Cross-Technology Communication through Symbol-Level Energy Modulation for Commercial Wireless Networks

Junmei Yao[1], Xiaolong Zheng[2], Jun Xu[1] and Kaishun Wu[1]
[1]College of Computer Science and Software Engineering, Shenzhen University, China
[2]School of Computer Science, Beijing University of Posts and Telecommunications, China
Email: [1]{yaojunmei, xujun, wu}@szu.edu.cn, [2]zhengxiaolong@bupt.edu.cn

***Abstract*—The coexistence of heterogeneous devices in wireless networks brings a new topic on cross-technology communication (CTC) to improve the coexistence efficiency and boost collaboration among these devices. Current advances on CTC mainly fall into two categories, *physical-layer CTC* and *packet-level energy modulation* (PLEM). The *physical-layer CTC* achieves a high CTC data rate, but with channel incompatible to commercial devices, making it hard to be deployed in current wireless networks. PLEM is channel and physical layer compatible, but with two main drawbacks of the low CTC data rate and MAC incompatibility, which will induce severe interference to the other devices' normal data transmissions. In this paper, we propose symbol-level energy modulation (SLEM), the first CTC method that is fully compatible with current devices in both channel and the physical/MAC layer processes, having the ability to be deployed in commercial wireless networks smoothly. SLEM attaches the CTC bits to one WiFi data packet through adjusting the energy levels of WiFi symbols, achieving concurrent CTC and WiFi transmissions. We make theoretical analysis to figure out the performance tradeoff between CTC and WiFi, and also conduct experiments to demonstrate the feasibility of SLEM and its performance under different network situations.**

I. Introduction

With the widespread proliferation of the Internet of Things (IoT), it is becoming a common phenomenon that numerous devices with different wireless technologies (e.g., WiFi, ZigBee and Bluetooth) share the unlicensed ISM spectrum. The coexistence of these devices brings a new topic on cross-technology communication (CTC), which establishes direct communication among heterogenous devices [1]–[3]. CTC has the potential to bring about quite a few benefits and applications [2], [4], [5], such as combating the cross-technology interference through exchanging coordination information among the devices [4], enabling the WiFi AP to directly control the Zigbee devices deployed for smart home [2], and etc.

Current works on WiFi to ZigBee CTC design are generally achieved through two methods: *physical-layer CTC* and *packet-level energy modulation* (PLEM). The *physical-layer CTC* makes a commercial WiFi device transmit ZigBee signals directly through signal emulation, such that this signal can be detected through ZigBee normal demodulation process [1]. It achieves the high CTC data rate comparable to a ZigBee radio. However, the main problem is that it is is hard to be deployed in commercial wireless networks due to the channel incompatible. According to WEBee [1] design, the pilot/null OFDM (orthogonal frequency division modulation) subcarriers should be avoided in the CTC transmission [1], but our investigation on the standard WiFi and ZigBee channels finds that no combination satisfies this requirement; CTC can only be achieved when the WiFi central frequency is adjusted to a non-standard one. Although some commercial chips surely have this ability, it is hardly permitted in commercial networks since all devices should comply with the standards.

The PLEM methods convey cross-technology information through employing the packet-level features, like packet transmission duration [6], [7], duration pattern [8], [9], and interval [2], [10], so that receivers can detect the information through energy sensing. This kind of methods are compatible with commercial devices in channel and the physical layer process. However, they have two main drawbacks. Besides with the low CTC data rate that can only be up to about $1Kbps$, they are incompatible with the commercial devices in the MAC (Medium Access Control) layer process. The commercial WiFi devices generally adopt CSMA/CA (carrier sense multiple access/collision avoidance) to access the channel and avoid interference through random backoff [11], while PLEM requires the devices to access the channel in encoded time patterns, which are usually in contradiction with random backoff. Thus, the CTC transmission will easily induce severe interference to the other devices' normal transmissions.

In this paper, we propose symbol-level energy modulation (SLEM), the first CTC method that is fully compatible with commercial devices in both channel and the physical/MAC layer processes, having the ability to be deployed in current wireless networks smoothly. SLEM attaches CTC bits to WiFi symbols through exploiting known features of the WiFi signal. Since QAM (quadrature amplitude modulation) adopted in WiFi devices naturally has the feature of energy modulation, CTC can be achieved through redesigning the QAM points of the transmitting signal to make each symbol have distinguishable low or high power

978-1-7281-4657-7/20/$31.00 ©2020 IEEE

levels. Specifically, at the transmitter side, SLEM designs the transmitting bits according to the WiFi data bits and CTC data bits. When these bits are passed through the standard WiFi transmission process, the transmitting signal exhibits the characteristic of energy modulation for CTC and can deliver both kinds of information concurrently. After receiving this signal, the ZigBee receiver decodes its data bits through energy sensing, while the WiFi receiver first decodes the transmitted bits and then recovers the original WiFi data bits.

Compared to PLEM, SLEM coincides with commercial devices in the MAC process, thus avoids unnecessary interference to current wireless networks. SLEM is more flexible than PLEM as the CTC bits can be delivered at any time when a WiFi packet is transmitting. This design also benefits SLEM with much higher CTC date rate than PLEM. In addition, it is worthy to note that SLEM has no channel incompatibility problem as *physical-layer CTC*, since a single pilot subcarrier has little effect on the overall energy of multiple subcarriers.

The key contributions are summarized as follows:

- We design SLEM, the first CTC method that is fully compatible with commercial devices in both the channel usage and the physical/MAC layer processes. SLEM attaches CTC bits to WiFi symbols to deliver both kinds of information concurrently.
- We give theoretical analysis for the SLEM performance in delivering both the CTC and WiFi data bits, compared to a typical PLEM method. The results show that there is a tradeoff between the CTC and WiFi performance, since the higher-order QAM results in higher CTC performance, but at the cost of sacrificing more WiFi performance.
- We implement and evaluate SLEM on hardware testbed based on the USRP N210 and TelosB platforms. The experimental results reveal that SLEM can achieve a robust and fast concurrent transmissions of CTC and WiFi. Especially, with one CTC transmission, SLEM has about $6 \sim 10Kbps$ CTC data rate, and the WiFi performance is cut by about 7.3% when QAM-16 is adopted.

The rest of this paper is organized as follows. Section II gives the motivation of SLEM. Section III gives the overview of SLEM. Section IV describes the detailed SLEM design. Section V provides theoretical performance analysis of SLEM. Section VI demonstrates the SLEM performance by hardware experiments. Section VII introduces the related works. Section VIII concludes this paper.

II. Motivation

This section illustrates the motivation of SLEM through observing on both WiFi and ZigBee transmission processes.

A. Opportunity for CTC within One WiFi Packet

Some current packet-level energy modulation (PLEM) mechanisms have an assumption that the WiFi transmission duration τ_w is very small, Actually, from the point of view of WiFi protocol design, it is more efficient to have the data packet transmitted with larger τ_w, as this would induce smaller transmission overhead to the WiFi network, such as backoffs, control frame transmissions, etc.

Retrospecting the history of WiFi standards – the IEEE 802.11 family, we could see that they have made great efforts on avoiding extremely small value of transmission duration τ_w. As demonstrated in Table. I, with the increase of the physical layer data rate R from $11Mbps$ in 802.11b and $54Mbps$ in 802.11a/g, to $600Mbps$ in 802.11n [11] and $>6Gbps$ in 802.11ac [12], the MAC layer is also revised to enlarge the maximum packet length L_w [1] to achieve comparable τ_w values among the standards, since τ_w is inversely proportional to the data rate R_w ($\tau_w = L_w/R_w$), as listed in Table I. Especially, 802.11n and 802.11ac introduce A-MPDU (Aggregated - MAC Protocol Data Unit) to accomplish the super-length packet.

TABLE I
Attribute comparisons of different 802.11.

Attribute	**802.11a/g**	**802.11n**	**802.11ac**
Maximum R_w	$54Mbps$	$600Mbps$	$6.9Gbps$
Maximum L_w	4095bytes	65535bytes	4,692,480bytes
Maximum τ_w	$5.46ms$	$5.484ms$	$5.484ms$

Compared to the WiFi packet transmission duration that is up to $5.48ms$, the RSSI (Received Signal Strength Indicator) sampling interval of ZigBee devices is extremely small, e.g., $32\mu s$ for TelosB [3]. Accordingly, we have the opportunity to accomplish a CTC transmission within one WiFi packet through energy modulation.

B. Opportunity for Symbol-Level Energy Modulation

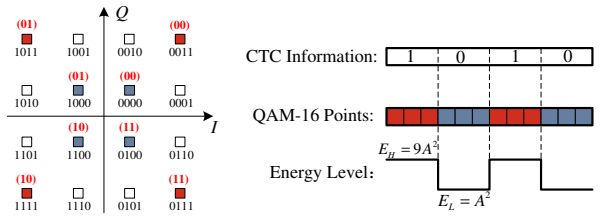
We then investigate the WiFi transmission process to answer the question about how to achieve energy modulation within one WiFi packet.

At the WiFi transmission side, the data bits will be mapped to constellation points after passing through the QAM (Quadrature Amplitude Modulation) module. QAM modulation can be regarded as a combination of both phase and amplitude modulations. Fig. 1(a) depicts the QAM-16 constellation points, each of which represents $M = log_2(16) = 4$ data bits. Among these 16 points, the four red points have 3× amplitude over the four blue points, corresponding to 9× energy difference. This characteristic provides us with an opportunity for symbol-level energy modulation within a single WiFi packet. For instance, if we let the blue points carry the CTC information '0' and let the red points carry '1', the two kinds of information will possess distinguishable energy levels and then have the possibility to be discerned at ZigBee, as shown in Fig. 1(b).

C. Opportunity for Concurrent Data Transmission

The aforementioned analysis demonstrates the possibility of CTC through symbol-level energy modulation in a WiFi

[1]Here the packet length indicates the PLCP (Physical Layer Convergence Procedure) payload size.



(a) QAM-16 constellation points (b) Energy modulation for CTC

Fig. 1. An example of symbol-level energy modulation.

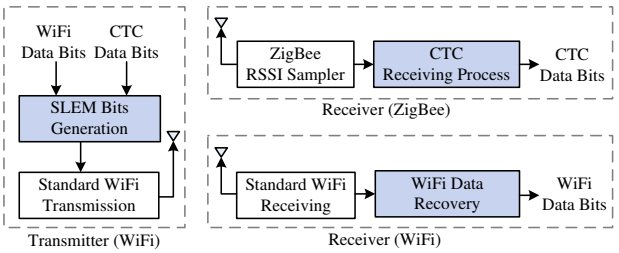


Fig. 2. Overview of SLEM.

data packet. The remaining question is whether the WiFi data can still be delivered successfully along with the CTC transmissions. The answer is yes. Actually, SLEM can utilize the amplitude characteristic of the QAM constellation points for CTC transmission, and utilize the phase characteristic for WiFi data transmission. As shown in Fig. 1(a), QAM-16 contains two sets of QPSK (Quadrature Phase Shift Keying) points (the four red points and the for blue points). We can make two points with the same phase represent the same WiFi data bits, for example, both the red and blue points in the first quadrant represent '00'. This method, however, will definitely decrease the WiFi data transmission rate, and this part of performance is sacrificed for obtaining the high-rate CTC transmissions.

III. SLEM Overview

Fig. 2 depicts the overview of SLEM's communications from a WiFi transmitter to both the ZigBee receiver and the WiFi receiver. The white block represents that this process already exists in commercial devices based on standards, while the grey block represents new component of SLEM. The following figures are described in the same way.

The WiFi transmitter first generates the transmitting bits, which is called SLEM bits in this paper, according to both the WiFi data bits and CTC data bits. The SLEM bits are the payload of the WiFi packet, they will be passed through the standard WiFi transmission process and finally be transmitted after Radio Frequency (RF) front end. When receiving this signal, the ZigBee receiver first obtains the RSSI samples through a standard component, then conducts the CTC receiving process to get the CTC data bits. Meanwhile, the WiFi receiver conducts the standard WiFi receiving process to obtain the SLEM bits, then conducts a recovery process to get the original WiFi data bits.

For the ease of description, in the following parts, we let the term 'WiFi signal' represent the signal of a normal WiFi data packet, and let the term 'SLEM signal' represent the signal of a WiFi data packet attached with CTC bits.

IV. SLEM design

This section gives the detailed design of SLEM at the transmitter side, the ZigBee receiver side and the WiFi receiver side, respectively.

A. SLEM Design at the Transmitter Side

The main objective of SLEM at the transmitter side is to design the SLEM bits according to the WiFi and CTC data bits. When the SLEM bits are passed through the standard WiFi transmission process, the transmitted SLEM signal contains both the desired energy modulated CTC signal and the WiFi signal, thus can deliver both kinds of data bits concurrently. Here we first introduce the standard WiFi transmission process, then give the detailed design of SLEM bits generation. After that, we show how to determine a key parameter in SLEM, and discuss how to extend the design to higher-order QAM modulation types.

1) Standard WiFi Transmission Process: The process is illustrated in Fig 3(b). The data bits are first transformed to complex symbols after QAM modulation, and mapped into OFDM subcarriers after passing through the S/P (serial-to-parallel) module, then output as the time-domain OFDM symbols after IFFT (inverse fast fourier transform) and P/S (parallel-to-serial) processes; afterwards, each OFDM symbol is inserted with CP (cyclic prefix) to eliminate the inter-symbol interference; the signal will finally be transmitted after the RF front end.

2) SLEM bits Generation Process: The process of generating the SLEM bits according to the WiFi and CTC data bits is shown in Fig. 3(a). The transmitter first modulates the WiFi data bits and transforms them to parallel constellation points, while the modulation type is related to the subcarrier index: if the subcarrier is for CTC transmission, QPSK is adopted, otherwise QAM is adopted. Then, for the QPSK modulated points, the transmitter further remaps them to the QAM points according to the CTC data bits. All the parallel QAM points will be passed through the P/S and QAM demodulation to generate the SLEM bits. Please note that in case only CTC transmission is required but no WiFi transmission, the WiFi data bits in Fig. 3(a) will be dummy data and generated randomly.

To remap the QPSK constellation points to another set of QAM points which carry the CTC data bits, a simple mapping table should be established at first. For the example in Fig. 1, the QPSK point '00' will be remapped to the QAM-16 point '0000' when the energy of this OFDM symbol should be low, otherwise it will be remapped to '0011'. From Fig. 3(c) we see that, the energy levels of the OFDM symbols are determined by both the the CTC data bits and the CTC symbol duration τ_{CTC}, which finally determine the number of OFDM symbols required for one CTC bit transmission, denoted by N_s. Since the OFDM symbol duration is fixed as $\tau_{OFDM} = 4\mu s$, we get $N_s = \frac{\tau_{CTC}}{\tau_{OFDM}}$.

Through this process, the remapped symbols carry both the WiFi and CTC data bits and will be delivered to the

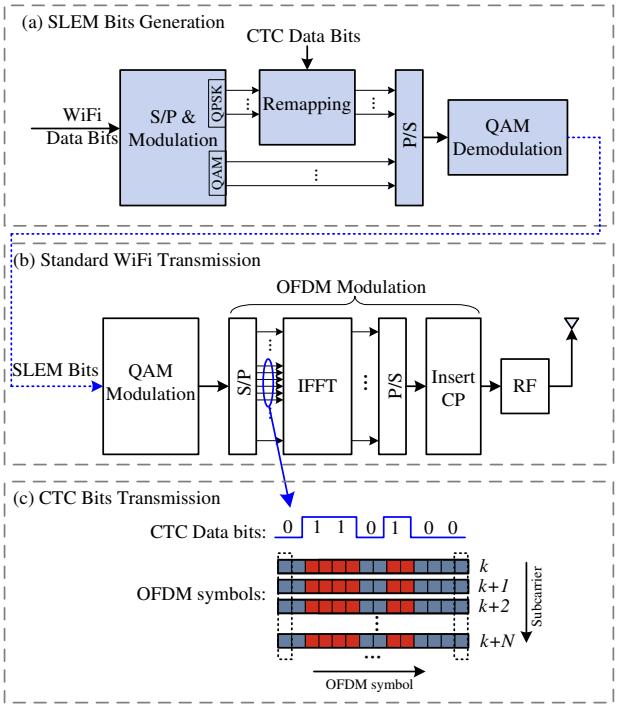


Fig. 3. Architecture of SLEM at the transmitter side. SLEM bits are first generated according to the WiFi and CTC data bits (a), then passed through the standard WiFi transmission process for signal transmission (b), the transmitted signal can deliver the CTC bits concurrently (c). This architecture is fully compatible with commercial devices.

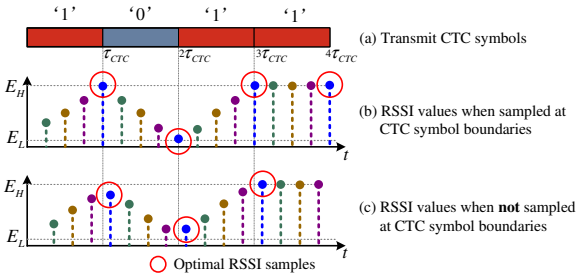
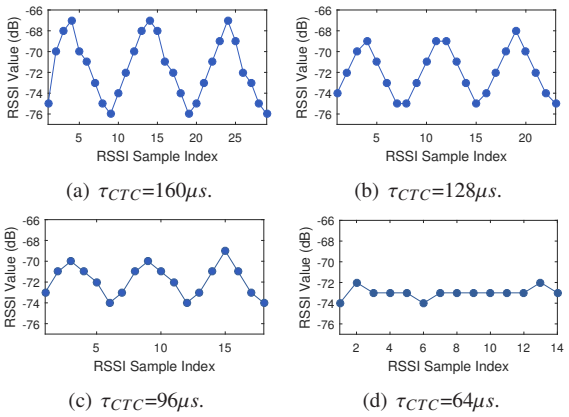


Fig. 4. An example of RSSI sampling at the receiver side.



(a) τ_{CTC}=160μs. (b) τ_{CTC}=128μs. (c) τ_{CTC}=96μs. (d) τ_{CTC}=64μs.

Fig. 5. The RSSI samples under different CTC symbol durations through experiments.

corresponding receivers concurrently.

3) CTC Symbol Duration Determination: The CTC symbol duration τ_{CTC} is decided by the characteristic of the ZigBee receiver, and in turn determines the parameter N_s at the transmitter side.

For the TelosB platform we use as ZigBee in this paper, the RSSI samples are generated every 32μs, although the values are averaged over 128μs. Under this circumstance, the CTC symbol duration τ_{CTC} and even the RSSI sample positions would affect the RSSI values at TelosB. Fig. 4 shows an example of the CTC bits $\{1, 0, 1, 1\}$ transmitted through a series of symbols with energy $\{E_H, E_L, E_H, E_H\}$, where E_H and E_L indicate the high and low energy levels, and $E_H = 9 \times E_L$ under QAM-16; the symbol duration is 128μs. We see that the RSSI sample values are very different within one CTC symbol duration. When the RSSI values are not sampled at the CTC symbol boundaries, as shown in Fig. 4(c), the RSSI distance d_{RSSI}, which is the distance between the maximum and minimum RSSI values, will be much smaller than that in Fig. 4(b) when RSSI values are sampled at the CTC symbol boundaries, and the shorter distance will result in lower performance.

To demonstrate the effect of τ_{CTC}, we let USRP N210 transmit a set of CTC bits $\{1, 0, 1, 0, 1, 0\}$, and let τ_{CTC} equal to 160μs, 128μs, 96μs and 64μs, respectively. The RSSI samples collected at TelosB under each situation are shown in Fig. 5. We see that the RSSI values demonstrate regular peaks and dips when $\tau_{CTC} \geq 96\mu s$. Specifically, the maximum d_{RSSI} is about 9dB when $\tau_{CTC} = 160\mu s$ (Fig. 5(a)), it has about 2dB and 5dB loss when τ_{CTC} is 128μs and 96μs, respectively. As to $\tau_{CTC} = 64\mu s$ in Fig. 5(d), the peaks and dips disappear and the CTC bits can not be detected at all.

4) Higher-Order QAM Adoption: The aforementioned discussion utilizes QAM-16 as an example. However, the SLEM design can be smoothly extended to the higher-order QAM modulation types, such as QAM-64 and QAM-256 which are also recommended by the 802.11 standard. Although with more constellation points, we only select eight points, four with the lowest energy and four with the highest energy, for CTC transmission, just like that of QAM-16 in Fig. 1. This kind of design will inevitably degrade the WiFi performance. As the design does not affect the subcarriers unrelated to CTC, we will show in Section V-C that the performance degradation is not critical.

B. SLEM Design at ZigBee Receiver Side

The SLEM design at the ZigBee receiver side is to make a ZigBee node decode the CTC bits through energy sensing. The receiving process is depicted in Fig. 6: the receiver first determines the optimal RSSI sample set from the received RSSI samples, then conducts energy demodulation to obtain the original ZigBee data bits. We note that the data bits of one ZigBee packet can be transmitted by CTC through multiple WiFi packets since the WiFi packet duration always varies, the receiver needs to collect the CTC information continuously until the complete ZigBee packet is received.

1) Optimal RSSI Sample Set Determination: As shown in Fig. 4, the RSSI samples with red circles can repre-

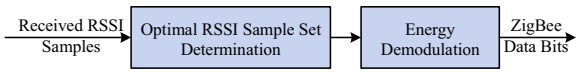


Fig. 6. The CTC receiving process.

sent the energy of the transmitted symbols best, they are regarded as the optimal RSSI sample set. The determination of this sample set contains two steps: (i) obtain the sample set candidates from the RSSI samples $\{r_i\}$, and (ii) determine the optimal one from the candidates.

The sample set candidates, denoted by $\{\hat{r}_i^k\}$ where k is the candidate index, can be easily obtained from the RSSI samples, simply through taking the samples from $\{r_i\}$ with the fixed interval $N_{intv} = \frac{\tau_{CTC}}{32\mu s}$ and different beginning positions, the number of candidates is N_{intv}. For example, in Fig. 4, the samples with the same color belongs to a candidate; there are $N_{intv} = \frac{128\mu s}{32\mu s} = 4$ candidates, corresponding to four colors.

The optimal RSSI sample set is then determined from the sample set candidates. Our observation is that the optimal RSSI sample set has the largest RSSI distance d_{RSSI} compared to the other candidates. As shown in Fig. 4 and Fig. 5, the sample set candidates exhibit different characteristic of RSSI distance, and the one with the largest RSSI distance is obviously optimal. We present a simple method to obtain this optimal RSSI sample set. At first, the mean value of the received RSSI samples $\{r_i\}$ is calculated as $m_r = MEAN(\{r_i\})$. Please note that this calculation should be performed numerically while the RSSI samples obtained from TelosB are expressed in decibels. Then, for each candidate $\{\hat{r}_i^k\}$ ($k \in [1, N_{intv}]$, $i \in [i, N]$), the accumulated RSSI distance from m_r is calculated as $d_{RSSI}^k = \sum_{i=1}^{N} \mid \hat{r}_i^k - m_r \mid$. The kth candidate with the largest d_{RSSI}^k is discerned as the optimal sample set, which is denoted by $\{\bar{r}_i\}$.

2) Energy Demodulation: With the optimal RSSI samples $\{\bar{r}_i\}$, the ZigBee node will decode the CTC data bits through energy decoding. The process is pretty simply: if an RSSI value is over a threshold β, the corresponding bit is '1', otherwise the bit is '0'.

The threshold β can not be fixed due to the varied RSSI values, which changes with the transmission power, the transmitter-receiver distance, etc. Here we simply use the mean value m_r of $\{r_i\}$ as the threshold. As $r_i = x_i + n_i$, where x_i indicates the transmitting signal and n_i is the noise with fixed mean value among the received samples, the value m_r can obviously vary adaptively with background noise.

C. SLEM Design at WiFi Receiver Side

After receiving the transmitted signal, the WiFi receiver first conducts the 802.11 standard receiving process to obtain the SLEM bits, then conducts a recovery process to get the original WiFi data bits.

1) Overview of WiFi Receiving: As shown in Fig. 7, according to the standard, the received signal is passed through the OFDM demodulation and QAM demodulation module sequentially to recover the SLEM bits. We note

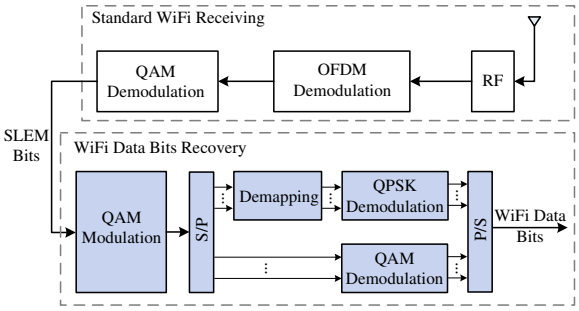
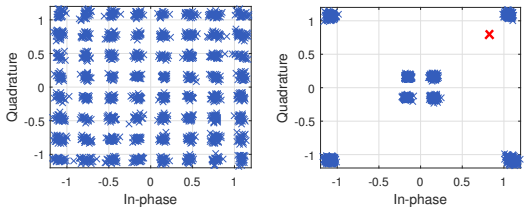


Fig. 7. The WiFi receiving process.

that the level M of QAM is related to the RATE field in the packet header, which is set at the transmitter side according to the adopted QAM type. The receiver will obtain the value at first for the following QAM demodulation.

As to SLEM design, the SLEM bits will be first transformed to QAM constellation points and then shapes in parallel, so that differential processes are conducted for each subcarrier: the points within the subcarriers for CTC will be demapped to QPSK points for QPSK demodulation, while the other points will be demodulated through QAM. WiFi data bits are obtained through combining the bits recovered from the two ways. These processes are generally the inverse processes of those in the transmitting side, as depicted in Fig. 3(b).



(a) Normal WiFi signal. (b) SLEM signal.

Fig. 8. Constellation points at the receiver side under QAM-64. The red cross can be corrected to the top right point through *soft demapping*.

2) Demapping: The demapping module is to map the QAM constellation points to the QPSK constellation points, it can use the same mapping table as that in the remapping process, as discussed in Section IV-A2. For example, in Fig. 1, both the QAM-16 points '0000' and '0011' correspond to one QPSK point '00'.

Besides the aforementioned simple process, we further propose a *soft demapping* scheme to improve the performance of WiFi transmission. The key insight of this design is based on the observation that, the SLEM signal within the ZigBee channel possesses much less constellation points compared to the normal WiFi signal, as shown in Fig. 8, and some errors can be corrected in this situation. This scheme is achieved in the following process: after QAM demodulation, if a constellation point does not fall into the eight points for CTC transmission, the receiver calculates the distances between it and the eight points, then corrects it to the one with the shortest distance. Through this way, the red cross in Fig. 8(b) can be corrected to the top right point successfully

V. Theoretical Analysis

In this part, we try to theoretically figure out the SLEM performance of delivering both the WiFi and CTC data bits.

A. Analysis for CTC Transmission

1) Symbol Error Rate (SER): From the perspective of CTC transmission, the bits are transmitted by symbols with two energy levels E_H and E_L. We let $\{x_i\}$ indicate the transmitting signal, and let the CTC symbol duration τ_{CTC} be large enough such that the optimal RSSI sample sets $\{\bar{r}_i\}$ can represent the actual energy of the received signal.

We have:

$$\bar{r}_i = x_i + n_i, \tag{1}$$

where the noise n_i is the additive white gaussian noise (AWGN) and $n_i \sim \mathcal{N}(0, \sigma^2)$. Then, the received signal r_i also subjects to the normal distribution with the mean of x_i and the variance of σ^2. That means, for the symbol x_i with mean $A_L = \sqrt{E_L}$, the received signal $r_i \sim \mathcal{N}(A_L, \sigma^2)$; for the symbol x_i with mean $A_H = \sqrt{E_H}$, $r_i \sim \mathcal{N}(A_H, \sigma^2)$.

Fig. 9 depicts the relationship of the probability density function (PDF) of the two symbols. With $\{\bar{r}_i\}$, the symbol is determined to be '1' if $\bar{r}_i > \beta$, otherwise it represents '0'. Here β is set as $\frac{A_L+A_H}{2}$. In real network situations, the number of '1' or '0' is nearly equal within a packet, thus, β here is approximate to that in Section IV-B2.

A symbol error occurs when '1'/'0' is transmitted but '0'/'1' is detected, as the shaded area shown in Fig. 9, then the symbol error probability is calculated as:

$$P_e = P(\bar{r}_i < \beta) = Q(\frac{A_H - A_L}{2\sigma}). \tag{2}$$

where $Q(x) = \int_x^{+\infty} \frac{1}{\sqrt{2\pi}} exp(-\frac{1}{2}t^2)dt$. Using this equation and $SNR = \frac{E_s}{\sigma^2} = \frac{E_L+E_H}{2\sigma^2}$, we can calculate the theoretical SER values of each kind of mechanisms.

(i) PLEM: It makes the symbol '0' or '1' transmitted through the absence or presence of a data packet. It can be regarded as a special case of the aforementioned situation where $E_L = 0$. As $SNR = \frac{E_H}{2\sigma^2}$, we have:

$$P_e(PLEM) = Q(\sqrt{\frac{SNR}{2}}). \tag{3}$$

(ii) SLEM: The SER of SLEM changes with the QAM modulation types. When QAM-16 is adopted, as shown in Fig. 1, $A_H = 3A_L$ and we have:

$$P_e(SLEM\_16P) = Q(\sqrt{\frac{SNR}{5}}), \tag{4}$$

Similarly, for QAM-64, $A_H = 7A_L$ and:

$$P_e(SLEM\_64P) = Q(\frac{3}{5}\sqrt{SNR}). \tag{5}$$

For QAM-256, $A_H = 15A_L$ and:

$$P_e(SLEM\_256P) = Q(\sqrt{\frac{49}{113}SNR}). \tag{6}$$

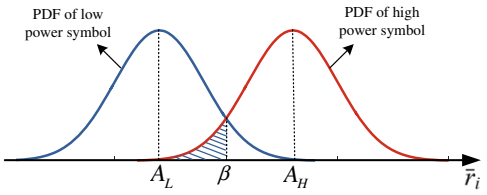


Fig. 9. The probability density function (PDF) of CTC symbols with low and high energy levels.

2) Packet Error Rate (PER): A packet error occurs once one or more symbol errors occur. The packet error rate (PER) P_{ep} of a CTC packet with L_z-bit length is:

$$P_{ep} = 1 - (1 - P_e)^{L_z}. \tag{7}$$

3) Summary: Fig. 10 depicts the theoretical SER and PER of PLEM and SLEM, where the CTC symbol duration $\tau_{CTC} = 160\mu s$ and $L_z = 32bits$, which implies that the required WiFi transmission duration $\tau_w = 160\mu s \cdot L_z = 5.12ms$. The results demonstrate that the SER and PER of CTC transmission under QAM-16 is much lower than PLEM, while that of SLEM under QAM-256 highly approaches PLEM. In addition, we see that when the modulation type changes from QAM-16 to QAM-64, the CTC has remarkable performance improvement; however, when it changes from QAM-64 to QAM-256, the improvement is not so significant. Moreover, SER increases obviously when τ_{CTC} decreases, since the value of $A_H - A_L$ in Eq. (2) decreases in this situation.

B. Analysis for WiFi Transmission

SLEM demotes the high-order QAM modulation to the low-order QPSK modulation for the WiFi data transmission in the CTC subcarriers. It sacrifices some performance of WiFi to achieve the WiFi and CTC concurrent transmissions. Here we want to quantify how the WiFi performance is affected.

Performance of both QPSK and QAM modulations have been studied for a long history. Here we simply borrow the results from [13] and neglect the details of the equation derivation due to the page limit. For the AWGN channel, the bit error rate (BER) of QPSK can be calculated as:

$$P_{eb}(QPSK) = Q(\sqrt{2 \cdot SNR}). \tag{8}$$

As to the M-level QAM modulation, the BER is:

$$P_{eb}(QAM) = \frac{4}{log_2(M)} Q(\sqrt{\frac{3 \cdot SNR \cdot log_2(M)}{M-1}}). \tag{9}$$

The PER of a WiFi packet with L_w-byte length can be calculated through the similar equation as Eq. 7. To analyze the performance under the same situation as Fig. 10 where $\tau_w = 5.12ms$, the L_w value should vary with the modulation type. According to the WiFi transmission process, $log_2(M)$ bits are mapped to one QAM constellation point, and 48 points are fed into one OFDM symbol, which lasts for $4\mu s$. Then the required WiFi packet length L_w resulting in τ_w is, $L_w = \tau_w/\tau_s \cdot 48 \cdot log_2(M)/8$.

Fig. 11 demonstrates the BER and PER of WiFi transmission in terms of SNR under different modulation types.

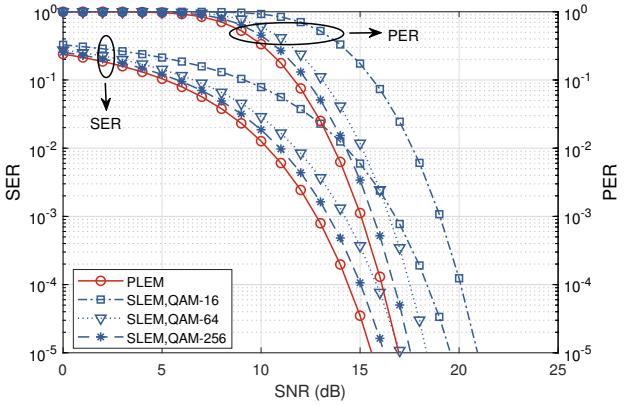


Fig. 10. SER and PER of PLEM and SLEM in terms of SNR when $L = 4bytes$.

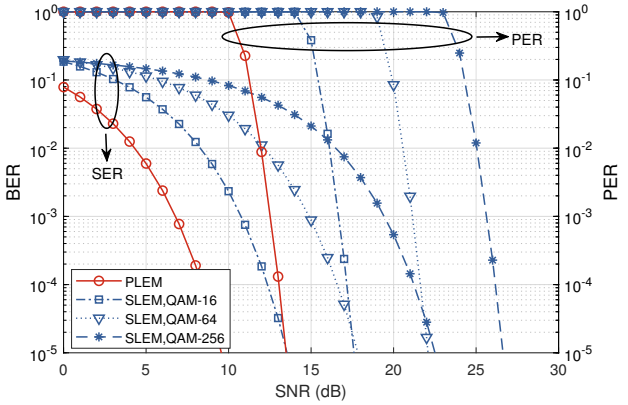


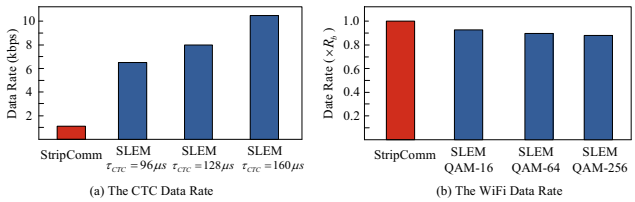
Fig. 11. BER and PER of WiFi data transmission in terms of SNR under different modulation types.

We see that both BER and PER increase under the higher order modulation type. Especially, to achieve concurrent WiFi and CTC data transmissions and guarantee the BER of 10^{-5}, QAM-16 has about $4dB$ cost, QAM-64 has about $8dB$ cost, and QAM-256 has about $13dB$ cost. Combining both Fig. 10 and Fig. 11, we see that there is obviously a tradeoff between the CTC and WiFi performance, as adopting the higher order modulation type can increase the CTC performance, but decreases the WiFi performance. QAM-16 and QAM-64 can be determined according to the situations of both the CTC and WiFi links. QAM-256 is not a good choice, not only because the CTC performance improvement is much limited, but also because the WiFi performance degradation is significant.

C. Data Rate

The CTC data rate of SLEM is mainly determined by τ_{CTC}, and its theoretical value is $\frac{1}{\tau_{CTC}} Kbps$. Fig. 12(a) demonstrates the comparison of CTC data rate under different mechanisms. Since SLEM can deliver a set of CTC data bits through one WiFi packet, its data rate can outperform all the PLEM mechanisms. Compared to the state-of-art StripComm [3] which can achieve about $1.1kbps$ data rate, SLEM has at least $6kbps$ data rate. Especially, when $\tau_{CTC} = 96\mu s$, the data rate can be up be about $10kbps$.

For the WiFi data transmission, it is hard to give a specified data rate R_w as it is related to many factors except the QAM modulation types. Thus, we use StripComm [3] as the baseline, set its data rate as R_b to evaluate that of SLEM. Since the ZigBee channel is $2MHz$ and the bandwidth of each subcarrier is $312.5KHz$, seven out of the 48 data subcarriers should be utilized for CTC data transmission. Thus, with one CTC transmission, SLEM under QAM-16 has about $92.7\% \times R_b$ data rate, the values under QAM-64 and QAM-256 are about $90.2\% \times R_b$ and $89.6\% \times R_b$ respectively, as depicted in Fig. 12(b).



(a) The CTC Data Rate (b) The WiFi Data Rate

Fig. 12. Comparison of data rate for CTC transmission.

VI. Experimental Evaluation

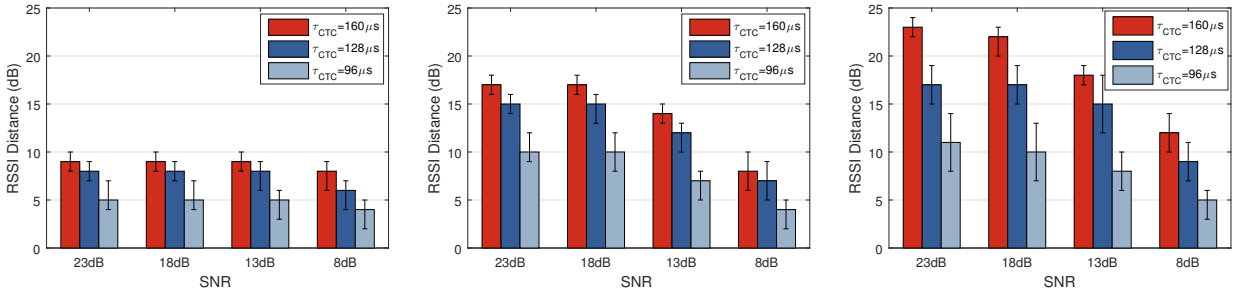
A. Experimental Settings

We implement a prototype of SLEM containing the Universal Software Radio Peripheral (USRP) N210 and TelosB. We use USRP N210 to generate the WiFi signals following the IEEE 802.11 standard, while the SLEM bits are obtained through MATLAB based on the WiFi and CTC data bits, both of which are generated randomly. We use TelosB, a commercial ZigBee platform, to collect the RSSI samples of the CTC signal. For each WiFi data packet, the CTC bits required to transmit is first fixed and the WiFi data transmission duration is set accordingly. Other parameters such as τ_{CTC}, QAM modulation type and SNR vary as required. In addition, as SLEM needs spectrum overlap for CTC transmission, we let USRP N210 work at 2.474GHz, which is the $13th$ WiFi channel at 2.4GHz, and let TelosB work at 2.475GHz, which is the $25th$ ZigBee channel. The following results are mainly based on this configurations. We have also tested other combinations of WiFi and ZigBee channels, the results have little change except when the ZigBee channel is overlapped with the WiFi null subcarriers.

B. Performance of CTC Transmission

1) RSSI Distance: The RSSI distance obviously affects the CTC performance. Here we test the RSSI distance with the affect of τ_{CTC}, SNR and QAM modulation types. In addition, we let the USRP N210 transmit WiFi signals with a fixed power, and adjust the distance between USRP N210 and TelosB to make the received CTC signals have designated SNRs, since the background noise varies very slightly and is approximate to $-90dBm$.

Fig. 13 demonstrates that the RSSI distance increases obviously with the QAM level, and the adoption of QAM-256 results in the largest RSSI distance, as shown in Fig. 13(c). In the case of high SNR situations, such as $23dB$, the RSSI distance is about 23dB with QAM-256, while the value is 16dB with QAM-64, and $9dB$ with QAM-16. In addition, the RSSI distance decreases significantly with the



(a) QAM-16. (b) QAM-64. (c) QAM-256.

Fig. 13. The RSSI distance in terms of SNR and τ_{CTC} under different QAM modulation types.

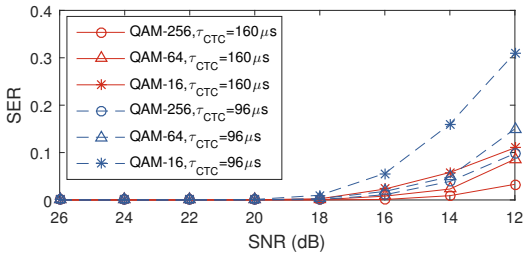


Fig. 14. SER of CTC transmission in terms of SNR under different modulation types and τ_{CTC}.

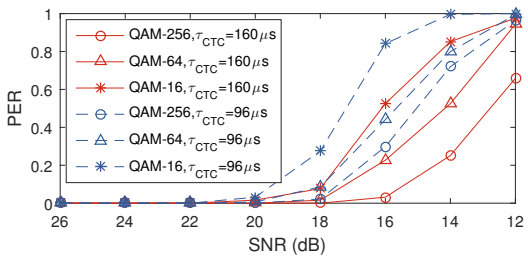


Fig. 15. PER of CTC transmission in terms of SNR under different modulation types and τ_{CTC}.

decrease of τ_{CTC} and SNR. For example, in Fig. 13(a), the RSSI distance with $\tau_{CTC} = 96\mu s$ has about $5dB$ decrease compared to $\tau_{CTC} = 160\mu s$ when SNR is as high as $23dB$.

2) SER and PER: The factors which affect the RSSI distance finally affect the SER and PER significantly, such as the received SNR, τ_{CTC}, and QAM modulation types. Fig. 14 depicts the SER of CTC transmission in terms of SNR under each QAM modulation type, while τ_{CTC} is set to be $160\mu s$ and $96\mu s$, respectively. We see that when SNR is above $18dB$, SER is approximate to zero nearly in all the situations; it has obvious increase when SNR decreases from $18dB$. We also see that although the smaller τ_{CTC} will inevitably result in more errors, it still exhibits a quite good performance when QAM-256 or QAM-64 is adopted. For example, the combination of QAM-256 and $\tau_{CTC} = 96\mu s$ results in a better performance than the combination of QAM-16 and $\tau_{CTC} = 160\mu s$.

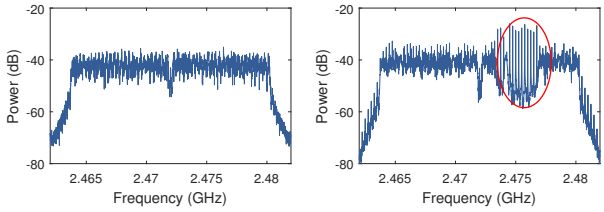
Fig. 14 depicts the PER of CTC transmission in each situation of Fig. 14, and the CTC packet length is $32bits$. We see that when QAM-256 is adopted and $\tau_{CTC} = 160\mu s$, PER is below 0.2 when SNR is above $14dB$. For the other situations, the same performance can be achieved only when SNR is above $18dB$.

The experimental performance is much lower than the theoretical counterpart, as we use the simplified model in the theoretical analysis. Actually, the results in Fig. 10 can be regarded as the upper bound of CTC transmission.

C. Performance of WiFi Transmission

1) Signal Analysis: We first intend to analyze how the SLEM design affects the signal transmissions.

Fig. 16 depicts the spectrum density of both WiFi and SLEM signals under QAM-16, while both the WiFi and CTC data bits are generated randomly. We see that the SLEM signal obviously exhibits much higher peak values within the ZigBee channel, while that value out of the ZigBee channel remains similar to the WiFi signal. The spectrum density is barely affected by the the value τ_{CTC}, and that under both QAM-64 and QAM-256 has the similar feature. Fig. 16 impels us to figure out how the SLEM design affects the WiFi transmissions.



(a) Normal WiFi Signal (b) SLEM Signal

Fig. 16. Spectrum density of two kinds of packets.

One key related characteristic which affects the WiFi performance is the peak-to-average-ratio (PAPR) of the time domain signal, as the higher PAPR results in lower performance due to degrading the efficiency of the power amplifier, thus may lead to lower transmission power with the same transmission gain. We get the cumulative distribution function (CDF) of PAPR for the two kinds of signals, the results are shown in Fig. 17. We see that the PAPR of SLEM signal is just slightly over that of the WiFi signal. We also test the receiving power levels of the two kinds of signals under the same configurations, such as the transmission gain and transmitter-receiver distance, and find that they have no distinguishable difference. These results show that the SLEM design has little effect on the WiFi signal transmissions except the slightly decreased data rate.

2) PER: Fig. 18 depicts the PER of WiFi transmission in terms of SNR under QAM-16 and QAM-64 modulation

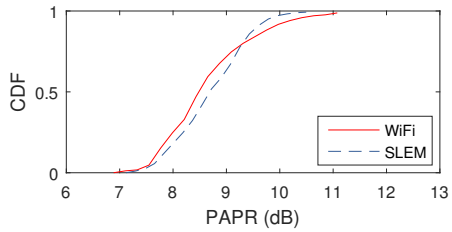


Fig. 17. The cumulative distribution function (CDF) of PAPR for both the normal WiFi and SLEM signals under QAM-16.

types. We do not show the results of QAM-256, as the WiFi performance under this situation is rather bad even when the SNR is high enough (over 50dB). This problem can certainly be solved through some methods, such as adding more redundancy, but it is no the key issue of this paper. The value τ_{CTC} is not used as a parameter as we find it hardly affect the WiFi performance in the experiments. The packet length is set to make the packet transmission duration equal to that in the CTC experiments.

The experimental results are much worse than the theoretical ones shown in Fig. 11, which actually gives the theoretical lower-bound for the WiFi performance. We see that when SNR is $35dB$ or above, PER is approximate to zero under the two QAM modulations, and it obviously increases when SNR decreases from $35dB$. Especially, when SNR is $20dB$, the PER of QAM-64 is over 50%, while that of QAM-16 still demonstrates a good performance. In addition, the transmission of SLEM signals results in a slightly lower PER compared to the WiFi signals, due to the design of soft demapping. As the soft demapping just works within the seven out of the 48 subcarriers, the averaged performance has only a slight improvement.

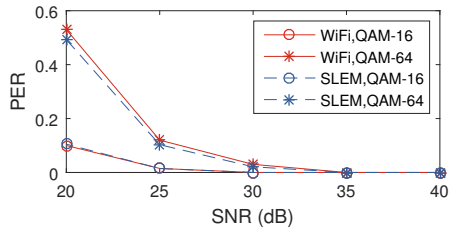


Fig. 18. Performance of WiFi transmissions.

VII. Related Work

Recent years have seen numerous research works on CTC between heterogenous devices at the $2.4GHz$ ISM band [1], [2], [8], [10], [14]–[19]. This paper focuses on WiFi to ZigBee CTC, and the previous works fall into two categories: *physical-layer CTC* and PLEM.

The *physical-layer CTC* was firstly proposed by WEBee [1] to make a commercial WiFi device elaborately construct the WiFi payload to transmit a ZigBee-compliant packet through signal emulation, which would then be detected by a ZigBee device directly. TwinBee [14] and LongBee [20] were further designed to improve its reliability and transmission range. They has the high CTC rate comparable to a ZigBee radio. The main problem of these mechanisms is that they can not work under the standard WiFi and ZigBee channels. As shown in Fig. 19, one standard WiFi channel overlaps with four ZigBee channels, while three of them overlap with the pilot subcarriers, and the last one overlaps with the null subcarriers, all the situations are not suitable for CTC transmissions.

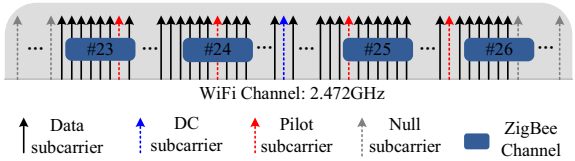


Fig. 19. An illustration of a WiFi channel overlapping with ZigBee channels.

PLEM is the pioneer in the CTC area. Esense [5], [6] induces an "alphabet set" for transmitting information between WiFi and ZigBee through certain durations. FreeBee [2] utilizes the interval between beacons to represent the conveyed information. C-Morse [8] and DCTC [9] propose to exploit a set of WiFi packets with carefully designed transmission duration to convey ZigBee information. WiZig [7] proposes a rate adaptation algorithm according to the channel conditions to optimize the CTC throughput; StripComm [3] introduces the concept of Manchester Coding to the packet level energy modulation to resist interference. All these mechanisms have low CTC data rate and are MAC incompatible with commercial devices, inducing severe interference to current wireless networks.

VIII. Conclusion and Discussion

In this paper, we present the design and implementation of SLEM, a novel CTC method which delivers both the WiFi and CTC data bits concurrently through one standard WiFi packet. Beyond SLEM, two aspects of CTC are worthy of further study.

At first, current CTC mechanisms including SLEM mainly focus on the physical layer design, and simplify the integration of CTC at the upper layer. Since CTC varies the communication methods among wireless devices, we believe this will lead to significant changes in the upper layer design, which need further investigation.

In addition, the distinct physical layer technologies adopted by heterogeneous devices result in quite specific design of CTC. For example, the CTC mechanisms from ZigBee to WiFi, WiFi to ZigBee and Bluetooth to ZigBee may be totally different. In real networks, it is worthy to study which physical layer technology should be used by a device under certain situations.

Acknowledgments

This research was supported in part by the China NSFC Grant (61702343, 61872248, 61672320, 61802263, U1736207), Guangdong NSF 2017A030312008, Fok Ying-Tong Education Foundation for Young Teachers in the Higher Education Institutions of China (161064), Shenzhen Science and Technology Foundation (ZDSYS20190902092853047), Faculty Research Fund of Shenzhen University (2019052, 860/000002110322), GDUPS (2015). Kaishun Wu is the corresponding author.

REFERENCES

[1] Z. Li and T. He, "WEBee: physical-layer cross-technology communication via emulation," in *Proc. of the ACM MobiCom*, 2017.

[2] S. M. Kim and T. He, "FreeBee: cross-technology communication via free side-channel," in *Proc. of the ACM MobiCom*, 2015.

[3] X. Zheng, Y. He, and X. Guo, "StripComm: interference-resilient cross-technology communication in coexisting environments," in *Proc. of the IEEE INFOCOM*, 2018.

[4] Z. Yin, Z. Li, S. M. Kim, and T. He, "Explicit channel coordination via cross-technology communication ," in *Proc. of the ACM MobiSys*, 2018.

[5] Y. Zhang and Q. Li, "HoWiES: a holistic approach to ZigBee assisted WiFi energy savings in mobile devices," in *Proc. of the IEEE INFOCOM*, 2013.

[6] K. Chebrolu and A. Dhekne, "Esense: communication through energy sensing," in *Proc. of the ACM MobiCom*, 2009.

[7] X. Guo, X. Zheng, and Y. He, "WiZig: cross-technology energy communication over a noisy channel," in *Proc. of the IEEE INFOCOM*, 2017.

[8] Z. Yin, W. Jiang, S. M. Kim, and T. He, "C-Morse: cross-technology communication with transparent Morse coding," in *Proc. of the IEEE INFOCOM*, 2017.

[9] W. Jiang, Z. Yin, S. M. Kim, and T. He, "Transparent cross-technology communication over data traffic," in *Proc. of the IEEE INFOCOM*, 2017.

[10] X. Zhang and K. G. Shin, "Gap sense: lightweight coordination of heterogeneous wireless devices," in *Proc. of the IEEE INFOCOM*, 2013.

[11] IEEE Computer Society. 802.11, "Wireless LAN medium access control (MAC) and physical layer (PHY) specifications amendment 5: Enhancements for higher throughput," 2009.

[12] M. S. Gast, "802.11ac: A survival guide," *O'Reilly Media*, 2013.

[13] A. Goldsmith, "Wireless communications," *Cambridge University Press*, 2005.

[14] Y. Chen, Z. Li, and T. He, "TwinBee: reliable physical-layer cross-technology communication with symbol-level coding," in *Proc. of the IEEE INFOCOM*, 2018.

[15] X. Guo, Y. He, X. Zheng, Z. Yu, and Y. Liu, "LEGO-Fi: transmitter-transparent CTC with cross-demapping." in *Proc. of the IEEE INFOCOM*, 2019.

[16] Z. Chi, Y. Li, H. Sun, Y. Yao, Z. Lu, and T. Zhu, "B^2W^2: N-way concurrent communication for IoT devices." in *Proc. of the ACM Sensys*, 2016.

[17] W. Jiang, Z. Yin, R. Liu, S. M. Kim, Z. Li, and T. He, "BlueBee: a 10,000x faster cross-technology communication via PHY emulation." in *Proc. of the ACM Sensys*, 2017.

[18] W. Jiang, S. M. Kim, Z. Li, and T. He, "Achieving receiver-side cross-technology communication with cross-decoding," in *Proc. of the ACM MobiCom*, 2018.

[19] S. Wang, S. M. Kim, and T. He, "Symbol-level cross-technology communication via payload encoding." in *Proc. of the IEEE ICDCS*, 2018.

[20] Z. Li and T. He, "LongBee: enabling long-range cross-technology communication," in *Proc. of the IEEE INFOCOM*, 2018.