making any hardware changes. Therefore, CoS can be easily integrated into the existing WiFi systems.

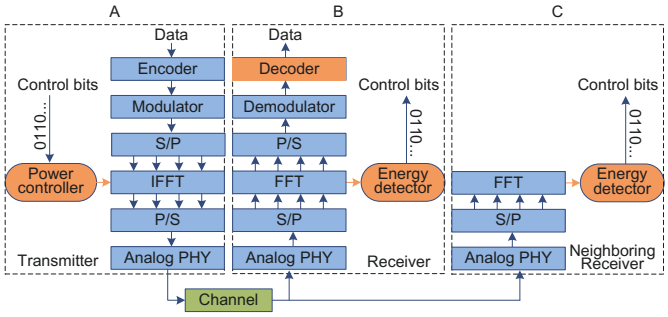


Fig. 4. System architecture of CoS. The orange blocks are CoS extensions to the OFDM-based IEEE 802.11a. A is a transmitter. B is the intend receiver of data packets while C is a neighboring receiver.

As shown in Fig. 4, transmissions and receptions of data packets follow the typical IEEE 802.11a standard except for the Viterbi decoder that is substituted with the proposed erasure Viterbi decoding. At the transmitter side (i.e., node A), control message encoding (sequence of binary bits) is done in the module of the Inverse Fast Fourier Transform (IFFT) by the power controller module. At the receiver side (i.e., both node B and node C), to interpret the transmitted control messages, subcarrier level energy detection is performed on the module of Fast Fourier Transform (FFT) by the energy detector module. Node B is the intended receiver of a data packet, and so it obtains both the data packet and the transmitted control message. Due to the broadcast nature of the wireless channel, the neighboring receiver, node C, obtains the transmitted control message without decoding the data packet. Notice that two silent subcarriers of the first OFDM symbol within a data packet indicate the start and end of the selected successive weak data subcarriers.

3.2 Encoding/Decoding of Control Messages

In OFDM, data bits are modulated into modulation signals that are carried by data subcarriers in parallel. During the encoding of control messages, inserting silent subcarriers is achieved by subcarrier level power allocation, which is performed on the IFFT. N modulation signals carried on N data subcarriers in the frequency domain are transformed into an OFDM signal in the time domain by performing N-point IFFT. Let $X[k]$ denote a modulation signal on data subcarrier k. In normal N-point IFFT, the modulation signal vector $\mathbf{X} = \{X[0], X[1], ..., X[N-1]\}$ is fed into IFFT. For example, there are two kinds of modulation signals ($1 + 0i$ and $-1+0i$) in BPSK modulation. To insert a silent subcarrier on data subcarrier k, 0 instead of modulation signal $X[k]$ is fed to data subcarrier k when performing IFFT, which results in zero transmission power on the corresponding data subcarrier. Therefore, silent subcarriers are subcarriers with zero transmission power within one OFDM symbol, which can be achieved easily.

At the receiver, N-point FFT is performed on the time domain OFDM signal to obtain N modulation signals in the frequency domain. The FFT result presents the magnitude of each OFDM subcarrier in the frequency domain [3]. If a data subcarrier is silent, its magnitude is zero. Based on the

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2019.2924000, IEEE Transactions on Mobile Computing

FFT result, subcarrier level energy detection can be achieved easily.

3.3 Threshold Selection of Energy Detection

In a practical system, the detected energy of silent subcarriers is not zero due to noise. The detection threshold of silent subcarriers is set to the noise floor. However, the noise floor varies at different environments, so dynamic estimation of the noise floor is necessary.

A pilot aided estimation scheme is proposed to estimate the noise floor. In the IEEE 802.11a, there are 4 pilot subcarriers where known modulation signal are transmitted. The 4 pilot subcarriers are distributed evenly across all data subcarriers. We exploit pilot subcarriers to extract the noise floor [13].

3.4 Subcarrier Selection Feedback

The subcarrier EVM is calculated to indicate channel condition at the subcarrier level. In practical communications, the actually transmitted modulation signals corresponding to the received modulation signals are unknown to the receiver. To address this problem, the subcarrier EVM is calculated after the cyclic redundancy check (CRC) [5]. In the practical implementation, we only use part of modulation signals on each data subcarrier to calculate subcarrier EVM because of the temporal stability of frequency diversity.

In CoS, an inserted silent subcarrier erases the data bits contained in a modulation signal within one OFDM symbol. Our observations in Section II suggest selecting weak data subcarriers to enable as many silent subcarriers as possible to fall onto the positions of erroneous modulation signals induced by wireless transmissions. However, this does not mean we select all weak data subcarriers in the practical design. Although an erroneous modulation signal results in data bit errors, but not all data bits contained in this erroneous modulation signal are errors. Fig. 5(a) presents 16QAM with Gray code constellation diagram. If the transmitted modulation signal encoded by "0111" falls around the constellation point "1111", it is demodulated to be the erroneous modulation signal "1111" that has a data bit error compared with "0111". If the channel condition is worse (i.e., higher EVM), the transmitted modulation signal falls around the constellation point "1010" and the erroneous modulation signal "1010" has three data bit errors compared with "0111". When the erroneous modulation signal "1111" is erased by a silent subcarrier, CoS introduces three new data bit errors, but a silent subcarrier falling onto the erroneous modulation signal "1010" only introduces a new data bit error. Therefore, an inserted silent subcarrier falling onto an erroneous modulation signal with more data bit errors introduces fewer new data bit errors and consumes less extra correction capability of channel code to correct the entire modulation signal. Our subcarrier selection algorithm selects part of weak data subcarriers, rather than all weak data subcarriers, to design CoS, which increases the number of silent subcarriers that can be inserted while maintaining simplicity.

After the receiver selects the data rate for the next data packet transmission, it determines the weak data subcarriers that are selected as the control subcarriers to convey control

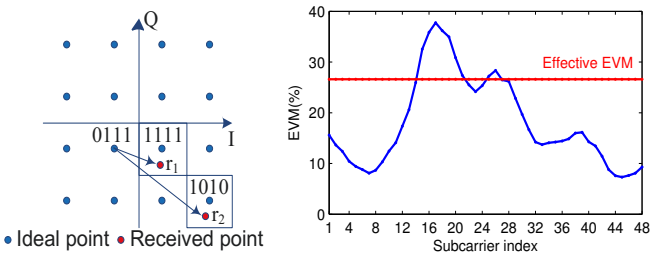


Fig. 5. (a) The 16QAM with Gray code constellation diagram. (b) EVM values for different data subcarriers, with the calculated effective EVM.

messages in the next data packet transmission. Based on the modulation type of the selected data rate, the relationship between BER and EVM can be established [12] [14]. Let BER_j and EVM_j denote the BER and EVM of data subcarrier j, respectively. The BER_j is calculated based on EVM_j [12] [14]. Then, the average data subcarrier BER is obtained by

$$BER_a = \frac{1}{48}\sum_{j=1}^{48} BER_j. \quad (1)$$

Let BER^{-1} denote the inverse mapping from BER to EVM, then we calculate the effective EVM by

$$EVM_e = BER^{-1}(BER_a). \quad (2)$$

The EVM_e is set to the selection threshold. We do not simply select all data subcarriers whose values of EVM are higher than EVM_e to design CoS. Taking into account the complexity in the practical implementation, successive weak data subcarriers with EVM higher than EVM_e are selected to design CoS, which only needs two silent subcarriers to indicate the start and the end of the selected weak data subcarriers. Fig. 5(b) presents EVM values for different data subcarriers. We can observe successive weak data subcarriers due to the frequency correlation of the wireless channel. Based on the calculated effective EVM, there are 10 data subcarriers whose values of EVM are higher than EVM_e in Fig. 5(b), but we only select 7 successive weak data subcarriers [15,16,17,18,19,20,21]. The feedback of the selected successive weak data subcarriers to the transmitter is conveyed by our CoS scheme, which is built on top of the transmission of an ACK frame.

3.5 Erasure Viterbi Decoding

In the IEEE 802.11 standards, the decoding of the convolutional code is achieved by the Viterbi algorithm, but the Viterbi algorithm is an error-only decoding scheme that simply treats data bits erased by inserted silent subcarriers as erroneous data bits induced by wireless transmissions. However, the data bit errors induced by inserted silent subcarriers can be considered as data bit erasures in the decoding process. As it is well-known, forward correction code can correct more erasures than errors. Data bit erasures affect decoding performance. Previous works [15] [16] have shown that erasures are preferable to errors.

We propose the erasure Viterbi decoding (EVD) scheme to achieve error-and-erasure decoding in CoS. The proposed

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2019.2924000, IEEE Transactions on Mobile Computing

EVD incorporates erasure decoding into the conventional Viterbi decoding. The advantage in achieving erasure decoding in CoS is that the decoder has perfect information of the distribution of erased data bits because silent subcarriers are located with subcarrier level energy detection. In CoS, an inserted silent subcarrier erases a modulation signal carried by a subcarrier within one OFDM symbol, and so data bits contained in the modulation signal are erased. EVD marks modulation signals erased by silent subcarriers as erasures and erases (or ignores) them in decoding. Let x_i denote the i-th transmitted modulation signal. A modulation signal modulated by an M-ary constellation contains $m = \log_2 M$ data bits. The j-th data bit contained in x_i is denoted by d_i^j, for $j = 1, 2, ...m$. The presence of a modulation signal erased by a silent subcarrier is indicated by the erasure indicator e_i where $e_i = 0$ for an erased modulation signal and $e_i = 1$ for a regular modulation signal. Let the pair (y_i, e_i) denote the i-th received modulation signal y_i with e_i. The receiver marks all modulation signals erased by silent subcarriers after the operation of the detection of silent subcarriers. The data bit metrics for all the m data bits $d_i^j = b(b \in \{0, 1\})$ with respect to the x_i are calculated by

$$\lambda(d_i^j = b) = \begin{cases} \log P(y_i | d_i^j = b), & \text{if } e_i = 1 \\ 0, & \text{if } e_i = 0 \end{cases} \tag{3}$$

where the data bit metrics for the data bits contained in an erased modulation signal ($e_i = 0$) are zero, i.e., $\lambda(d_i^j = b) = 0$ if $e_i = 0$, while the data bit metrics for the data bits contained in a regular modulation signal ($e_i = 1$) are calculated by a log likelihood function [15] [16], i.e.,

$$\begin{aligned} \log P(y_i | d_i^j = b) &= \log \sum_{x_i \in \chi_b^i} P(y_i | x_i) \\ &\approx \max_{x_i \in \chi_b^j} \log P(y_i | x_i), \end{aligned} \tag{4}$$

where $\chi_b^j = \{\mu(d_1, ..., d_j, ..., d_m) | d_j = b\}$ is the signal subset where the j-th data bit d_j equals to $b \in \{0, 1\}$ and μ is the mapping function that maps m-tuple data bits into an M-ary modulation signal.

Notice that the de-interleaver at the receiver de-interleaves the demodulated data bits, breaking the correlation between data bits contained in the same modulation signal [15]. Thus, the data bits with $\lambda(d_i^j = b) = 0$ in an erased modulation signal are spread across different positions in a codeword. Finally, the de-interleaved data bits are inputted into the Viterbi decoder, and the following decoding process is the same as the conventional Viterbi algorithm.

The key in EVD is that the data bit metrics for all data bits contained in modulation signals erased by silent subcarriers are taken as zero. The proposed EVD scheme only modifies the calculation of the data bit metrics without modifying the existing Viterbi decoder. Therefore, the implementation of EVD can be directly built upon the standard Viterbi decoder architecture.

4 Evaluation

4.1 CoS Implementation

The detailed implementation of CoS is based on the SoftWiFi, a software WiFi driver, which implements the fully featured IEEE 802.11a standard in the Sora platform [10]. We achieve all newly added components shown in Fig. 4 by the Sora User-mode Extension API. CoS does not require costly hardware modifications. The system parameters are set to the IEEE 802.11a default values.

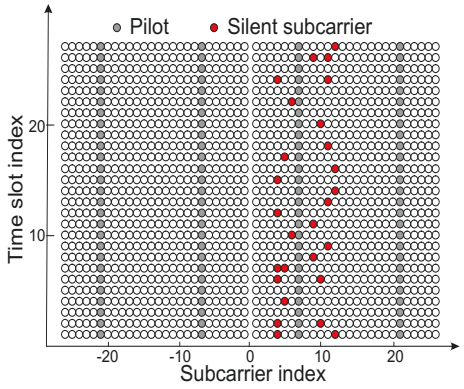


Fig. 6. The distribution of inserted silent subcarriers within a data packet.

In a practical OFDM system, the received signal is sampled with a rectangular window, so the actual spectrum on each OFDM subcarrier has sidelobes. If received OFDM signal exhibits a frequency shift, the power of an active subcarrier may leak into adjacent inactive subcarriers (i.e., silent subcarriers). Since CoS does not affect the physical preamble that is used to achieve frequency synchronization to avoid frequency shift, the OFDM subcarriers are still orthogonal and there is no power leakage in the practical implementation of CoS.

4.2 Capacity of Control Messages

This subsection studies the capacity of control messages provided by CoS under different channel conditions. We measure the number of silent subcarriers that can be inserted by CoS while ensuring the correct decoding of original data packets.

Method: The data rate adjustment in our measurements is according to the SNR-based adaptation scheme [17]. Control messages are generated randomly. Successive weak data subcarriers are selected as control subcarriers. For example, Fig. 6 plots the distribution of inserted silent subcarriers within a data packet. In this example, the selected control subcarriers are [4,5,6,8,9,10,11,12]. For clarity, Fig. 6 only shows the distribution of the first 27 OFDM symbols. Within the first OFDM symbol, there are two silent subcarriers indicating the start and the end of successive weak data subcarriers selected by the transmitter. Notice that an interval represents $k = 4$ bits in our implementation.

Under various channel conditions, we measure the maximum number of inserted silent subcarriers per second (denoted by R_m) in CoS. The measurement environment does not have strong interference. Our measurements include the data rates specified in the IEEE 802.11a standard. Notice that a data rate is a combination of modulation and code rate. For example, the combination (16QAM,3/4) produces the data rate of 36 Mbps. Each data rate corresponds to an SNR range. For example, the data rate of 36 Mbps is selected when the measured SNR is between 17.5dB and 21dB.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2019.2924000, IEEE Transactions on Mobile Computing

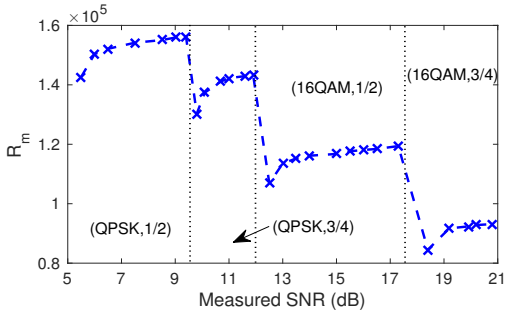


Fig. 7. The maximum number of silent subcarriers per second (R_m) under different channel conditions.

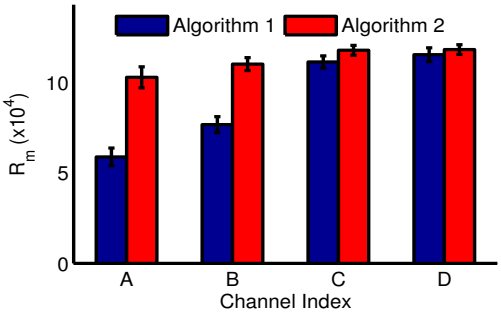


Fig. 8. R_m results for the two subcarrier selection algorithms.

Results: Fig. 7 plots R_m as a function of measured SNR. We observe two interesting results in Fig. 7. First, the maximum number of inserted silent subcarriers per second (R_m) is proportional to the available correcting capability rather than the measured SNR. Within an SNR range corresponding to a data rate, initially, R_m significantly increases with the measured SNR. The reason is that the increase of the measured SNR increases the SNR gap, so the number of erroneous data bits induced by wireless transmissions reduces. CoS can get more available correcting capability to insert more silent subcarriers. However, when the measured SNR exceeds a certain value, the increase in R_m is slight. This is because the increasing rate of the available correcting capability for CoS decreases with the increase of the measured SNR. The further increase of the measured SNR (or SNR gap) has much less impact on the increase of R_m. Second, different SNR ranges (or data rates) have different upper bounds of R_m. When SNR gap is high enough (i.e., the measured SNR is far enough from the minimum required SNR), there are no erroneous data bits induced by wireless transmissions and the channel code is totally consumed to recover data bits erased by inserted silent subcarriers. The upper bound of R_m is totally dependent on the correcting capability of the channel code. A lower code rate produces a higher upper bound of R_m when the same modulation is used. For example, (16QAM,3/4) and (16QAM,1/2) use the same modulation, but the upper bound of R_m for (16QAM,3/4) is smaller than (16QAM,1/2). This is because 1/2 code rate has higher correcting capability than 3/4 code rate. On the other hand, a higher modulation rate produces a smaller upper bound of R_m when the same code rate is used. The reason is that in a higher modulation rate, more data bits are modulated into a modulation signal. Thus, if the modulation signal is erased by an inserted silent subcarrier, more correcting capability is consumed to recover it. For example, (16QAM,3/4) and (QPSK,3/4) use the same code rate, but (16QAM,3/4) produces a smaller upper bound of R_m than (QPSK,3/4). The modulation signal modulated with 16QAM contains 4 bits while that modulated with QPSK contains 2 bits. Recovering a modulation signal modulated with 16QAM is more difficult than QPSK when the same code rate is used. In addition, as the measured SNR increases, a decreasing trend in the upper bound of R_m is shown in Fig. 7.

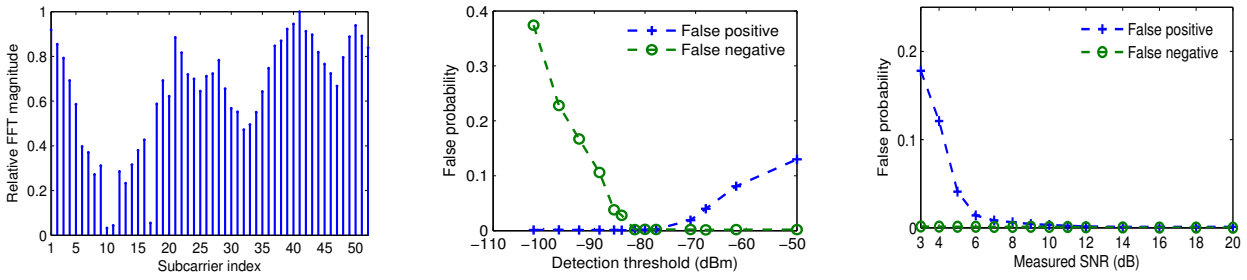
Impact of subcarrier selection: We investigate the impact of subcarrier selection on R_m and compare two subcarrier selection algorithms. In algorithm 1, all data subcarriers are used to design CoS without considering frequency selective fading. Algorithm 2 proposed in this paper selects certain weakest data subcarriers to design CoS. We consider 4 channel conditions where channels A and B have frequency diversity while channels C and D are flat fading. Fig. 8 shows R_m with respect to the 4 channel conditions for the two algorithms. As can be seen, if the frequency selective fading is significant, the R_m value of algorithm 2 is significantly higher than algorithm 1. Specifically, in channel A, the R_m gain for algorithm 2 over algorithm 1 is around 74.7%. This is because algorithm 2 can better take advantage of frequency selective fading to reduce data bit errors introduced by CoS when frequency diversity is significant. However, if the channel is flat fading, the benefit of frequency diversity cannot be utilized by algorithm 2. We observe that in channels C and D, algorithms 1 and 2 have similar performance. For example, in channel D, the R_m gain for algorithm 2 over algorithm 1 is only 2.43%. Therefore, in frequency selective fading channels, algorithm 2 obtain higher R_m compared to algorithm 1 which ignores frequency diversity.

4.3 Detection Accuracy of Silent Subcarriers

This subsection evaluates the accuracy of subcarrier level energy detection under various channel conditions. The FFT result at the receiver presents the magnitudes of all OFDM subcarriers. Fig. 9(a) plots the normalized FFT magnitudes of 52 OFDM subcarriers, of which there are 4 pilot subcarriers and 48 data subcarriers. We logically number these 52 OFDM subcarriers from 1 to 52. Based on the FFT result, we do not detect high magnitudes on the silent subcarriers. In Fig. 9(a), the 8 contiguous data subcarriers [10,11,...,17] are selected to design CoS. The magnitude difference between a silent (or inactive) subcarrier and an active subcarrier is apparent, and the silent subcarriers are data subcarriers 10, 11, and 17 in Fig. 9(a). Since the interval length between silent subcarriers 11 and 17 is 5, the conveyed information is "0101". Therefore, the silent subcarriers can be easily located based on the FFT result.

False positive and false negative are used to quantify the detection accuracy of silent subcarriers. The metric false negative represents that CoS misses a silent subcarrier that is actually present. The metric false positive represents that a silent subcarrier is detected but it is actually absent. The energy detection threshold is slightly higher than the estimated noise floor in practical systems. If the energy

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2019.2924000, IEEE Transactions on Mobile Computing



(a) (b) (c)

Fig. 9. (a) Relative FFT magnitude and subcarriers [10,11,...,17] are selected. (b) The impact of detection threshold on detection accuracy. (c) False positive and negative probabilities under different SNRs.

at a data subcarrier is below the detection threshold, a silent subcarrier is declared. Fig. 9(b) plots false negative probability and false positive probability under different detection thresholds when the measured SNR is 9.2dB. When the detection threshold is too high, the false positive probability is high because certain deep fading subcarriers are falsely detected as silent subcarriers. When the threshold is too low, the false negative probability is high because CoS misses certain silent subcarriers that are considered as active subcarriers. When the detection threshold is below -84.2dBm, the false negative probability increases significantly but the false positive probability remains nearly 0. When the detection threshold is above -77.8dBm, the false positive probability increases slightly while the false negative probability remains nearly 0. Therefore, the false negative probability is sensitive to the decrease of detection threshold while the false positive probability can tolerate a slight increase in detection threshold. The reason is that the energies at different silent subcarriers are very close while the energy difference between silent subcarriers and active subcarriers with the lowest received energy is significant.

We measure the detection accuracy under different channel conditions. As shown in Fig. 9(c), the false negative probability is close to 0 even if the channel SNR is very low. When the measured SNR is below 6.3dB, the false positive probability increases with the decrease of the measured SNR. It is slightly high within a low channel SNR range but is still at reasonably low level. For example, the false positive probability is about 0.143 when measured SNR is as low as 3.2dB. Under low channel SNRs, the energy at an active subcarrier is approaching the noise floor due to deep fading, which results in an incorrect detection. Since the typical working SNR region in WiFi networks is above 10dB [18], the false positive probability is close to zero within this SNR region.

4.4 Overall Performance of CoS

In this subsection, we evaluate the overall performance of CoS in realistic network scenarios. We conduct experiments in 5 different locations. In each location, we collect 1,000 data packets. We compare CoS with IEEE 802.11a that does not insert silent subcarriers in data packets.

Results: Fig. 10 depicts the packet reception rates (PRRs) of CoS and IEEE 802.11a in realistic network scenarios. We observe that the PRRs of CoS and IEEE 802.11a vary

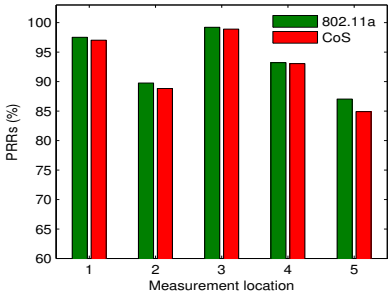


Fig. 10. PRRs of CoS and 802.11a in various measurement positions.

across different measurement locations, but the PRR difference between CoS and IEEE 802.11a is significantly small. For instance, the PRR of CoS is 98.9% at location 3 while the corresponding PRR of IEEE 802.11a is 99.2%. Even in the worst case (location 5), CoS only experiences a slight reduction in PRR of 2.45% compared to the IEEE 802.11a. We also observe that the fluctuation of PRR varies due to unexpected interference in realistic network scenarios. Fig. 10 reveals that CoS achieves the same performance in PRR as the IEEE 802.11a while conveying extra control messages.

Performance with mobility: We now investigate the performance of CoS under mobility. Our measurements are conducted in two mobility scenarios including low mobility and high mobility. Six different walking paths are used to collect PRRs in each mobility scenario and CoS is compared with the IEEE 802.11a.

TABLE 1
Packet Reception Rates for Both CoS and IEEE 802.11a Under Various Walking Paths.

Walking paths		1	2	3	4	5	6
Low mobility	802.11a	99.6	99.8	99.2	98.3	99.2	99.7
	CoS	99.4	99.3	98.8	97.8	99.2	99.5
High mobility	802.11a	97.5	97.3	96.4	97.9	99.0	99.2
	CoS	82.5	78.3	90.3	87.4	82.6	91.9

Results: Table 1 presents the PRRs for both CoS and IEEE 802.11a under various walking paths. We observe that in low mobility scenario, both CoS and IEEE 802.11a perform fairly well and they are close to each other in terms of PRR. However, at high mobility, CoS performs worse in most walking paths compared with IEEE 802.11a, as what is expected. For example, the PRR of CoS reduces to 87.4% in walking path 4 while the corresponding PRR of

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2019.2924000, IEEE Transactions on Mobile Computing

IEEE 802.11a is 97.9%, which means the reduction in PRR is about 10.5%. The reason is that the channel quality is unpredictable in high mobility scenario and the mobility of nodes may make the current channel estimation outdated. Therefore, packet transmission failures result from the inaccurate prediction of the number of silent subcarriers that can be inserted in CoS when the channel coherence time is small. We must point out that in indoor WiFi networks, the usage pattern of WiFi users is static or move with low mobility, so CoS still works well.

4.5 Discussions

This work implements CoS based on IEEE 802.11a, but CoS can be implemented in other IEEE 802.11 standards such as 802.11g and 802.11n because most IEEE 802.11 standards adopt OFDM at the physical layer. Various IEEE 802.11 standards used to implement CoS result in various capacities for control messages achieved by CoS, but do not affect the detection accuracy of silent subcarriers. Various IEEE 802.11 standards specify various modulation schemes and coding rates (i.e., various data rates), which affects the SNR gap. Therefore, the capacities of control messages in CoS in various IEEE 802.11 standards are different. In addition, when measuring the capacities of control messages in CoS, we should take into account various factors in various IEEE 802.11 standards. For example, unlike 802.11a and 802.11g where the bandwidth of a channel is fixed to 20 MHz, the bandwidth of a channel can be 20 MHz or 40 MHz in 802.11n, which results in various data rates and affects the capacities of control messages in CoS.

5 Application

CoS enables nodes to exchange lightweight control messages with other nodes in a distributed manner, which can be used to enhance the performance of various applications. The existence of the SNR gap is opportunistic, which requires a CoS-based application to opportunistically utilize CoS to improve network performance. In what follows, we propose CoS-MAC, one of the CoS-based applications, to validate the effectiveness of CoS.

5.1 CoS-MAC

Current WiFi networks adopt the distributed coordination function (DCF), a distributed contention scheme, to coordinate the channel access. In DCF, each node randomly selects a backoff counter to execute a backoff procedure in a distributed manner. Various adaptive MAC protocols were proposed to proactively reduce the collisions or minimize the idle time during channel contention [19], [20], [21]. EBA [9] was proposed to exchange backoff counters selected for nodes' next packet transmissions to reduce packet contentions, which introduces reservation into the contention-based DCF. Inspired by EBA, we propose CoS-MAC to provide information sharing among nodes in a distributed manner via the proposed communication scheme CoS. Compared with EBA adopting the traditional piggybacking scheme, CoS-MAC is more reliable to transmit control messages.

EBA adds a new control field in the MAC header of the original 802.11 data packet format, so each node can announce its backoff counter selected for its next packet transmission. Nodes in the network know when a node will start its next packet transmission and could select their backoff counters to avoid transmitting simultaneously with this node, so packet collisions can be eliminated. Each node in the network maintains a reservation table locally to record backoff counters that have been reserved by other nodes. CoS-MAC follows the basic scheme of EBA but exploits CoS to embed a node's MAC address and its reserved backoff counter into the data packet being sent. In CoS-MAC, if a CoS-MAC node cannot exploit CoS to convey reserved backoff counter due to its small SNR gap, it works as a legacy DCF node but is aware of extracting embedded messages transmitted by other CoS-MAC nodes. Notice that a legacy DCF node not only does not convey its reserved backoff counter but also is not aware of extracting backoff counter information from received data packets.

Since CoS uses 4 bits to encode an interval between two adjacent silent subcarriers, the number of bits of a control message should be a multiple of 4. We adopt the 48-bit MAC address to specify a node ID. The maximal value of a backoff counter is 1023 in the IEEE 802.11 standards, so the BC is encoded by 12 bits (a multiple of 4). In addition, 8-bit cyclic redundancy check (CRC) is used to check the correctness of the conveyed extra control information (48-bit MAC address and 12-bit backoff counter). If the control message extracted by a node fails the CRC check due to realistic factors such as inaccurate detection of silent subcarriers, the node ignores the conveyed control message. Notice that CoS-MAC exploits CoS to embed the extra information (48-bit MAC address, 12-bit backoff counter, and 8-bit CRC) into physical signals without changing the 802.11 MAC frame format. CoS-MAC only needs to insert 17 silent subcarriers to encode a control message of 68 bits, which introduces very few data bit errors into a data packet.

In CoS-MAC, if a data packet's transmission failure is due to channel errors, the reserved backoff counter embedded into the data packet may still be correctly obtained by some nodes because CoS extracts information without packet decoding. To reduce collisions, we use the reserved backoff counter for the data packet's first retransmission. If two consecutive transmission failures occur, a new backoff counter is selected randomly for the retransmission just as DCF does.

CoS-MAC in multiple collision domains: In the scenario of multiple collision domains, a node's hidden nodes are not in its collision domain and cannot hear its packet transmissions. The message exchanges among nodes and its hidden nodes are not functional, i.e., the reserved backoff counters conveyed by a node are not known by its hidden nodes. CoS-MAC cannot reduce packet collisions induced by hidden nodes.

Coexistence with legacy DCF: CoS-MAC nodes can coexist with legacy DCF nodes. CoS is transparent to the legacy DCF nodes that simply treat the data bits erased by inserted silent subcarriers as data bit errors induced by wireless transmissions. In addition, since CoS does not change the 802.11 data packet format, legacy DCF nodes process data packets transmitted by CoS-MAC nodes as

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2019.2924000, IEEE Transactions on Mobile Computing

802.11 data packets and can obtain the MAC frame content but are not aware of the embedded information conveyed by CoS-MAC nodes. In the case that the AP is a legacy DCF node, CoS-MAC clients still can exploit CoS to convey extra messages while transmitting 802.11 data packets. Although the AP is not aware of the embedded message, other clients implementing CoS-MAC in the network can still extract the embedded message and avoid packet collisions with this CoS-MAC client. CoS-MAC clients determine the existence of embedded messages by detecting silent subcarriers. Notice that in this case, EBA clients should use the original 802.11 data frame format to communicate with the AP, so backoff counter information cannot be conveyed. EBA can work only when the AP is upgraded to implement EBA because legacy DCF nodes cannot communicate with EBA nodes that change the 802.11 data packet format. Compared with EBA, CoS-MAC can more easily be incorporated into legacy WiFi systems. When legacy DCF nodes and CoS-MAC nodes coexist in the same WiFi network, the network performance will be worse than in the WiFi network that only consists of CoS-MAC nodes.

5.2 Performance Evaluation of CoS-MAC

In this subsection, we use the simulator OPNET (version 14.5) to evaluate the performance of CoS-MAC.

5.2.1 Simulation Setting

In the simulations, we consider a typical WiFi scenario where clients randomly distribute within a 30 m circle around an AP. In each generated random network topology, all clients have no mobility and always have data packets to transmit (i.e., the saturation state). The carrier-sense range is set to 65 m, so all clients in a single WiFi network can sense each other, i.e., they are in a single collision domain. The channel model incorporates path loss and multipath Rayleigh fading with a root mean square (RMS) delay spread of 50 ns [22]. The data packets transmitted by different clients encounter different channel fading. Each client selects data rate according to the SNR of its channel to the AP. For each generated random network topology, we run simulations for CoS-MAC, DCF, EBA [9], Back2F [3], and REPICK [23], respectively. Each simulation is run 5 times to collect the average simulation results. When performing simulations for EBA, Back2F, and REPICK, we adopt the default parameters presented in their papers. For example, the batch size is set to 3 in Back2F. Notice that REPICK works only when the number of clients in a single collision domain is no more than 16 [23]. Unless otherwise indicated, we configure the network parameters according to the default values specified in the IEEE 802.11a standard. For example, the initial contention window size is set to 32. RTS/CTS is disabled in our simulations. The default data packet length is 1000 Bytes.

5.2.2 Results

Overall performance: Fig. 11 plots the network throughput of CoS-MAC, DCF, EBA, Back2F, and REPICK as the number of clients increases from 5 to 50. Notice that we conduct simulations for REPICK only when the number of clients is no more than 16. In Fig. 11, we observe that in a single collision domain, CoS-MAC achieves higher network throughput than DCF and EBA but performs worse than Back2F and REPICK. Compared with CoS-MAC that is still a time domain backoff scheme, the frequency domain contention schemes in both Back2F and REPICK can reduce idle slots induced by the time domain backoff at the cost of extra hardware (an additional listening antenna). In Fig. 11, we also observe that when the number of clients increases, the throughput gain achieved by Back2F over CoS-MAC degrades. This is because Back2F cannot totally eliminate collisions in the frequency domain. Notice that the number of rounds of contention is set to 2 in Back2F. Both EBA and CoS-MAC outperform DCF due to backoff counter exchanges among clients, but CoS-MAC achieves higher throughput gain over DCF compared with EBA. The reason is that CoS-MAC is more reliable to transmit backoff counter from one client to other clients in the network.

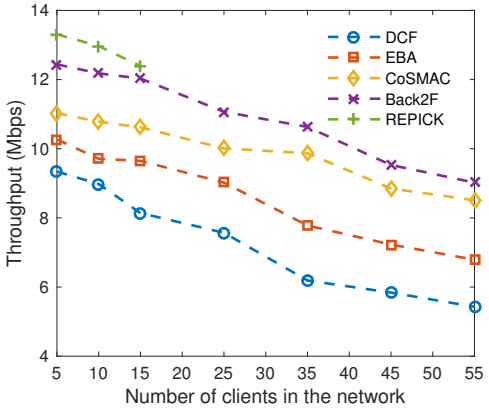


Fig. 11. Network throughput comparison in random network topologies.

Comparisons between CoS-MAC and EBA: To better understand that the throughput gain achieved by CoS-MAC over EBA is mainly due to reliable transmissions of backoff counters, we present more simulation details for the simulation results of Fig. 11. For simplicity, we consider the case of 10 clients. Table 2 presents the 10 clients' SNRs of their channels to the AP. The 10 clients' data rates are selected according to the mapping between channel SNRs and data rates defined in the 802.11a standard. In the simulations for CoS-MAC, the client 5 and 7 cannot exploit CoS to convey reserved backoff counters due to their small SNR gaps but still can extract backoff counters conveyed by other clients. Let θ denote the ratio of the number of data packets from which a client can correctly obtain the backoff counters to the number of its received data packets. Then, we have θ_{EBA} and $\theta_{CoS-MAC}$ in EBA and CoS-MAC, respectively. Notice that θ_{EBA} and $\theta_{CoS-MAC}$ do not include the failed transmissions induced by collisions. Inaccurate detection of silent subcarriers and receiving data packets from client 5 and 7 affect the value of $\theta_{CoS-MAC}$.

Table 2 presents the simulation results of clients' θ_{EBA} and $\theta_{CoS-MAC}$. We can clearly observe that at each client, $\theta_{CoS-MAC}$ is significantly larger than θ_{EBA}. For example, at client 4, θ_{EBA} is 23.5%, i.e., only 23.5% of the data packets received from other clients are decoded correctly to obtain backoff counters, while $\theta_{CoS-MAC}$ is 79.2%. In other words, in CoS-MAC, client 4 cannot correctly obtain backoff

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2019.2924000, IEEE Transactions on Mobile Computing

TABLE 2
Simulation Results for Both EBA and CoS-MAC in the Case of 10 Clients.

Client ID	SNR	Data Rate	θ_{EBA}	$\theta_{CoS-MAC}$
1	7.1 dB	12 Mbps	12.1%	57.5%
2	13.1 dB	24 Mbps	25.1%	68.8%
3	25.7 dB	54 Mbps	44.5%	80.1%
4	16.4 dB	24 Mbps	23.5%	79.2%
5	21.1 dB	48 Mbps	23.4%	90.7%
6	15.9 dB	24 Mbps	46.7%	79.9%
7	12.2 dB	24 Mbps	13.5%	89.7%
8	10.5 dB	18 Mbps	33.9%	79.9%
9	11.7 dB	18 Mbps	34.8%	68.4%
10	6.1 dB	12 Mbps	23.6%	46.9%

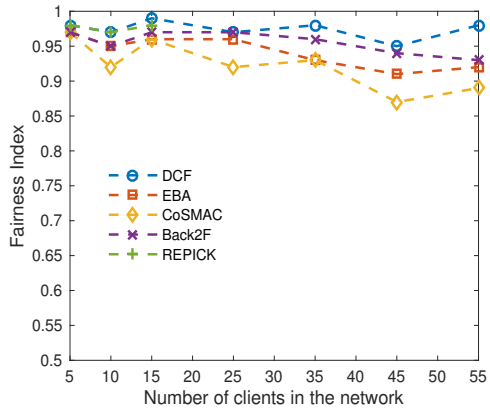


Fig. 12. Fairness comparison in random network topologies.

counters from 20.8% of its received data packets. This is mainly due to receiving data packets transmitted by clients 5 and 7. Table 2 verifies that compared with EBA adopting the traditional piggybacking scheme, CoS-MAC is more reliable to transmit backoff counters from one client to other clients in the network. We take client 4 as an example to analyze the reasons. The minimum channel SNR required to correctly decode client 4's data packets transmitted at 24 Mbps is 12 dB. Therefore, in EBA, a client can correctly obtain client 4's backoff counters by decoding the MAC header only when its SNR is higher than 12 dB. In the contrary, in CoS-MAC, the minimum channel SNR required to correctly extract client 4's backoff counters by physical layer energy detection is 4.2 dB. Therefore, some clients in CoS-MAC cannot correctly decode client 4's data packets, but they can still correctly obtain its embedded messages without packet decoding. Although Table 2 only presents the case of 10 clients, similar patterns of performance can be observed in cases of other numbers of nodes.

Fairness of CoS-MAC: In realistic network scenarios, some clients cannot exploit CoS due to their low SNR gaps, which favors the throughput of the clients who can exploit CoS to convey reserved backoff counters to reduce packet collisions. To evaluate CoS-MAC's fairness, we measure each client's throughput in the simulations. Fig. 12 plots the Jain's fairness index [9] of CoS-MAC, DCF, EBA, Back2F, and REPICK. We can observe that the fairness index of CoS-MAC is lower than DCF while other schemes sustain fairness index comparable to DCF, which implies that CoS-MAC does lose in fairness. However, CoS-MAC's fairness index still keeps above 0.87 in the worst case of 45 clients,

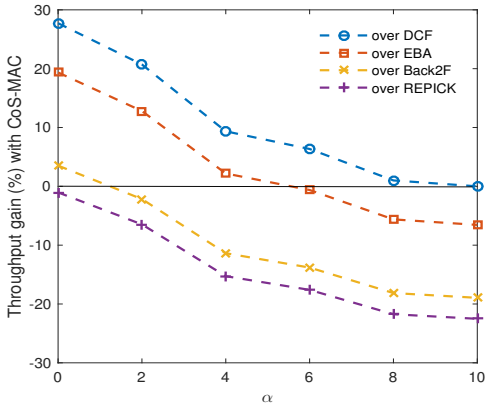


Fig. 13. Throughput gain achieved by CoS-MAC over DCF, EBA, Back2F, and REPICK for different values of α. The network consists of 10 clients.

which seems to be reasonable.

Next, we conduct simulations to evaluate the effects of realistic network factors such as SNR gap and channel fading on CoS-MAC in a single collision domain.

Impact of SNR gap: In CoS-MAC, a client's SNR gap depends on its practical channel condition. Let α denote the number of CoS-MAC clients that cannot exploit CoS due to their small SNR gaps in a random network topology. For each number of clients, we generate 30 random network topologies. Table 3 presents the maximum, minimum and average α of 30 random network topologies. The value of α varies with the practical network topology.

TABLE 3
Results of α for different numbers of clients in CoS-MAC.

Number of clients	5	10	15	25	35	45	55
Average α	1.03	1.93	3.20	4.33	6.93	8.80	10.53
Maximum α	3	5	5	8	12	17	11
Minimum α	0	0	1	1	3	3	6

In the simulations investigating the impact of SNR gap on CoS-MAC's performance, we adjust clients' positions in a generated random network topology with 10 clients so that we can vary α. Other simulation settings still adopt the descriptions presented in Section 5.2.1. Fig. 13 plots the network throughput gain achieved by CoS-MAC over DCF, EBA, Back2F, and REPICK for different values of α. CoS-MAC's throughput decreases with an increase of α. We can observe that in the ideal case of $\alpha = 0$, CoS-MAC is slightly worse than REPICK but performs better than other schemes. In the worst case of $\alpha = 10$ where all clients cannot exploit CoS, CoS-MAC is back to DCF. We also observe that CoS-MAC performs worse than EBA when α is larger than 6. The feasibility of CoS depends on the SNR gap, so it has significant effects on CoS-MAC's performance.

Impact of deep fading: In CoS-MAC, deep fading leads to inaccurate detection of silent subcarriers when channel SNR is very small. Let β denote the ratio of the number of backoff counters that a client fails to extract due to inaccurate detection of silent subcarriers to the number of its received backoff counters. Table 4 presents the maximum, minimum and average β for clients in each generated random network topology. A client's β depends on the practical network topology. We observe that in most cases, β is small.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2019.2924000, IEEE Transactions on Mobile Computing

For example, in the case of 25 clients, the average β is 6.5%. In most cases, the power of an active subcarrier with deep fading is larger than that of a silent subcarrier that only contains noise. We can accurately distinguish silent subcarriers from active subcarriers as long as the noise floor is estimated accurately. If the message extracted by a client fails the CRC check due to inaccurate detection of silent subcarriers, the client ignores the conveyed message, while other clients can still correctly obtain the message. Compared with the SNR gap, deep fading has less impact on CoS-MAC.

TABLE 4
Results of β for different numbers of clients in CoS-MAC.

Number of clients	5	10	15	25	35	45	55
Average β (%)	15.0	13.3	8.1	6.5	8.5	4.4	4.7
Maximum β (%)	25.0	22.2	14.3	16.7	26.5	18.2	16.7
Minimum β (%)	0	11.1	7.1	4.2	2.9	2.3	1.9

In the simulations investigating the impact of deep fading on CoS-MAC's performance, each client's detection accuracy of silent subcarriers is configured with β rather than according to its channel fading. Thus, we can vary each client's β. The 10 clients in a generated random network topology have the same value of β. Other simulation settings still follow the one presented in Section 5.2.1. Fig. 14 plots the network throughput gain achieved by CoS-MAC over DCF, EBA, Back2F, and REPICK for different values of β. CoS-MAC's performance degrades with an increase of β. Notice that the detection accuracy of silent subcarriers still affects Back2F and REPICK. In Fig. 14, we can observe that with the increase of β, the throughput gain achieved by CoS-MAC over DCF and EBA decreases while that over Back2F and REPICK increases.

Multiple collision domains: In the simulations for the scenario of multiple collision domains, we consider two WiFi networks, each of which is a single collision domain and adopts the previous simulation settings presented in Section 5.2.1. The distance between AP 1 and AP 2 is set to 45 m. In the overlapping area of the two WiFi networks, clients can hear packet transmissions from both WiFi networks. Some clients in WiFi network 2 but not in the overlapping area are hidden nodes to a client in WiFi network 1 because they cannot hear this client's packet transmissions but are within the AP 1's interference range. Thus, the packet transmissions of clients in WiFi network 1 may occur collisions at the AP 1 due to its hidden nodes' packet transmissions in WiFi network 2. We vary the number of clients in WiFi network 2 while the number of clients in WiFi network 1 is fixed to 10.

Fig. 15 plots the WiFi network 1's throughput under CoS-MAC, DCF, EBA, Back2F, and REPICK as the number of clients in WiFi network 2 increases from 0 to 40. We can observe that the WiFi network 1's throughput under all schemes decreases with the increase of the number of clients in WiFi network 2. The reason is that the number of hidden nodes of clients in WiFi network 1 increases. Fig. 15 also shows that the throughput under Back2F and REPICK degrades more sharply than other schemes. This is because the frequency domain contention schemes in both Back2F and REPICK totally eliminate random backoff in the time domain, which results in some clients' consecutive collisions due to hidden nodes. REPICK only solves the hidden node problem in the cases that the receiver (i.e., the AP) wins frequency domain contentions [23]. In Fig. 15, we also observe that when the number of clients in WiFi network 2 is greater than 15, CoS-MAC performs better than DCF, EBA, and Back2F.

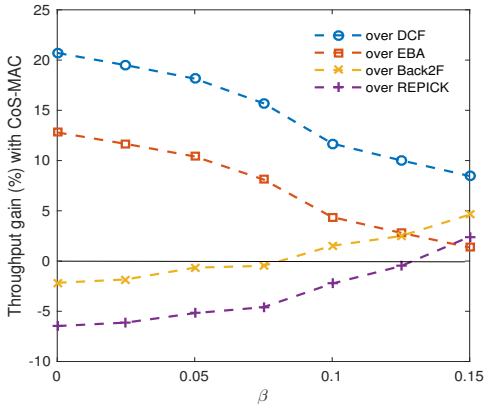


Fig. 14. Throughput gain achieved by CoS-MAC over DCF, EBA, Back2F, and REPICK for different values of β. The network consists of 10 clients.

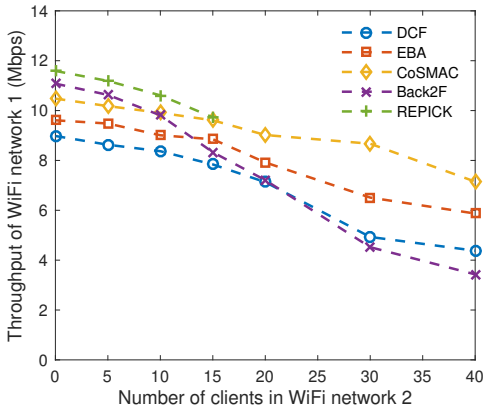


Fig. 15. Network throughput comparison in multiple collision domains. The number of clients in WiFi network 1 is fixed to 10.

5.3 Other Applications

In addition to reducing packet collisions, other applications in WiFi networks also benefit from the free message transmissions provided by CoS. We can exploit CoS to achieve contention-free scheduling or polling in a distributed manner. Specifically, the control message indicating the next scheduled node can be embedded into the transmitted packet. Moreover, if the embedded control message includes the node's queue length, we can design QoS-based scheduling. Also CoS can be used to design dynamic resource allocation. The unused channel resources of a node can be released and assigned to other nodes by embedding extra resource allocation information into the transmitted packet. We believe CoS can be used to improve the performance of various applications, which will be further investigated in our future work.

6 Related Work

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

Data rate selection: Various data rate selection schemes have been proposed. Halperin et al. [11] allocated the same data rate to all OFDM subcarriers but adopted a new metric, effective SNR taking into account frequency selective fading, to select data rate. Several papers [6] [7] investigated the gap between adjacent data rates and proposed seamless data rate adjustment schemes. A rate compatible modulation was designed in [6]. The time domain was added into conventional modulation to achieve 3-Dimensional modulation in [7]. However, both of these two schemes are complex, which limits their practical applications. Instead, we exploit, rather than fill, the existing SNR gap, to design CoS for conveying lightweight control messages for free.

Harnessing frequency diversity: Han et al. [24] conducted measurements to study bit error patterns in WiFi networks. Rahul et al. [25] proposed FARA that allocates different data rates across different OFDM subcarriers to achieve frequency-aware rate adaptation. However, allocating a different data rate per OFDM subcarrier significantly increases the system complexity. In [8] [26], frequency diversity was utilized to achieve unequal error protection where reliable OFDM subcarriers are selected to transmit important data bits. Different from the above works, CoS selects weak data subcarriers induced by frequency diversity to insert silent subcarriers.

Side channel design: There have been some works attempting to utilize physical layer techniques to design side channel. In [18] [27] [28], novel communication schemes were proposed to enable communications between heterogeneous wireless networks such as WiFi and ZigBee. CoS targets at quite a different application. To avoid overhead induced by control packets, Magistretti et al. [29] utilized a dictionary of correlatable symbol sequences to design control signals. Some papers exploited the link margin (or interference margin) to convey information. In [30] [31], the intended inference signal was used to represent information. However, their schemes have many limitations. First, the uncontrolled contention in control plane may destroy the original data packet, so coordination in the control plane still needs to be resolved. Second, it is challenging to ensure that an intended inference signal accurately fall onto a subcarrier within one OFDM symbol because data packets and intended inference signals are transmitted by different nodes. In contrast, CoS adopts quite a different communication mechanism. In CoS, both data packet and control message are transmitted by the same node, and the intervals between adjacent silent subcarriers are used to encode information. Most importantly, the frequency diversity is exploited to enhance the capacity of control messages. In [32], the idea of inserting silent subcarriers to encode information was proposed to reduce energy consumption induced by packet overhearing. Different from [30] [31], Tan et al. [33] exploited the link margin to convey a cryptographic signature by adding authentication tags to modulation schemes at the physical layer. The idea of interference margin also has been used for power control in wireless ad hoc networks [34] [35]. Muqattash et al. [36] enhanced spatial reuse in ad hoc networks by utilizing interference margin. Chen et al. [37] leveraged it to obtain spectrum access in cognitive radio networks.

7 Conclusion

In this paper, we exploit the wasted SNR gap to design CoS, a novel communication scheme, to convey lightweight control messages for free in indoor WiFi networks. The key intuition behind CoS is that we can erase a reasonable number of data bits by inserting silent subcarriers while not impacting the original data packet. Some practical issues are resolved in designing CoS. Compared with traditional piggybacking schemes, CoS is more reliable to transmit control messages among nodes. Moreover, we design CoS-MAC, one of the CoS-based applications, to validate the effectiveness of CoS.

In practical network scenarios, a node may not be able to exploit CoS to transmit extra messages because its SNR gap cannot ensure that the number of inserted silent subcarriers does not corrupt the transmitted data packet. Therefore, CoS is an opportunistic communication scheme. In other words, CoS-based applications opportunistically exploit CoS to improve their performance.

Acknowledgments

This work was partially supported 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 Grant WK2101020006. The work of J. Liu and Y. Fang was partially supported by the US National Science Foundation under Grants CNS-1409797 and CNS-1343356.

References

[1] B. Feng, J. Liu, C. Zhang, and Y. Fang, "Communication through symbol silence: Towards free control messages in indoor wlans," in *Proc. IEEE ICDCS*, 2017, pp. 880–888.

[2] *Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications*, IEEE 802.11 Std., 2007.

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

[5] 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.

[6] H. Cui, C. Luo, J. Wu, C. W. Chen, and F. Wu, "Compressive coded modulation for seamless rate adaptation," *IEEE Trans. Wireless Commun.*, vol. 12, no. 10, pp. 4892–4904, 2013.

[7] 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.

[8] 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.

[9] J. Choi, J. Yoo, S. Choi, and C. Kim, "Eba: An enhancement of the ieee 802.11 dcf via distributed reservation," *IEEE Trans. Mobile Comput.*, vol. 4, no. 4, pp. 378–390, 2005.

[10] K. Tan, J. Zhang, J. Fang, H. Liu, Y. Ye, S. Wang, Y. Zhang, H. Wu, W. Wang, and G. M. Voelker, "Sora: high performance software radio using general purpose multi-core processors," in *Proc. USENIX NSDI*, 2009, pp. 75–90.
[11] D. Halperin, W. Hu, A. Sheth, and D. Wetherall, "Predictable 802.11 packet delivery from wireless channel measurements," in *Proc. ACM SIGCOMM*, 2011, pp. 159–170.
[12] 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.
[13] M. Vutukuru, H. Balakrishnan, and K. Jamieson, "Cross-layer wireless bit rate adaptation," in *Proc. ACM SIGCOMM*, 2009, pp. 3–14.
[14] H. A. Mahmoud and H. Arslan, "Error vector magnitude to snr conversion for nondata-aided receivers," *IEEE Trans. Mobile Comput.*, vol. 8, no. 5, 2009.
[15] 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.
[16] 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.
[17] 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.
[18] X. Zhang and K. G. Shin, "Gap sense: Lightweight coordination of heterogeneous wireless devices," in *Proc. IEEE INFOCOM*, 2013, pp. 3094–3101.
[19] Y. Kwon, Y. Fang, and H. Latchman, "Design of mac protocols with fast collision resolution for wireless local area networks," *IEEE Trans. Wireless Commun.*, vol. 3, no. 3, pp. 793–807, 2004.
[20] ——, "A novel mac protocol with fast collision resolution for wireless lans," in *Proc. IEEE INFOCOM*, vol. 2, 2003, pp. 853–862.
[21] ——, "Fast collision resolution (fcr) mac algorithm for wireless local area networks," in *Proc. IEEE GLOBECOM*, vol. 3, 2002, pp. 2250–2254.
[22] A. Doufexi, S. Armour, M. Butler, A. Nix, D. Bull, J. McGeehan, and P. Karlsson, "A comparison of the hiperlan/2 and ieee 802.11 a wireless lan standards," *IEEE Communications magazine*, vol. 40, no. 5, pp. 172–180, 2002.
[23] X. Feng, J. Zhang, Q. Zhang, and B. Li, "Use your frequency wisely: Explore frequency domain for channel contention and ack," in *Proc. IEEE INFOCOM*, 2012, pp. 549–557.
[24] 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.
[25] 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.
[26] 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.
[27] S. M. Kim and T. He, "Freebee: Cross-technology communication via free side-channel," in *Proc. ACM MobiCom*, 2015, pp. 317–330.
[28] K. Chebrolu and A. Dhekne, "Esense: communication through energy sensing," in *Proc. ACM MobiCom*, 2009, pp. 85–96.
[29] E. Magistretti, O. Gurewitz, and E. W. Knightly, "802.11 ec: collision avoidance without control messages," in *Proc. ACM MobiCom*, 2012, pp. 65–76.
[30] 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.
[31] A. Cidon, K. Nagaraj, S. Katti, and P. Viswanath, "Flashback: Decoupled lightweight wireless control," in *Proc. ACM SIGCOMM*, 2012, pp. 223–234.
[32] B. Feng, C. Zhang, H. Ding, and Y. Fang, "Exploiting wireless broadcast advantage for energy efficient packet overhearing in wifi," *IEEE Trans. Veh. Technol.*, vol. 68, no. 4, pp. 3586–3599, April 2019.
[33] X. Tan, K. Borle, W. Du, and B. Chen, "Cryptographic link signatures for spectrum usage authentication in cognitive radio," in *Proceedings of the fourth ACM conference on Wireless network security*, 2011, pp. 79–90.
[34] P. Li, X. Geng, and Y. Fang, "An adaptive power controlled mac protocol for wireless ad hoc networks," *IEEE Trans. Wireless Commun.*, vol. 8, no. 1, pp. 226–233, 2009.
[35] P. Li, Q. Shen, Y. Fang, and H. Zhang, "Power controlled network protocols for multi-rate ad hoc networks," *IEEE Trans. Wireless Commun.*, vol. 8, no. 4, 2009.
[36] 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.
[37] 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.

Bing Feng is currently a Ph.D. student at the University of Science and Technology of China. He received the B.E. degrees from the Anhui University, Hefei, China, in 2013. His research interests include wireless communication and wireless local area networks.

Chi Zhang received the B.E. and M.E. degrees in electrical and information engineering from the Huazhong University of Science and Technology, China, in 1999 and 2002, respectively, and the Ph.D. degree in electrical and computer engineering from the University of Florida in 2011. He joined the School of Information Science and Technology, University of Science and Technology of China, as an Associate Professor in 2011. His research interests include the areas of network protocol design and performance analysis and network security particularly for wireless networks and social networks.

Jianqing Liu received the Ph.D. degree from University of Florida in 2018 and the B.Eng. degree from University of Electronic Science and Technology of China in 2013. He is currently a tenure-track assistant professor in the Department of Electrical and Computer Engineering at University of Alabama in Huntsville. His research interest is to apply cryptography, differential privacy and convex optimization to design secure and efficient protocols for various IoT systems. He is the recipient of the 2018 Best Journal Paper Award from IEEE Technical Committee on Green Communications & Computing (TCGCC) and the Best Paper Award from 2012 IEEE Workshop on Microwave and Millimeter-Wave Circuits and Systems (MMWCST).

Yuguang "Michael" Fang (F'08) received an MS degree from Qufu Normal University, Shandong, China in 1987, a PhD degree from Case Western Reserve University in 1994 and a PhD degree from Boston University in 1997. He joined Department of Electrical and Computer Engineering at University of Florida in 2000 and has been a full professor since 2005. He held a University of Florida Research Foundation (UFRF) Professorship (2006-2009), a Changjiang Scholar Chair Professorship (Xidian University, Xi'an, China, 2008-2011; Dalian Maritime University, Dalian, China, 2015-present), and a Guest Chair Professorship with Tsinghua University, China (2009-2012). Dr. Fang received the US National Science Foundation Career Award in 2001, the Office of Naval Research Young Investigator Award in 2002, the 2015 IEEE Communications Society CISTC Technical Recognition Award, the 2014 IEEE Communications Society WTC Recognition Award, the Best Paper Award from IEEE ICNP (2006), and the 2010-2011 UF Doctoral Dissertation Advisor/Mentoring Award. He is the Editor-in-Chief of IEEE Transactions on Vehicular Technology, was the Editor-in-Chief of IEEE Wireless Communications (2009-2012), serves/served on several editorial boards of technical journals. He is a fellow of the IEEE and the AAAS.