Simultaneous Data Dissemination Among WiFi and ZigBee Devices

Wei Wang, Xin Liu, Yao Yao, Zicheng Chi, *Member, IEEE*, Stuart Ray, Ting Zhu, and Yanchao Zhang, *Fellow, IEEE*

***Abstract*— Recent advances in Cross-Technology Communication (CTC) have opened a new door for cooperation among heterogeneous IoT devices to support ubiquitous applications, such as smart homes and smart offices. However, existing work mainly focuses on physical layer performance improvements. In this paper, we explore how to leverage the latest CTC techniques for network layer performance improvements. Specifically, we introduce Waves, which leverages WiFi to ZigBee CTC and WiFi access point's adaptive transmit power control techniques for reliable and fast data dissemination in low-duty-cycle ZigBee networks. We extensively evaluate our design under various settings. Evaluation results show that Waves can provide reliable data dissemination and is 33.5 times faster than the state-of-the-art protocol in terms of dissemination time.**

***Index Terms*— Cross-technology communication, wireless communication, wireless networks.**

I. Introduction

THE exponentially increasing number of IoT devices leads to densely coexisting wireless technologies in the unlicensed spectrum (i.e., ISM bands). To leverage the unique features of coexisting wireless technologies, researchers have proposed cross-technology communication (CTC) techniques [1], [2], [3], [4] that enable direct communication between WiFi and ZigBee without requiring any additional hardware (e.g., gateways). One of the most recent CTC techniques – WEBee [3] enables high throughput communications among commodity WiFi and ZigBee devices. By controlling the WiFi's payload, WEBee emulates the ZigBee signal that can be demodulated at the commodity ZigBee node. Since WEBee utilizes only 7 out of 64 WiFi subcarriers that are overlapped with the ZigBee channel to conduct signal emulation, the remaining majority of WiFi subcarriers are still able to transmit WiFi data. As demonstrated in PMC [4], the WiFi device can conduct parallel WiFi-to-WiFi and WiFi-to-ZigBee communications by using a single WiFi data stream.

The advances in CTC techniques at the physical layer are very encouraging. However, little work has been proposed to explore the network layer design for physical layer CTC techniques. To fill this gap, we introduce Waves, which leverages WiFi to ZigBee CTC and WiFi access point's adaptive transmit power control techniques for reliable and fast data dissemination in low-duty-cycle ZigBee networks. Figure 1 shows the difference between a traditional approach and our approach. As shown in Figure 1 (a), when the WiFi-ZigBee dual-radio gateway needs to send out the ZigBee packets and WiFi packets, the gateway has to send out packets in different time slots to avoid collisions with the WiFi and ZigBee devices. In our approach (see Figure 1 (b)), the WiFi AP broadcasts hybrid packets that contain both ZigBee data and WiFi data using the latest CTC techniques [3], [4]. The ZigBee data and WiFi data can be demodulated by corresponding commodity ZigBee and WiFi devices. To minimize the interference with other coexisting IoT devices and save energy, the WiFi AP uses the adaptive transmission power control technique, which has been defined in IEEE 802.11 standard [5] and proved to be very effective by many researchers [6], [7], [8]. Therefore, when the WiFi AP needs to send packets to another WiFi device (e.g., $W2$ in Figure 1 (b)), it increases its transmission power, which also enables the WiFi AP to reach ZigBee node $Z2$ (shown in Figure 1 (c)). In our design, we use fountain code to encode the ZigBee-WiFi hybrid packets to enable reliable communication from WiFi AP to ZigBee nodes under unreliable wireless communication environments. After the WiFi AP sends out sufficient ZigBee-WiFi hybrid packets to ZigBee nodes, it can send pure WiFi packets to WiFi devices. ZigBee nodes can propagate the data dissemination inside the low-duty-cycle ZigBee networks (in Figure 1 (d)). In addition, we use a linear network coding technique to encode the ZigBee-to-ZigBee packets and further reduce the redundant transmissions.

The advantages of Waves are as follows: i) it seamlessly enables the simultaneous WiFi-to-WiFi communication and ZigBee data dissemination. Unlike traditional protocols that treat WiFi-to-WiFi communication as interference and force ZigBee nodes to back-off, our hybrid ZigBee-WiFi packet transmissions can significantly reduce the ZigBee data dissemination delay while still preserve the original

Manuscript received 27 June 2022; revised 26 December 2022; accepted 3 February 2023; approved by IEEE/ACM TRANSACTIONS ON NETWORKING Editor M. Caesar. Date of publication 20 April 2023; date of current version 19 December 2023. This project is partially supported by NSF grants CNS-1652669, CNS-1824491, CNS-1824355, CNS-1933069, CNS-2305246, CNS-2127881, and CNS-2055751. *(Corresponding author: Ting Zhu.)*

Wei Wang and Stuart Ray are with the Department of Computer Science, Saint Louis University, St. Louis, MO 63103 USA (e-mail: wei.wang.5@slu.edu; stuart.ray@slu.edu).

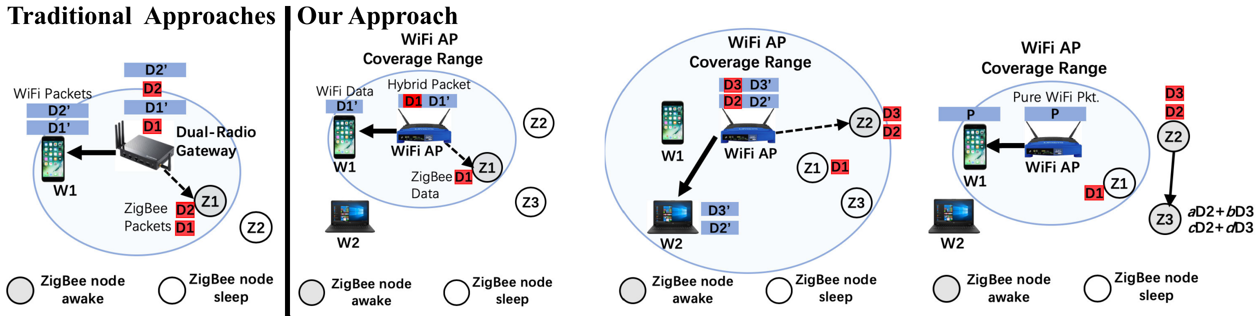
Xin Liu and Ting Zhu are with the Department of Computer Science and Engineering, The Ohio State University, Columbus, OH 43210 USA (e-mail: liu.10663@osu.edu; zhu.3445@osu.edu).

Yao Yao is with the Department of Computer Science and Electrical Engineering, University of Maryland, Baltimore, MD 21250 USA (e-mail: of90379@umbc.edu).

Zicheng Chi is with the Department of Electrical Engineering and Computer Science, Cleveland State University, Cleveland, OH 44115 USA (e-mail: z.chi@csuohio.edu).

Yanchao Zhang is with the School of Electrical, Computer and Energy Engineering, Arizona State University, Tempe, AZ 85287 USA (e-mail: yczhang@asu.edu).

Digital Object Identifier 10.1109/TNET.2023.3243070



(a) The dual-radio gateway sends out ZigBee packets and WiFi packets at different time slots to avoid collisions at the WiFi and ZigBee devices.

(b) WiFi AP broadcasts hybrid packets to W1 and Z1 using low transmit power to achieve simultaneous WiFi and ZigBee data delivery.

(c) WiFi AP broadcasts hybrid packets to W2 and Z2 using high transmit power. Z3 is asleep, so it cannot receive packets from WiFi AP.

(d) When WiFi AP is sending pure WiFi packets to W1, Z2 can forward the ZigBee data to Z3 using linear network coding after Z3 is awake.

Fig. 1. Compared to traditional approaches, our approach enables the simultaneous WiFi-to-WiFi communication and ZigBee data dissemination. Therefore, it can achieve more efficient spectrum utilization and significantly reduce the delay in ZigBee networks.

WiFi-to-WiFi communication; ii) since WiFi devices normally transmit at 20dBm while ZigBee nodes transmit at 0dBm, the WiFi AP has a much larger communication range than that of ZigBee-to-ZigBee communication. Therefore, the WiFi AP can cover a greater number of ZigBee nodes in each transmission, which further reduces the delay; and iii) by using the WiFi-to-ZigBee CTC for ZigBee network data dissemination, the overall dissemination reliability is increased.

To transform the idea behind Waves into a practical system, we need to overcome the following three main challenges. First, the WiFi device does not know the working schedule of the ZigBee node. Different from traditional homogeneous IoT networks (i.e., WiFi network or ZigBee network), it is difficult for ZigBee to inform WiFi of its working schedule. This is because the ZigBee to WiFi communication is packet-level CTC. It requires the ZigBee device to generate duplicated packets to transmit several bits [1], [2], [9], which may introduce a huge overhead to the network. To overcome this challenge, we introduce a *Cross-technology Sensing approach* that only requires the WiFi device to passively sense the ZigBee network without introducing additional traffic. Second, the traditional WiFi adaptive power control is designed for improving the spectral efficiency and reducing the interference in the WiFi network [10], which does not take CTC and the ZigBee traffic into consideration. Simply determining the transmission power based on the WiFi network may result in reducing the ZigBee network performance. To overcome this challenge, we model the interference in the WiFi and ZigBee coexistence network and introduce a *transmission power optimization method* to determine the WiFi transmission power. Third, the WiFi does not know the transmission status from the WiFi to ZigBee communication. In the traditional ZigBee network, the sender can expect the receiver to transmit acknowledgements (ACKs) to guarantee data dissemination reliability. However, due to the large overhead introduced by packet-level ZigBee to WiFi communication, this approach is not applicable. To overcome this challenge, we propose a *Distributed Fountain Codes Transmission scheme*, which does not require feedbacks from the receiver. Moreover, this technique has the additional advantage of improving the data dissemination reliability.

In summary, the contributions of this paper are as follows:

• To the best of our knowledge, this is the first work that investigates how to use CTC for providing reliable and fast data dissemination in ZigBee networks. We believe that the design principles and challenges in Waves are generic and applicable to a whole set of future heterogeneous IoT network layer design that leverages CTC for further performance improvements.

• We design a WiFi AP Initiated Dynamic Broadcasting (WIDB) to find the optimal solution for the WiFi device to control its transmission power. We also introduce a Distributed Fountain Codes Transmission (DFCT) techniques to conduct reliable data dissemination from WiFi to ZigBee.

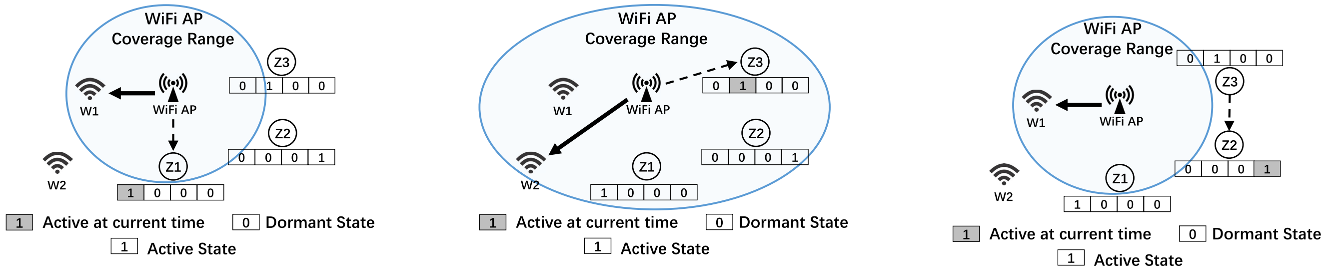
• We implemented our design on USRP and TelsoB nodes and extensively evaluated our design under different settings. The evaluation results demonstrate that Waves is reliable and 33.5 times faster than the state-of-the-art protocol in terms of the dissemination time.

II. Key Mechanisms in Waves

There are two key mechanisms in Waves to provide fast and reliable data dissemination:

• **WiFi AP Initiated Dynamic Broadcasting (WIDB):** Waves utilizes the WiFi AP to conduct data dissemination for ZigBee nodes. By leveraging WiFi adaptive power control, the packets are transmitted to ZigBee nodes at different distances, which avoids cross-technology interference (CTI) and reduces the delay introduced by the low duty-cycle of ZigBee nodes.

• **Distributed Fountain Codes Transmission (DFCT):** To enable reliable data dissemination and reduce the impact on the WiFi-to-WiFi communication, we introduce a Distributed Fountain Codes Transmission technique which only requires the WiFi AP to deliver a limited number of coded packets to a subset of ZigBee nodes inside the ZigBee networks. As a result, Waves can conduct reliable data dissemination and has little impact on original WiFi-to-WiFi communications.



(a) WiFi AP simultaneously transmits WiFi packets and ZigBee packets to $W1$ and $Z1$, respectively.

(b) By controlling the transmission power, WiFi AP can communicate with $W2$ and $Z3$. The corresponding delay is only two time slots.

(c) WiFi AP is communicating with $W1$ while $Z3$ can transmit received packets to $Z2$.

Fig. 2. An example of WiFi AP initiated dynamic broadcasting.

A. Benefits of WIDB

The mechanism of WiFi AP initiated dynamic broadcasting allows the WiFi AP to conduct data dissemination for ZigBee nodes. In contrast, traditional approaches may face high CTI from the WiFi traffic [11], [12], [13] and may not conduct data dissemination due to the Carrier Sense Multiple Access (CSMA) scheme adopted by ZigBee nodes. Even if we assume that ZigBee nodes do not encounter CTI, the multi-hop transmissions in low-duty-cycle ZigBee networks still introduce high delays.

In Waves, we leverage the WiFi adaptive power control to overcome this challenge. Specifically, the transmission power of a typical WiFi AP can dynamically change from 0dBm to 20dBm. As the WiFi AP changes its transmission power to communicate with other WiFi devices, it can simultaneously conduct data dissemination to the ZigBee nodes at different distances. By doing this, we can reduce the number of hops, reduce the CTI and significantly reduce the delay. For the sake of clarity, a simplified example is shown in Figure 2(a). In the first time slot, the WiFi AP is communicating with $W1$. Since $Z1$ is active, the WiFi AP simultaneously transmits ZigBee data to $Z1$ and WiFi data to $W1$ using ZigBee-WiFi hybrid packets. Then, as shown in Figure 2(b), the WiFi AP increases the transmission power to communicate with $W2$ at the second time slot. Since $Z3$ is active, the WiFi AP can simultaneously transmit packets to $Z3$. At the fourth time slot, the WiFi AP communicates with $W1$ again (in Figure 2(c)). Since $Z2$ and $Z3$ are not interfered by the WiFi AP, $Z3$ can transmit received packets to $Z2$. In this example, instead of waiting for multi-hop transmissions in the ZigBee device and avoiding the CTI, each ZigBee node receives the data after switching to the active state. **In summary**, *WiFi AP initiated dynamic broadcasting can avoid the CTI and significantly reduce the data dissemination delay*.

B. Benefits of DFCT

Normally, the sender expects the receiver to transmit acknowledgements (ACKs) to guarantee the data dissemination reliability. However, in CTC networks, although several approaches have enabled ZigBee-to-WiFi CTC [2], [4], [14], it is still difficult for ZigBee nodes to transmit ACKs to the WiFi AP due to the following reasons: i) Since the WiFi AP is transmitting packets to other WiFi devices, it cannot receive

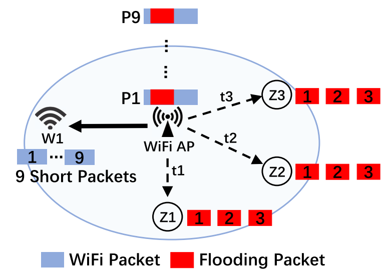


Fig. 3. The WiFi AP transmits coded packets to $Z1$, $Z2$ and $Z3$ during their wake up time $t1$, $t2$, and $t3$, respectively.

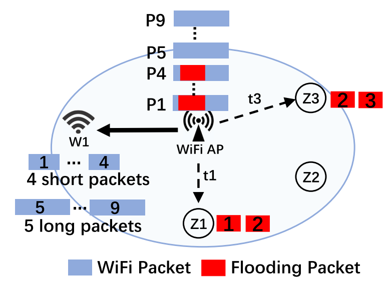


Fig. 4. The throughput of WiFi AP to $W1$ is much higher since only 4 out of 9 WiFi packets are short packets.

ZigBee packets at the same time; ii) Current WiFi-to-ZigBee and ZigBee-to-WiFi CTC are based on different techniques. For instance, the communication from ZigBee to WiFi may be based on packet-level CTC, which requires the ZigBee nodes to generate a huge number of packets to initiate the ZigBee to WiFi communication. These generated packets will introduce high network overhead and interfere with the ongoing WiFi-to-WiFi communications.

In Waves, the WiFi AP uses fountain codes to encode ZigBee packets for reliable data dissemination. Prior work [15] requires the sender to keep transmitting the coded packets until receiving the ACKs from them. However, since the WiFi needs to sacrifice its overlapped subcarriers to communicate with ZigBee device, simply applying prior approach will reduce the WiFi throughput. As shown in Figure 3, assume each ZigBee node requires 3 coded packets to decode the ZigBee data. Therefore, the WiFi AP should deliver 3 coded packets during each ZigBee node's active state. The total number of hybrid packets transmitted from the WiFi AP is 9 while the WiFi device $W1$ only receives 9 short packets, which reduces the throughput from the WiFi AP to $W1$. Furthermore, since the transmission power is dynamically changing according to the current WiFi traffic, the AP cannot guarantee that enough coded packets are transmitted to each ZigBee node.

To address this issue, Waves introduces a distributed fountain codes transmission technique, which only requires the WiFi AP to dynamically transmit coded ZigBee packets to a limited number of ZigBee nodes and does not require a specific ZigBee node to receive coded packets. When transmitting enough packets to the ZigBee network, the WiFi AP can terminate the data dissemination. We give an example in Figure 4. Assume the ZigBee nodes need to receive 3 coded packets to perform decoding. However, due to the current WiFi traffic status, the WiFi AP can only transmit 2 coded packets to $Z1$ and $Z3$ during their active states, respectively. In this example, $Z1$ receives packet 1 and 2 while $Z3$ receives packet 2 and 3. Since there are already **four** coded packets in the network, the WiFi AP can stop transmitting the hybrid packets and transmit pure WiFi packets to $W1$. The ZigBee nodes can exchange the received packets in the ZigBee network when they do not interfere with the WiFi traffic. In this example, the WiFi AP only transmits 4 hybrid packets and the remaining 5 packets are pure WiFi packets. **In summary**, *Waves can conduct reliable data dissemination and reduce the influence on the ongoing WiFi traffic*.

III. Detailed Protocol of Waves

The design of Waves mainly consists of three steps.

1. **Cross-technology Sensing and Transmission Power Optimization:** The WiFi devices sense the channel to learn the working schedules of ZigBee nodes. Then, according to the WiFi traffic, the WiFi AP controls its transmission power to conduct transmissions to WiFi devices and ZigBee nodes simultaneously.

2. **ZigBee Data Dissemination:** To improve the data dissemination reliability and reduce the network overhead, the data disseminated to the ZigBee device is encoded by using the Distributed Fountain Codes Transmission technique. The WiFi AP will terminate the dissemination immediately when transmitting enough coded packets to the ZigBee network.

3. **Packets Exchange in ZigBee Network**: To cover the whole network and improve the data dissemination reliability, a ZigBee node can exchange the received packets to its neighboring nodes. To reduce the number of redundant transmissions, each ZigBee node leverages the network coding technique to improve the packet exchange efficiency.

A. Cross-Technology Sensing and Transmission Power Optimization

1) Cross-Technology Sensing: In CTC networks, ZigBee nodes cannot directly inform their working schedules to the WiFi AP due to the huge communication overhead introduced by uplink CTC (i.e., ZigBee to WiFi). To overcome this challenge, we introduce a cross-technology sensing approach to passively sense the working schedules of ZigBee nodes. This approach is based on the fact that the WiFi device can distinguish transmissions from different ZigBee devices by

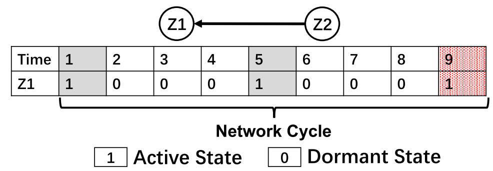


Fig. 5. The WiFi senses the traffic among ZigBee nodes.

detecting Received Signal Strength (RSS) values even under high interference [16]. In Waves, since a ZigBee node only receives the packets in the active state, the WiFi can sense the transmissions and records the corresponding durations of RSS values. This duration is the active state of the ZigBee node. We note that since multiple devices (i.e., Bluetooth, Baby Monitor, etc) work on the same overlapped channel, the WiFi device may mistakenly record the wrong device. Fortunately, the ZigBee nodes normally have a fixed packet size based on smart applications, which will result in a fixed RSS duration [17]. By checking the RSS duration, the WiFi AP can distinguish the ZigBee packets and know their corresponding applications.

When successfully sensing the ZigBee transmissions, the WiFi does not need to know which ZigBee node is active. It only needs to record the time information. By repeating this procedure, the recorded time will start to cycle, which is defined as the **Network Cycle**. Therefore, the WiFi AP only needs to conduct WiFi-to-ZigBee transmission during the active states in the network cycle. As shown in Figure 5 at times 1 and 5, $Z2$ transmits packets to $Z1$ during $Z1$'s active state. The WiFi device can sense and record the ZigBee traffic and transmits the time and RSS duration to the WiFi AP. For the WiFi AP, it finds out that every four time slots, a ZigBee node will switch to the active state. Then, the WiFi AP can broadcast the ZigBee packets at time slot 9.

2) Transmission Power Optimization: The objective of transmission power optimization is to conduct communications to the WiFi destination and ZigBee devices at different locations. Since the ZigBee data is embedded within the WiFi traffic, the throughput of the WiFi network should be as high as possible to conduct fast WiFi-to-ZigBee data dissemination. Traditionally, the minimal transmission power $P_{i,min}$ of the WiFi AP to the WiFi device i is determined as:

$$P_{i,min} = PathLoss + P_{threshold} + M_{threshold} \tag{1}$$

where $P_{threshold}$ is the minimum threshold that a packet can be detected by the WiFi client while $M_{threshold}$ is the threshold to prevent packet loss. However, this solution is based on WiFi to WiFi communication. In CTC networks, since the interference generated by ZigBee devices will also affect the WiFi throughput, we need to take ZigBee devices into consideration.

Formally, we denote the interference generated by WiFi and ZigBee devices in the CTC network as $\gamma_i(w)$ and $\gamma_i(z)$, respectively. Then, the SINR ϕ_i for the WiFi AP to a WiFi device i can be calculated as:

$$\phi_i = \frac{P_i g_i}{\gamma_i(w) + \gamma_i(z) + N_0} \tag{2}$$

TABLE I
AN EXAMPLE OF THE WIFI AP THROUGHPUT STEP FUNCTION

ϕ_i (dB)	5	6	7	9	13	17	20	22
$f(x)$ $(Mbps)$	6	9	12	18	24	36	48	54

where P_i is the transmission power from WiFi AP to WiFi device i and g_i is the channel gain. N_0 is the noise at i. Then, the maximum throughput r_i from WiFi AP to the device i can be estimated as $r_i = \psi_i f(10log(\phi_i))$, where ψ_i is the fraction of time for WiFi device i acquiring the wireless channel and $f(10log(\phi_i))$ is the step function of the throughput with different SINR value for a specific WiFi AP (e.g., the step function for CISCO Aironet 1520 is shown in table I [18].) Since it has been shown that the channel access for CSMA protocols are inherently fair [19], [20], assume the time duration of the active state for ZigBee node j is τ_j, then ψ_i can be estimated as:

$$\psi_i \approx \frac{T_c - \sum_0^{n_z} \tau_j}{n_w T_c} + \frac{\sum_0^{n_z} \tau_j}{(n_w + n_z)T_c} \quad (3)$$

where T_c is the time duration of the network cycle and n_w is the number of WiFi devices. n_z is the number of ZigBee nodes in the current coverage range of the WiFi AP. Therefore, the first term of this equation represents the fraction of time for the WiFi devices to acquire the wireless channel, while the second term represents the fraction of time for the ZigBee devices to acquire the wireless channel. Finally, the throughput of the WiFi network r_w can be represented as:

$$r_w = \sum_i^{n_w} \psi_i f(10log(\phi_i)) \quad (4)$$

As shown in Equation 4, when the transmission power of the WiFi AP is increased, the second term increases. However, since the increase of the transmission power will cover more ZigBee devices (n_z), the first term ψ_i is reduced. Since we cannot predict the WiFi traffic, it is difficult to find the global optimal solution. In Waves, the WiFi AP can try every value larger than $P_{i,min}$ in the predefined step function $f(10log(\phi_i))$ that can achieve highest r_w. This transmission power $P_{i,opt}$ is the local optimal solution, which preserves the WiFi throughput and reduces the ZigBee data dissemination delay at the same time.

We need to mention that the entire transmission power optimization scheme is efficient and fast. Specifically, due to the limitation of the hardware, in practice, the transmission power of WiFi AP is selected from a very small search space. As shown in table I, the CISCO Aironet 1520 has 8 possible values that can be selected by the WiFi AP. Therefore, instead of conducting the selection in a large space, our optimization scheme only needs to try several discrete values to find the optimal solution, which improves the searching efficiency. Moreover, since the transmission power is changed at the hardware layer, the changing process is extremely fast. According to our experiment, the entire optimization process can be done within 1 second.

We also need to mention that the above optimization scheme mainly focuses on the fixed ZigBee working schedule and

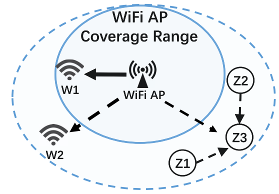


Fig. 6. 1) $Z1$ and $Z2$ can transmit coded packets to $Z3$ when not interfered by the WiFi AP. 2) When the WiFi AP communicates with W2, it simultaneously transmits coded packets to $Z3$.

WiFi modulation scheme. In practice, the ZigBee nodes can change working schedules according to their applications, which may result in the change of network cycle T_c. In addition, since the WiFi transmission power can dynamically change, the WiFi device may suffer a performance drop (e.g., using BPSK or QPSK instead of using 64-QAM) when the transmission power is reduced. In Waves, to maintain the power optimization performance, the WiFi device should conduct cross-technology sensing and update the network cycle (T_c) periodically. Moreover, it is also important to make sure that the minimum threshold $P_{i,min}$ in Equation 1 is determined based on the current modulation scheme.

B. ZigBee Data Dissemination

1) Preliminaries: Fountain codes are widely utilized to achieve reliable communication [21]. Assume there are multiple packets waiting for transmission. The sender will generate an *infinite* number of encoded packets using an XOR process and keep transmitting these coded packets to the receiver. The receiver can decode the original packets by solving linear equations after receiving enough coded packets.

In Waves, we use Luby Transform codes (LT codes) [22] as a specific realization of Fountain codes, which requires low computational resources and can be applied to ZigBee nodes. Traditional approaches require every receiver to receive a sufficient number of coded packets and transmit ACKs back to the sender for transmission termination [15], [23], which cannot be applied to the CTC network. This is because the WiFi device uses 7 overlapped subcarriers to communicate with a ZigBee node, thus transmitting coded packets to all the nodes will significantly reduce the WiFi throughput. To overcome this challenge, we develop a distributed fountain codes transmission technique to improve the data dissemination reliability and preserve the WiFi throughput at the same time.

2) Distributed Fountain Codes Transmission: Intuitively, the WiFi AP should transmit as many coded packets to the ZigBee nodes as possible. However, this solution reduces the throughput of the WiFi network while having little improvements on the data dissemination reliability. As shown in Figure 6, according to the WiFi traffic, after transmitting coded packets to $Z1$ and $Z2$, the WiFi AP starts to communicate with $W1$. Since $Z1$ and $Z2$ are not interfered by the WiFi AP, they can forward coded packets to $Z3$. However, due to the lack of feedbacks from ZigBee nodes, when the WiFi AP is communicating with $W2$, it transmits coded packets to $Z3$ again, which introduces redundant transmissions. Moreover, even if $Z1$ and $Z2$ do not receive enough coded packets, $Z3$ may

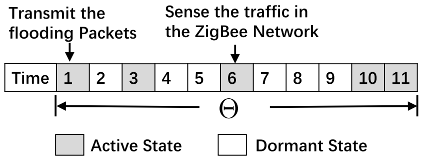


Fig. 7. The WiFi AP broadcasts coded packets at time 1. Then, the WiFi device senses the ongoing ZigBee traffic at time 6.

still successfully decode the coded packets by combining the received packets from $Z1$ and $Z2$ together. Therefore, simply transmitting the coded packets to all the ZigBee nodes neither reduces the data dissemination delay nor improves the data dissemination reliability.

In Waves, the WiFi AP treats the entire ZigBee network as a single ZigBee node with dynamic working schedules. Since the packets are transmitted directly through WiFi, Waves does not care about the topologies of the ZigBee network and receiving status of some specific ZigBee nodes. The data dissemination reliability is unaffected as long as the ZigBee network receives enough packets. Specifically, the WiFi AP will transmit the coded packets according to the active states in the network cycle. The selections of the active state are mainly based on two factors: *i) the time duration of the current WiFi traffic; and ii) the traffic in the ZigBee network.* Formally, for a ZigBee network with N ZigBee nodes, we denote the complete set of the active states during the network cycle as Θ. The active states that receive the coded packets are defined as the **Selected States**.

Based on the WiFi traffic, the WiFi AP can broadcast the coded packets at the time of the nearest active state in the network cycle. Then, this active state will be deleted from the set Θ. Since the WiFi traffic is dynamically changing, the corresponding coverage range of the WiFi AP is also changing. Therefore, for the ZigBee nodes that receive the coded packets, it can transmit the received packets to their neighboring nodes when they are not covered by the WiFi AP. To further reduce the redundant transmissions, WiFi devices will sense the transmissions in the ZigBee network. When ZigBee nodes are forwarding the received packets during its neighboring nodes' active states, these active states in the set Θ will also be deleted, which is shown in Figure 7. This process will continue until all the active states in the set Θ are deleted.

3) Termination of Data Dissemination: In general, the WiFi AP should terminate the data dissemination when Θ is empty. However, due to the unreliable links between WiFi and ZigBee, the ZigBee network may still not receive a sufficient number of coded packets. On the other hand, if the entire network has already received enough packets, the WiFi can conduct early termination to preserve the WiFi throughput. In Waves, the WiFi AP will count the number of transmitted coded packets. If the total number of transmitted packets from the WiFi AP to the ZigBee network does not reach the minimal requirements P_T^{min}, the WiFi AP will continue to transmit the coded packets during the active states in the next network cycle until this lower bound is reached. Otherwise, the WiFi AP can conduct early termination.

Formally, for a number of K coded packets, the corresponding degree distribution can be represented as $P(d)$. The degree of a coded packet k_j is represented as d_j. The link quality between the WiFi AP and the ZigBee node i is denoted as p_i^w. Assume a number of m packets have been transmitted to the ZigBee node i during its active state. Therefore, the probability $p_r^i(k)$ for a packet to be a redundant coded packet is:

$$p_r^i(d') = \sum_{l=d'}^{d'+\lfloor mp_i^w \rfloor - x} \left(P(l)\frac{\binom{x}{l}\binom{\lfloor mp_i^w \rfloor - x}{l-d'}}{\binom{\lfloor mp_i^w \rfloor}{l}}\right) \tag{5}$$

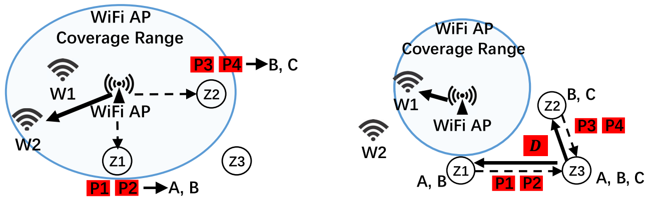
where d' is the reduced degree, x is the number of undecoded packets, and ρ is the termination threshold. In other words, when $p_r^i(d') > \rho$, the WiFi AP should stop the transmission. Therefore, the minimum number of transmitted packets P_T^{min} from the WiFi AP to the ZigBee network should satisfy $\operatorname{argmin}_{P_T^{min}} \sum_{i=1}^{P_T^{min}} (\frac{p_r^i(\rho_i)}{P_T^{min}}) > \rho$. When the number of transmitted packets reaches P_T^{min}, the WiFi AP can terminate the transmission. The determination of ρ is tricky. When ρ increases, the data dissemination reliability will be high and the delay will be low. However, it requires the WiFi AP to transmit a higher number of coded packets to the ZigBee network, which sacrifices the WiFi network throughput. Therefore, in practice, the value of ρ should be determined based on the users' applications. Since the WiFi AP does not care which ZigBee node has received the coded packets, ρ does not need to be precisely defined. As long as the whole network receivers enough packets, the data dissemination reliability remains unaffected.

As discussed above, Waves does not require ZigBee nodes to transmit acknowledgments back to the WiFi AP, which avoids the limitations of the packet-level ZigBee-to-WiFi CTC (discussed in section III-B.2) and significantly reduces the network overhead. After transmitting coded packets to the ZigBee network, the WiFi AP can sense the ZigBee traffic instead of communicating with the WiFi client immediately. We are aware that in some cases, the WiFi AP may need to communicate with the WiFi client immediately due to the importance of the WiFi traffic. As a result, the WiFi AP cannot sense the ZigBee traffic from some specific ZigBee nodes. However, we argue that Waves can work properly even in this scenario. This is because Waves only considers the total number of code packets transmitted to the ZigBee network. Therefore, the WiFi AP can always adjust the transmission threshold P_T^{min} to determine when to terminate the transmission.

C. Packets Exchange in the ZigBee Network

To cover the whole network and further improve the data dissemination reliability, when receiving the coded packets from the WiFi AP, ZigBee nodes should decode and transmit these packets to its neighboring nodes. Since the neighboring nodes may have already received some of the coded packets from the WiFi AP or other nodes, we use network coding to reduce the number of redundant transmissions.

For a node i, if the received data is successfully decoded, it will create random linear combinations of the received packets and then transmit them to its neighboring nodes. Formally, we represent a number of K successfully decoded packets



(a) $Z1$ and $Z2$ receive insufficient number of coded packets from WiFi AP. Each node can only decode two packets.

(b) $Z3$ have received enough packets and can decode A, B and C. Then, it can broadcast one coded packet D to $Z1$ and $Z2$.

Fig. 8. An example of packet exchange in the ZigBee network. Assume each node has to at least receive 3 coded packets (e.g., any 3 packets from P1, P2, P3, and P4) to decode original packets A, B, and C.

as $\{A_1, A_2, \ldots, A_K\}$. Then, these packets will be combined together by multiplying a matrix with random values, which is shown as follows:

$$\begin{bmatrix} C_1 \\ \vdots \\ C_K \end{bmatrix} = \begin{bmatrix} a_1 & \cdots & a_K \\ \vdots & \ddots & \vdots \\ k_1 & \cdots & k_K \end{bmatrix} \begin{bmatrix} A_1 \\ \vdots \\ A_K \end{bmatrix} \tag{6}$$

The node i will keep transmitting the combined packets from C_1 to C_K until receiving acknowledgments from its neighboring nodes. If node i cannot decode the information, it will request the coded packets from its neighboring nodes. As described in section III-B.2, even if all its neighboring nodes do not receive enough packets from the WiFi AP, the node i can still decode the information after receiving enough coded packets from its neighboring nodes. In this case, the data dissemination reliability remains unaffected. Moreover, by comparing the packets received from its neighboring nodes, the node i can transmit the missing packets to these nodes during their active states.

If the node i's neighboring nodes have the same working schedule, rather than simply broadcasting the missing packets, the node i can apply the network coding to further reduce the number of redundant transmissions. As shown in Figure 8, assume each ZigBee node requires to receive 3 packets to decode the information. In Figure 8(a), $Z1$ and $Z2$ only receive two coded packets. In Figure 8(b), they transmit the received coded packets to $Z3$. Now, since $Z3$ receives enough packets, it can decode the received packets. Then, based on the transmitted packets from A and B, $Z3$ knows the missing packets of $Z1$ and $Z2$ are C and A, respectively. Then, instead of simply transmitting the missing packets to $Z1$ and $Z2$, $Z3$ only broadcasts the combined packets D, where D can be represented as $D = \alpha_1 A + \alpha_2 C$. α_1 and α_2 are two random values that are indicated in the packet header. By leveraging this approach, Waves can improve the data dissemination reliability with lower number of redundant transmissions.

We need to mention that the reliability of the packet exchange process can be affected by the wireless environment. For example, it is possible that $Z1$ or $Z2$ did not receive the coded packet D from ZigBee node $Z3$ in Figure 8 (b). In this case, $Z3$ has to conduct retransmission to ensure the packet exchange reliability, which may increase the network overhead.

IV. Advanced Waves

Although the WiFi device can emulate a ZigBee signal without any hardware modifications, in a real-world scenario, the emulated signal is still not the same as the legitimate ZigBee signal. In the worst scenario, even if we can leverage the DFCT to enable reliable communication between WiFi and ZigBee, the data dissemination reliability is still not guaranteed. In this section, we will dig into details about this challenge and introduce a potential solution to further improve the data dissemination reliability.

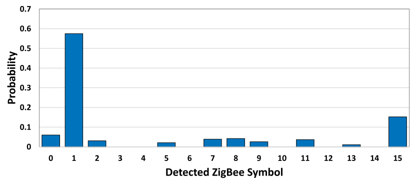
A. Analysis of the WiFi-to-ZigBee CTC Technique

Normally, to generate an emulated ZigBee signal, the WiFi device controls its payload so that the transmitted RF signal is similar to the ZigBee signal. However, as shown in Figure 10, due to the limitation of the 802.11 physical layer, the emulated signal is not exactly the same as the desired ZigBee signal for the following reasons: *First,* according to the ZigBee signal, the WiFi device should select the nearest corresponding QAM constellation point. The Minimum Euclidean Distance between the selected QAM point and the desired point is the distortion introduced during the signal emulation process. *Second,* the WiFi uses the Cyclic prefix (CP) to eliminate the Inter-Symbol Interference (ISI) and the Inter-Carrier Interference (ICI) while the ZigBee signal does not have cyclic prefix, which introduces imperfect emulation. *Third,* the duration of one WiFi symbol is $4\mu s$ while the duration of one ZigBee symbol is $16\mu s$. Therefore, WiFi needs to use 4 symbols to emulate one ZigBee symbol. The discontinuity between each WiFi symbol also introduces imperfection.

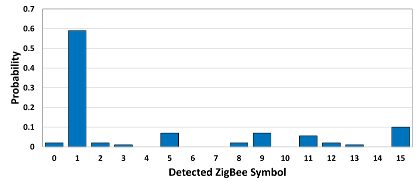
For the ZigBee device, it uses a 32 Pseudo-random Noise Chip Sequence (PN Sequence) to express a 4-bit symbol for chip error tolerance, which is also known as the Direct Spreading Spectrum Sequence (DSSS). In practice, although hardware defects, multipath effects and the imperfect wireless environments (i.e., noise, interference etc.) introduce distortions to ZigBee signals, as long as the number of chip errors is lower than the threshold, the ZigBee receiver can get the correct PN sequence. However, the imperfect emulation is introduced in the WiFi to ZigBee CTC, which makes it challenging for the ZigBee device to detect and receive the desired PN sequence.

B. Observation of the Imperfect Emulation

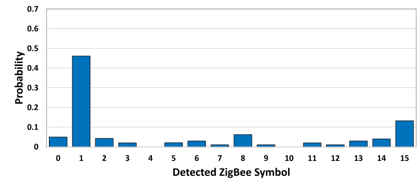
To prove our analysis in the above section, we implement the WiFi part on a USRP B210 to support WiFi to ZigBee communication. The WiFi is set to emulate and transmit all 16 ZigBee PN sequences and each transmission is repeated for 1×10^4 times in both outdoor and indoor scenarios. Since these experiments show similar trends, we show the results of the detected PN sequences by the ZigBee device when the WiFi is emulating ZigBee PN sequence 1. As shown in Figure 9(a), around 58% of decoded PN sequences are recognized as the ZigBee PN sequence 1. However, we also can observe that the remaining emulated ZigBee signals are detected as ZigBee PN sequence 0, 2, 5, 7, 8, 9, 11, 13, and



(a) The detected ZigBee symbol distribution (outdoor location 1).



(b) The detected ZigBee symbol distribution (outdoor location 2).



(c) The detected ZigBee symbol distribution (indoor location 1).

Fig. 9. When the WiFi device is broadcasting the same emulated ZigBee symbol 1 (ZigBee PN sequence 1), the distribution of the detected ZigBee symbols changes according to the locations of the ZigBee receiver.

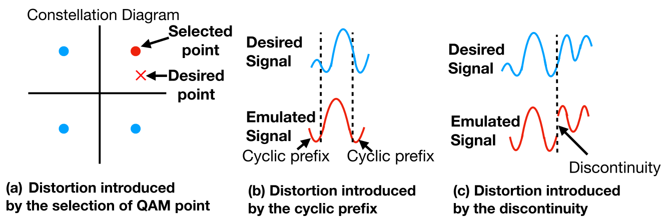


Fig. 10. The distortions introduced during the emulation process.

15 with different probabilities. We also need to mention that around 3% emulated ZigBee signals cannot be recognized by the ZigBee receiver during our experiments. Moreover, we also can observe that the received PN sequences vary across different environments. As shown in Figure 9(c), around 47% emulated ZigBee signals are detected by the ZigBee receiver as PN sequence 1 while the remaining emulated ZigBee signal are recognized as 0, 2, 3, 5, 6, 7, 8, 9, 11,12, 13,14 and 15.

Moreover, we also study the distribution of the detected ZigBee symbol in the same scenario. As we can see from Figure 9(a) and Figure 9(b), the distribution of the detected ZigBee symbols varies according to the location of the devices. Specifically, although DSSS is efficient in tolerating potential wireless communication errors, it is not designed for cross-technology communication. In CTC, since the emulated signal cannot perfectly match the desired ZigBee signal, the slight change in the wireless environment will affect the final detection results. In this experiment, the ZigBee receiver in Figure 9(a) is around 3 meters from the WiFi device, while the ZigBee receiver in Figure 9(b) is 10 meters from the WiFi device. As a result, the distributions of the detected ZigBee symbol are different. The above experiments prove our analysis of the imperfect emulation. In our design, although fountain codes can correct some errors, the errors introduced by the imperfect emulation will still significantly reduce the data dissemination reliability. Therefore, we need to design an advanced approach to further improve the reliability of Waves.

C. ZigBee Symbol Compensation

In Waves, to effectively leverage the DFCT technique, we introduce a ZigBee symbol compensation scheme during the data dissemination process. Specifically, the WiFi device will send the predefined symbol sequences to ZigBee device before transmitting the actual data. The predefined symbol sequences are known by both WiFi and ZigBee devices. The ZigBee receiver will check which emulated symbol cannot be recognized. Then, it will transmit the actual received symbols back to the WiFi device. At last, the WiFi device can use different payloads to emulate the corresponding ZigBee symbol. For example, assume PN sequences PN_1 and PN_2 are emulated by the WiFi combinations $S_1S_2S_3S_4$ and $S_5S_6S_7S_8$, respectively. After receiving the actual received symbols from the ZigBee receiver, the WiFi device finds out that the corresponding emulated signal PN_1 cannot be recognized while PN_2 can be correctly detected by the ZigBee receiver. In this case, the WiFi device may use n consecutive combinations $S_5S_6S_7S_8$ to represent PN_1 for reliable communication. For the ZigBee device, once it receives n consecutive PN sequences PN_1, it will consider these sequences as PN_1.

We also note that the wireless environment is dynamically changing. Therefore, the distribution of the detected ZigBee symbols may also change over time. In this case, using a fixed communication compensation scheme may be insufficient to enable reliable data dissemination. To overcome this challenge, the WiFi device should actively sense the traffic in the ZigBee network during the packet exchange process. If there is a huge amount of ongoing traffic in the ZigBee network, it is highly possible that ZigBee nodes cannot detect some specific emulated ZigBee symbols. In this case, the WiFi device should retransmit the predefined symbol sequences to update the communication compensation symbols.

V. Implementation & Evaluation

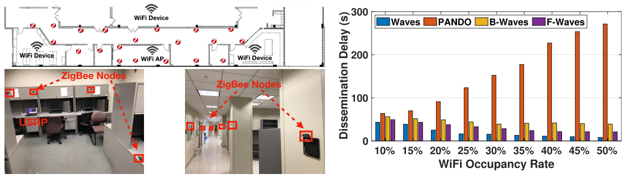
A. Experiment Setup

We evaluate Waves under various network settings in smart office and smart home scenarios. We use the existing open source 802.11g [24], [25] to implement the WiFi AP part of Waves on a USRP B210 [26] device. Three additional USRPs are used as WiFi devices to communicate with the WiFi AP. The transmission power of the WiFi AP varies between $1dBm$, $10dBm$, and $20dBm$ according to the distances from the WiFi AP to the WiFi devices. Since the WiFi data will not affect the WiFi to ZigBee communication, we use a stream of '0' as the WiFi traffic. We use Contiki to implement Waves on 20 off-the-shelf ZigBee compliant TelosB nodes. The duty cycles of ZigBee nodes are set as 10%. The termination threshold ρ is set to 0.8.

Since this is the first work of utilizing the WiFi AP to conduct data dissemination for ZigBee nodes in heterogeneous IoT networks, we can only compare the performance of Waves with the latest data dissemination approach in ZigBee

TABLE II
COMPARISON BETWEEN STATE-OF-THE-ART SOLUTIONS

	CTC	Fountains codes	ACKs	Network Coding
PANDO	×	✓	×	×
B-Waves	✓	×	×	×
F-Waves	✓	✓	×	×



(a) (b)

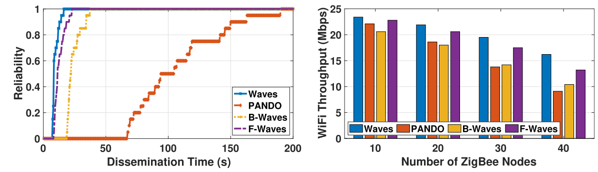
Fig. 11. (a) Smart office scenario. (b) Dissemination delay.

networks PANDO [15] as our baseline. To further show the benefits of our design and conduct fair evaluations, we also implement **Basic Waves (B-Waves)** and **Fountain Waves (F-Waves)**. The comparison between these solutions are listed in table II. Specifically, B-Waves does not apply any coding techniques nor require the ZigBee nodes to transmit ACKs back to the WiFi AP. The main purpose of implementing B-Waves is to understand the disadvantages of physical-level CTC and show the effectiveness of our coding techniques. F-Waves is the advanced version of B-Waves. It utilizes fountain codes to conduct transmissions from WiFi to ZigBee and does not require ACKs from the ZigBee devices. The reason why we implement F-Waves is to show the effectiveness of Waves during the packet exchange process in the ZigBee network.

B. Smart Office Experiments

The smart office scenario mainly contains indoor experiments with relatively high interference [in Figure 11(a)]. We first evaluate the average data dissemination delay under different WiFi occupancy rates in Figure 11(b). All approaches show relatively low data dissemination delay when the WiFi occupancy rate is as low as 10%. However, with the increase in the WiFi traffic, the delay of Waves decreases quickly while the delay of PANDO increases rapidly. When the WiFi occupancy rate reaches 50%, the average delay of Waves is $8.1s$, which is around ***33.5 times*** faster than that of PANDO ($271.3s$). This is because Waves can leverage the ongoing WiFi traffic to conduct WiFi-to-ZigBee communication while PANDO suffers high interference from the WiFi traffic. The performance of Waves is around 4.5 times better than that of B-Waves. This is because Waves utilizes distributed fountain codes transmissions to improve the data dissemination reliability and the packet exchange process of Waves is faster than other approaches. The performance of F-Waves is around 2.4 times worse than that of Waves. This is because the packet exchange processes of F-Waves is inefficient, which reduces the overall data dissemination delay.

Figure 12(a) shows the reliability progress when the WiFi occupancy rate is 35%. For Waves, more than 80% of the ZigBee nodes finish the data dissemination within $20s$ and



(a) (b)

Fig. 12. (a) Dissemination reliability. (b) The WiFi throughput.

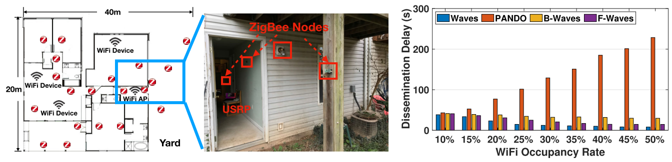
the average delay is around $23s$. For B-Waves and F-Waves, the average delays are around $43s$ and $25s$, respectively. This is because the WiFi AP in Waves can change its transmission power to reach the ZigBee nodes at different distances, which avoids the delay introduced by multi-hop transmissions. In contrast, PANDO is struggling to conduct data dissemination in the first $70s$. This is because PANDO is not designed for CTC networks. It treats the WiFi traffic as interference. Therefore, due to the high WiFi occupancy rate, it is difficult for the sender to perform data dissemination. Moreover, the silence feedback scheme in PANDO only works under low CTI, which further reduces the network performance. As packets reach the ZigBee nodes that far from the WiFi AP, it is less possible that the transmissions are interfered by the WiFi traffic. As a result, the average delay of PANDO is $185s$, which is around ***9 times*** slower than Waves.

Figure 12(b) shows the impact on WiFi throughput under different network densities. The WiFi throughput of Waves remains the highest among the state-of-the-art solutions. When the number of ZigBee nodes reaches 40, the throughput of Waves is 1.81***,*** 1.67 ***and*** 1.22 ***times*** better than that of PANDO, B-Waves and F-Waves, respectively. This is because the WiFi-to-ZigBee communication and packet exchange process in Waves are much more efficient than those of the state-of-the-art solutions. For PANDO, the WiFi must frequently back off according to the CSMA scheme. Since B-Waves sacrifices part of the WiFi subcarriers for CTC while the communication reliability is still low, the performance of B-Waves is the worst.

C. Smart Home Experiments

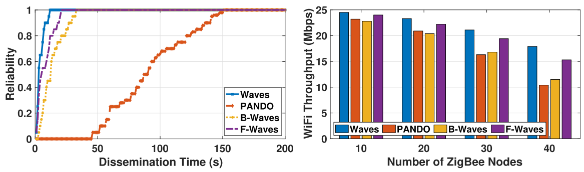
The smart home scenario contains both indoor and outdoor experiments [in Figure 13(a)]. Specifically, the WiFi AP is deployed inside the home while the ZigBee nodes are deployed both inside and outside the smart home. As shown in Figure 13(b), the average delay of Waves is much than that of PANDO, B-Waves and F-Waves. When the WiFi occupancy rate is 10%, the delay of Waves is slightly better than PANDO, B-Waves and F-Waves. As the WiFi traffic increases to 50%, the average delay of Waves is around 27.5***,*** 3.5 ***and*** 1.74 ***times*** better than that of PANDO, B-Waves and F-Waves, respectively.

As shown in Figure 14(a), the data dissemination process of Waves shows the advantage of our design. 80% of the ZigBee nodes still receive the packets within $20s$. The dissemination processes of PANDO, B-Waves and F-Waves are smoother when compared to Figure 12(a). This is because the interference in smart home is lower than that of the smart office scenario. For PANDO, it can transmit coded fountain



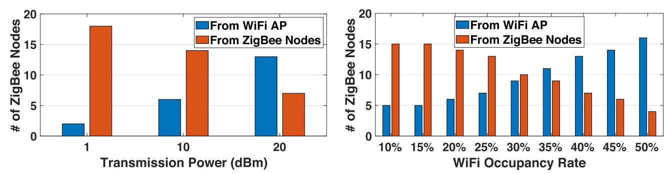
(a) (b)

Fig. 13. (a) Smart home scenario. (b) Dissemination delay.



(a) (b)

Fig. 14. (a) Dissemination reliability. (b) The WiFi throughput.



(a) (b)

Fig. 15. (a) Contribution of the WiFi AP vs. WiFi AP transmission power. (b) Contribution of the WiFi AP vs. WiFi traffic.

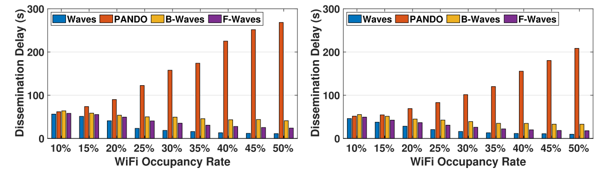
codes and terminate transmissions easier. For B-Waves and F-Waves, they also can easily exchange the received packets in this scenario. Figure 14(b) shows the WiFi throughput in the smart home scenario. Similar to the Smart Office scenario, the performance of Waves is much better than that of other solutions. As the number of ZigBee nodes reaches 40, the performance of Waves is around 1.72, 1.55 and 1.16 times better than PANDO, B-Waves and F-Waves, respectively.

D. System Insight Analysis

In this section, we explain why Waves has better performance by revealing some system insights. Since the smart office and smart home scenarios have the same trend, we only show the evaluation results in the smart home scenario.

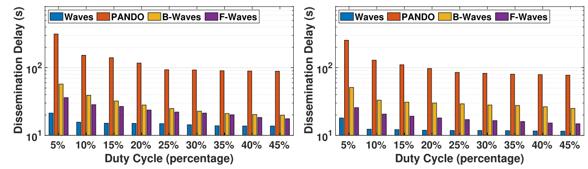
Figure 15(a) depicts the number of ZigBee nodes that receive the coded packets from the WiFi AP directly under different transmission power constraints. When the transmission power is set to $1dBm$, only a small number of ZigBee nodes can receive packets from the WiFi AP directly and most of the data dissemination packets are exchanged through the ZigBee network. As transmission power increases, the data dissemination packets can be directly transmitted to a larger number of ZigBee nodes. ***Insight:*** *Waves can leverage the WiFi AP adaptive power control to reach the nodes that are far from the WiFi AP, which reduces the delay introduced by multi-hop transmissions.*

Figure 15(b) shows the number of ZigBee nodes that directly receive the packets from the WiFi AP under different WiFi occupancy rates. When the WiFi occupancy rate is 10%, only a small number of ZigBee devices receive packets directly from the WiFi AP. This is because the interference from the



(a) (b)

Fig. 16. (a) Dissemination delay (Smart Office). (b) Dissemination delay (Smart Home).



(a) (b)

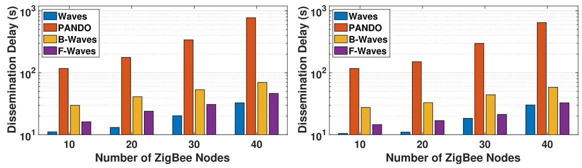
Fig. 17. (a) Dissemination delay (Smart Office). (b) Dissemination delay (Smart Home).

WiFi traffic is low and has little impact on the ZigBee network. When the WiFi Occupancy rate reaches 50%, a larger number of ZigBee nodes have to frequently back off. In this case, the WiFi AP directly performs data dissemination to these nodes to reduce the data dissemination delay. ***Insight:*** *Waves can dynamically change the transmissions from WiFi AP to the ZigBee nodes to reduce the average delay.*

E. System Sensitivity Analysis

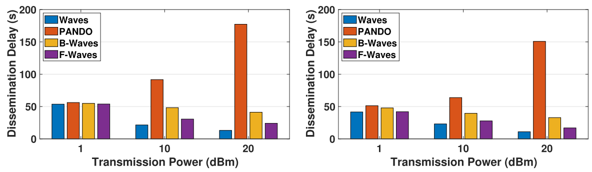
1) Mobility: Figure 16(a) and 16(b) shows the average delay when WiFi devices are moving at $1m/sec$. To achieve the desired speed accurately, we implement the WiFi device on a DJI robot master platform [27]. As we can see from these figures, Waves still shows the best performance while PANDO performs better under the mobility scenario when the WiFi occupancy rate is low. This is because the CTI is lower as WiFi devices move away, which enables the transmissions in the ZigBee network. On the contrary, B-Waves performs worst when the WiFi occupancy rate is 10%. This is because B-Waves cannot conduct reliable WiFi to ZigBee communication. It requires ZigBee nodes to frequently exchange the received packets in the ZigBee network, which increases the data dissemination delay.

2) Duty Cycles: The average data dissemination delay under different ZigBee duty cycles are shown in Figure 17(a) and 17(b). Waves shows great advantages under different duty cycles. When the duty cycle is as low as 5%, the average delay of Waves ($21.32s$ smart office and $18.03s$ smart home) is around ***14.1 times*** better than PANDO ($314.6s$ smart office and $254.1s$ smart home). This is because the transmissions in PANDO not only interfere with the WiFi traffic but suffer multihop transmission delays. As the duty cycle increases, the delay of PANDO reduces rapidly ($88.48s$ smart office and $25.01s$ smart home) while the performance of Waves almost remains the same ($13.72s$ smart office and $11.53s$ smart home). For B-Waves and F-Waves, due to the inefficiency of the packet exchange process, the average delays are around 2.60 ***times and*** 1.31 ***times*** worse than that of Waves.



(a) (b)

Fig. 18. (a) Dissemination delay (Smart Office). (b) Dissemination delay (Smart Home).



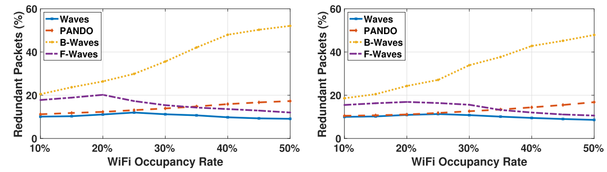
(a) (b)

Fig. 19. (a) Dissemination delay (Smart Office). (b) Dissemination delay (Smart Home).

3) Network Densities: Figure 18(a) and 18(b) shows the average delay under different network densities. During the experiment, the WiFi occupancy rate is set to 35%. As shown in these figures, the delays of Waves and PANDO increase at different speeds. This is because the data dissemination in PANDO is conducted by a single ZigBee source while multiple ZigBee nodes in Waves can exchange the received packets. The delays of B-Waves and F-Waves are also increasing faster than those of Waves due to the unreliability and redundancy introduced during the data dissemination process. When the number of ZigBee nodes reaches 40, the average delay of Waves is around 22***,*** 2.1***, and*** 1.4 ***times*** less than those of PANDO, B-Waves and F-Waves, respectively.

4) WiFi AP Transmission Power: Figure 19(a) and 19(b) shows the average delay under different WiFi AP power restrictions. When the transmission power is as low as $1dBm$, the WiFi AP only covers a small area. In this case, a limited number of ZigBee nodes can receive the packets from the WiFi AP. Meanwhile, only the ZigBee nodes that are close to the WiFi AP are affected by the WiFi traffic. Therefore, the average delays of Waves, PANDO, TwinBee, B-Waves and F-Waves are almost the same. As the transmission power increases, more ZigBee nodes can be reached by the WiFi AP and the corresponding delay reduces rapidly. However, since PANDO is not designed for high CTI, a large number of ZigBee nodes in PANDO are interfered with WiFi devices, which significantly hampers the data dissemination process.

5) Message Overhead: We study the message overhead in Figure 20(a) and 20(b). The smart office and smart home scenarios show the same trend. When the WiFi occupancy rate is 10%, the percentage of redundant packets introduced by PANDO and Waves are almost the same. B-Waves has the highest overhead, which is introduced by the ZigBee-to-WiFi ACKs and redundant packet exchange in the ZigBee network. Counterintuitively, the overhead of Waves and F-Waves are reduced as the WiFi occupancy rate reaches 50%. This is because most of the ZigBee nodes can receive the packets through the WiFi AP. Therefore, the overhead is mainly introduced by fountain codes. As a result, when the WiFi



(a) (b)

Fig. 20. (a) Percentage of redundant packets (Smart Office). (b) Percentage of redundant packets (Smart Home).

Occupancy rate reaches 50%, the performance of Waves is around 1.9, 5.6, and 1.3 times better than that of PANDO, B-Waves and F-Waves, respectively.

VI. Discussions

I. Impact of different WiFi standards. In Waves, although the WiFi device mainly utilizes 802.11g to perform CTC, the overall performance of WiFi devices will not be affected by other WiFi standards (i.e., 802.11e or 802.11n). This is because the CTC physical layer emulation techniques do not change the WiFi physical layer. It only requires the WiFi device to emulate the ZigBee signal by controlling the payload of a WiFi packet. Since the ZigBee device occupies a 2MHz band, only the overlapped 7 WiFi subcarriers are used to emulate the ZigBee signal. For the 802.11e, it mainly focuses on the MAC layer enhancement, which does not change the physical layer of the WiFi device. Therefore, the performance of Waves remains unaffected. For the 802.11n, it utilizes OFDM modulation to conduct communication, which is similar to 802.11g. The only difference is that the 802.11n applies OFDM on a 40MHz channel and the number of data-carrying subcarriers increases to 114. However, since the ZigBee device occupies a 2MHz band, the WiFi device still utilizes the same 7 subcarriers to conduct the WiFi to ZigBee communication. Therefore, the performance of Waves remains unaffected.

II. Impact of multiple WiFi APs. In Waves, although we mainly focus on the single WiFi AP network, the proposed scheme can be extended to the network with multiple WiFi APs. This is because we did not change the WiFi physical layer and MAC layer. For multiple WiFi APs, they can utilize the existing CSMA scheme to avoid the interference between each other. Moreover, for the ZigBee node that is currently out-of the coverage range of a single WiFi AP, the WiFi AP can transmit the data to its neighboring APs and ask those WiFi APs to conduct the data dissemination.

III. Impact of out-of-range ZigBee nodes. In Waves, the WiFi AP leverages the physical-level CTC to conduct data dissemination to the ZigBee network. To mitigate the interference and increase the coverage range, we introduce the WIDB scheme, which enables the WiFi device to effectively control its transmission power to reach the ZigBee nodes at different distances. In addition, the ZigBee nodes can also receive the coded packets from its neighboring nodes during the packet exchange process in the ZigBee network, which improves the data dissemination reliability.

IV. The data dissemination reliability. In this work, the WiFi device only needs to transmit a limited number of coded packets to the ZigBee network. The ZigBee nodes can exchange the received packets if they cannot decode the data. This approach can guarantee approximately 100% reliability in most cases. However, if the ZigBee nodes have aperiodic transmissions, the data dissemination reliability will be affected. This is because the cross-technology sensing scheme requires the WiFi device to understand the network cycle. If a ZigBee device is conducting aperiodic transmissions, the WiFi device will mistakenly consider a single ZigBee nodes as multiple nodes, which will result in broadcasting the data to the same ZigBee node multiple times. Moreover, without the accurate network cycle, the WiFi device cannot control its transmission power precisely, which reduces the data dissemination reliability. To overcome this challenge, the ZigBee node with aperiodic transmissions has to leverage packet-level CTC to inform the WiFi device of its working schedules. However, as mentioned in section III-A.1, this packet-level CTC will increase the network overhead.

V. The deployment of Waves. Waves only requires the software-level changes to be deployed to the WiFi and ZigBee coexistence networks. Specifically, the WiFi adaptive power control utilized in Waves is defined in the IEEE 802.11 standard while the physical-level CTC techniques only require the WiFi device to control its payload to support the WiFi-to-ZigBee communication. In Waves, we also utilize coding techniques to improve the data dissemination reliability and reduce the network overhead. However, these techniques do not require hardware modifications for WiFi and ZigBee devices, which reduces the deployment requirements for Waves.

VI. The impact of multiple ZigBee networks. Waves has the potential to support multiple ZigBee networks. Specifically, Waves does not change the Extended PAN ID (EPID) and PAN ID (PID) formats for ZigBee nodes. However, since Waves mainly focuses on the WiFi and ZigBee coexistence network, the EPID and PID should be selected by the WiFi AP. In addition, if there are multiple ZigBee networks, the WiFi AP should select different EPID and PID for different ZigBee networks. Similarly, when a new ZigBee node joins the network, it should send corresponding request to the WiFi AP (the controller) by using packet-level ZigBee-to-WiFi CTC. In this case, the corresponding request will introduce overhead to the network. However, we argue that this network overhead only appears when new nodes are trying to join the network, which can be ignored comparing to the traffic transmitted from WiFi to ZigBee network.

VII. The encryption of the hybrid packet. In Waves, the encryption of the hybrid packets will not affect the WiFi-to-ZigBee CTC. This is because the WiFi AP only needs to control its payload according to the desired ZigBee waveform. In other words, according to the encrypted ZigBee data, the WiFi AP can always change its payload to emulate the corresponding ZigBee waveform.

VIII. The overhead of hybrid packets. To enable WiFi-to-ZigBee CTC, the WiFi AP needs to use 4 WiFi-overlapped-ZigBee subcarriers to conduct the transmission. Since the WiFi has 52 subcarriers while 48 subcarriers can be used to transmit data (4 pilot subcarriers cannot be used to carry modulated data), the hybrid packets will, at most, reduce the WiFi throughput by around 8.3%. More importantly, in a real-world scenario, the affected WiFi throughput will be much smaller than 8.3%. This is because the max size of a ZigBee packet is 128 bytes while the max size of a WiFi packet is 2304 bytes. The number of hybrid packets transmitted from the WiFi AP is relatively small and can be ignored. Moreover, since the required data flow transmitted to the ZigBee device is normally smaller than that of the WiFi data flow, the WiFi AP does not need to change all the WiFi packets to hybrid packets. As a result, the performance of the WiFi network remains unaffected.

IX. The impact of the duty-cycle sensing accuracy. The WiFi AP should frequently conduct duty-cycle sensing as some ZigBee nodes may change their duty cycles. However, in practice, due to the change of the wireless environment, the WiFi AP may not be able to accurately sense the duty cycle of the network. In this scenario, the performance of Waves still remains the same. This is because Waves takes the entire ZigBee network into consideration. In other words, the WiFi AP only counts the number of coded packets transmitted to the entire ZigBee network. As a result, even if some specific ZigBee nodes' duty cycles cannot be accurately detected, as long as the entire ZigBee network receives enough packets, data dissemination reliability can be guaranteed.

VII. Potential Applications

Nowadays, more and more IoT devices have been deployed in smart homes and smart offices to support different applications, such as control of electrical loads, control heating, cooling, lighting, and human in the loop control for office automation, etc. These IoT devices are not only required to provide efficient and reliable services but also required to conduct fast responses according to the users' behaviors and dynamic requests [28], [29]. To provide a fast reaction to the users' behaviors, the server needs to continuously send out control signals to various IoT devices regardless of application scenarios and the communication distance [30], [31]. For example, in a smart home scenario, when a user comes back home, the server (WiFi AP) should send out control signals to the cooling units, lighting, TV, ventilation units, and other IoT devices to automatically adjust the environment to the user's most comfortable settings. In addition, the server also needs to continuously sending out the control signals to different IoT devices, when the user is moving from one room to another room. Similarly, in a large smart office, some ZigBee devices (e.g., smart lock, motion sensor, etc.) are normally deployed far from the server, while the server should also be able to reach these devices and control these devices with low delay. However, as the number of IoT devices increases, these IoT devices are suffering higher interference. According to CSMA, they need to frequently back off to avoid collisions, which introduces a huge delay to the network. Moreover, the communication from these IoT devices also interferes with the ongoing WiFi traffic, which affects the user experience. Waves can be applied to overcome the challenges. Specifically, instead of considering the WiFi-to-WiFi communication as noise and continuous conducting back-off, Waves leverages the WiFi traffic to conduct data dissemination for the ZigBee network. When there is an ongoing WiFi traffic, the corresponding ZigBee packet can be directly transmitted to ZigBee devices regardless of the communication distance. More importantly, as more and more data is transmitted through WiFi [32], Waves has the potential to satisfy the real-time management and control requirements for IoT devices in smart office and smart home applications.

VIII. Related Work

I. Cross-technology Communication has been proposed to support seamless, gateway-free communications among heterogeneous IoT radios [1], [2], [33]. Recently, researchers have developed several techniques to enable simultaneous communication among multiple heterogeneous IoT devices. EMF [9] is able to realize communication between ZigBee and WiFi simultaneously by shifting the packet transmission order. B^2W^2 [14] achieves N-way simultaneous communication between WiFi and Bluetooth devices. Since these approaches use packet level CTC, they can only achieve low throughput. The physical layer CTC technique WEBee [3] achieves high throughput communication from WiFi to ZigBee by using a small number of WiFi subcarriers (that are overlapped with ZigBee) to emulate ZigBee packets. PMC [4] demonstrates that the non-overlapped WiFi subcarriers can also be utilized to transmit traditional WiFi data. Therefore, a WiFi device can conduct parallel WiFi-to-WiFi and WiFi-to-ZigBee communications by using a single WiFi data stream. One of the most interesting projects is X-MIMO [34], which introduces a physical-layer design for WiF-to-ZigBee and ZigBee-to-WiFi CTC. Specifically, X-MIMO also utilizes physical-layer emulation technique to enable WiFi-to-ZigBee CTC. However, to achieve the ZigBee-to-WiFi CTC, X-MIMO leverages the CSI information measured by the WiFi AP to decode the ZigBee packets. To do this, the WiFi and ZigBee devices have to disable CSMA scheme in the network. Moreover, the ZigBee devices in X-MIMO have to conduct synchronization with the WiFi AP and WiFi clients to ensure the packets transmitted from the WiFi client and the packets transmitted from ZigBee devices are collided at the WiFi AP side. In a real-world scenario, since most of devices utilize CSMA to avoid collision and it is hard to conduct synchronization for a large number of devices, X-MIMO may not work for WiFi and ZigBee coexistence network. Different from the recent CTC techniques, we design Waves, which utilizes WiFi AP to initiate data dissemination for ZigBee nodes. By enabling simultaneous WiFi-to-WiFi and WiFi-to-ZigBee communication, Waves can significantly reduce the data dissemination delay. Moreover, since Waves does not require i) modifications to hardware, ii) disabling CSMA, and iii) strict synchronization among WiFi and ZigBee devices, it has the potential to be applied to commodity devices.

II. Data Dissemination has been applied to numerous networks and applications [35], [36], [37], [38]. Opportunistic Flooding [39] mainly utilizes delay distribution to reduce the delay and redundancy in low-duty-cycle wireless sensor networks. A wireless link-correlation feature [40] has also been widely investigated to conduct efficient data dissemination [41], [42], [43]. For example, Collective Flooding [42] and Correlated Flooding [43] explore the link correlation to reduce the redundant transmissions and reduce the dissemination delay. Constructive interference has also been utilized to improve the data dissemination performance [12], [13], [44], [45]. Splash [46] achieves reliable data dissemination with low latency by exploiting constructive interference and channel diversity. Other data dissemination techniques [15], [47] leverage the coding techniques. Rateless Deluge [47] utilizes rateless codes to improve the transmission reliability over regular Deluge. The most recent technique – Pando [15] improves the performance of Deluge by using the combination of LT codes and pipelining. Although data dissemination has been extensively investigated, prior approaches mainly focus on improving the data dissemination performance within the same network (i.e., WiFi or ZigBee network). Little work has been conducted to investigate how to leverage CTC in heterogeneous IoT networks for further performance improvement, especially when the number of IoT devices is exponentially increasing. Instead of treating the IoT devices from other networks (e.g., WiFi) as interference and harmful, our work is the first work that explores how to leverage the WiFi AP as a collaborative and benign device to conduct data dissemination in the ZigBee network, which proceeds to become more and more common nowadays.

IX. Conclusion

The exponentially increasing number of IoT devices and recent advances in CTC physical layer design motivates us to investigate how to leverage the CTC technique for further performance improvements in heterogeneous IoT networks (i.e., WiFi and ZigBee coexistence networks). In this paper, we introduce Waves, which seamlessly enables the simultaneous WiFi-to-WiFi communication and ZigBee data dissemination. Our approach not only leverages a novel WiFi AP Initiated Dynamic Broadcasting (WIDB) scheme to effectively control the WiFi transmission power but also utilizes a Distributed Fountain Codes Transmission (DFCT) techniques to support reliable CTC for WiFi-to-ZigBee data dissemination. We extensively evaluated Waves under different settings. Evaluation results indicate that Waves can achieve reliable and fast data dissemination. With the support of the latest CTC technologies, Waves has the potential to be deployed on commodity devices. Moreover, Waves opens a new direction for collaborative network layer design for heterogeneous IoT networks.

References

[1] Y. Zhang and Q. Li, "HoWiES: A holistic approach to ZigBee assisted WiFi energy savings in mobile devices," in *Proc. IEEE INFOCOM*, Apr. 2013, pp. 1366–1374.

[2] S. M. Kim and T. He, "FreeBee: Cross-technology communication via free side-channel," in *Proc. 21st Annu. Int. Conf. Mobile Comput. Netw.*, Sep. 2015, pp. 317–330.

[3] Z. Li and T. He, "WEBee: Physical-layer cross-technology communication via emulation," in *Proc. 23rd Annu. Int. Conf. Mobile Comput. Netw.*, Oct. 2017, pp. 2–14.

[4] Z. Chi, Y. Li, Y. Yao, and T. Zhu, "PMC: Parallel multi-protocol communication to heterogeneous IoT radios within a single WiFi channel," in *Proc. IEEE 25th Int. Conf. Netw. Protocols (ICNP)*, Oct. 2017, pp. 1–10.

[5] *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, IEEE Standard 802.11-1997, IEEE Computer Society LAN MAN Standard Committee, 1997.

[6] D. Qiao, S. Choi, A. Jain, and K. G. Shin, "MiSer: An optimal low-energy transmission strategy for IEEE 802.11a/h," in *Proc. 9th Annu. Int. Conf. Mobile Comput. Netw.*, Sep. 2003, pp. 161–175.

[7] D. Qiao, S. Choi, and K. Shin, "Interference analysis and transmit power control in IEEE 802.11a/h wireless LANs," *IEEE/ACM Trans. Netw.*, vol. 15, no. 5, pp. 1007–1020, Oct. 2007.

[8] L. Sun, H. Deng, R. K. Sheshadri, W. Zheng, and D. Koutsonikolas, "Experimental evaluation of WiFi active power/energy consumption models for smartphones," *IEEE Trans. Mobile Comput.*, vol. 16, no. 1, pp. 115–129, Jan. 2017.

[9] Z. Chi, Z. Huang, Y. Yao, T. Xie, H. Sun, and T. Zhu, "EMF: Embedding multiple flows of information in existing traffic for concurrent communication among heterogeneous IoT devices," in *Proc. IEEE INFOCOM Conf. Comput. Commun.*, May 2017, pp. 1–9.

[10] C. Gandarillas, C. Martin-Engenos, H. L. Pombo, and A. G. Marques, "Dynamic transmit-power control for WiFi access points based on wireless link occupancy," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Apr. 2014, pp. 1093–1098.

[11] M. Maróti, B. Kusy, G. Simon, and Á. Lédeczi, "The flooding time synchronization protocol," in *Proc. 2nd Int. Conf. Embedded Networked Sensor Syst.*, Nov. 2004, pp. 39–49.

[12] F. Ferrari, M. Zimmerling, L. Thiele, and O. Saukh, "Efficient network flooding and time synchronization with glossy," in *Proc. 10th ACM/IEEE Int. Conf. Inf. Process. Sensor Netw.*, Apr. 2011, pp. 73–84.

[13] Y. Wang, Y. He, X. Mao, Y. Liu, Z. Huang, and X. Li, "Exploiting constructive interference for scalable flooding in wireless networks," in *Proc. IEEE INFOCOM*, vol. 21, no. 6, Mar. 2012, pp. 1880–1889.

[14] Z. Chi, Y. Li, H. Sun, Y. Yao, Z. Lu, and T. Zhu, "B2W2: N-way concurrent communication for IoT devices," in *Proc. 14th ACM Conf. Embedded Netw. Sensor Syst.*, Nov. 2016, pp. 245–258.

[15] W. Du, J. C. Liando, H. Zhang, and M. Li, "When pipelines meet fountain: Fast data dissemination in wireless sensor networks," in *Proc. 13th ACM Conf. Embedded Networked Sensor Syst.*, Nov. 2015, pp. 365–378.

[16] Z. Chi et al., "EAR: Exploiting uncontrollable ambient RF signals in heterogeneous networks for gesture recognition," in *Proc. 16th ACM Conf. Embedded Networked Sensor Syst.*, Nov. 2018, pp. 237–249.

[17] A. Acar et al., "Peek-a-boo: I see your smart home activities, even encrypted!" in *Proc. 13th ACM Conf. Secur. Privacy Wireless Mobile Netw.*, 2020, pp. 207–218.

[18] (2020). *CISCO Aironet 1520*. [Online]. Available: https://www.cisco.com/c/en/us/td/docs/wireless/technology/mesh/7-3/design/guide/Mesh.html

[19] M. Durvy and P. Thiran, "A packing approach to compare slotted and non-slotted medium access control," in *Proc. 25th IEEE Int. Conf. Comput. Commun. (INFOCOM)*, Barcelona, Spain, 2006, pp. 1–12, doi: 10.1109/INFOCOM.2006.251.

[20] V. P. Mhatre, K. Papagiannaki, and F. Baccelli, "Interference mitigation through power control in high density 802.11 WLANs," in *Proc. 26th IEEE Int. Conf. Comput. Commun.*, May 2007, pp. 535–543.

[21] D. J. MacKay, "Fountain codes," *IEE Proc.-Commun.*, vol. 152, no. 6, pp. 1062–1068, 2005.

[22] M. Luby, "Lt codes," in *Proc. 43rd Annu. IEEE Symp. Found. Comput. Sci.*, Nov. 2002, p. 271.

[23] A. G. Dimakis, V. Prabhakaran, and K. Ramchandran, "Distributed fountain codes for networked storage," in *Proc. IEEE Int. Conf. Acoust. Speed Signal Process.*, 2006, pp. 1–4.

[24] (2013). *802.11G*. [Online]. Available: http://infocom.uniroma1.it/alef/802.11/standard/802.11g-2003.pdf

[25] *802.11g*. Accessed: Mar. 15, 2023. [Online]. Available: https://github.com/bastibl/gr-ieee802-11

[26] *USRP B210*. Accessed: Mar. 15, 2023. [Online]. Available: https://www.ettus.com/product/category/USRP-Bus-Series

[27] *DJI RoboMaster*. Accessed: Mar. 15, 2023. [Online]. Available: https://www.dji.com/robomaster-s1

[28] M. R. Hasan, Y. Zhao, Y. Luo, G. Wang, and R. M. Winter, "An effective AODV-based flooding detection and prevention for smart meter network," *Proc. Comput. Sci.*, vol. 129, pp. 454–460, Jan. 2018.

[29] Z. Huang and T. Zhu, "Leveraging multi-granularity energy data for accurate energy demand forecast in smart grids," in *Proc. IEEE Int. Conf. Big Data (Big Data)*, Dec. 2016, pp. 1182–1191.

[30] *Cisco Global Cloud Index: Forecast and Methodology, 2014–2019 White Paper*, CISCO, San Jose, CA, USA, 2019.

[31] W. Wang, T. Xie, X. Liu, Y. Yao, and T. Zhu, "ECT: Exploiting cross-technology transmission for reducing packet delivery delay in IoT networks," *ACM Trans. Sen. Netw.*, vol. 15, no. 2, pp. 1–28, 2019.

[32] (2018). *CISCO White Paper*. [Online]. Available: https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-738429.html#_Toc953327

[33] K. Chebrolu and A. Dhekne, "Esense: Communication through energy sensing," in *Proc. 15th Annu. Int. Conf. Mobile Comput. Netw.*, Sep. 2009, pp. 85–96.

[34] S. Wang, W. Jeong, J. Jung, and S. M. Kim, "X-MIMO: Cross-technology multi-user MIMO," in *Proc. 18th Conf. Embedded Networked Sensor Syst.*, 2020, pp. 218–231.

[35] L. Mottola, G. P. Picco, M. Ceriotti, C. S. Guna, and A. L. Murphy, "Not all wireless sensor networks are created equal: A comparative study on tunnels," *ACM Trans. Sensor Netw.*, vol. 7, no. 2, pp. 1–33, 2010.

[36] X. Zhang and K. G. Shin, "Chorus: Collision resolution for efficient wireless broadcast," in *Proc. IEEE INFOCOM*, Mar. 2010, pp. 1–9.

[37] M. Zuniga and B. Krishnamachari, "Optimal transmission radius for flooding in large scale sensor networks," *Cluster Comput.*, vol. 8, nos. 2–3, pp. 167–178, Jul. 2005.

[38] S. Li, L. Su, Y. Suleimenov, H. Liu, T. Abdelzaher, and G. Chen, "Centaur: Dynamic message dissemination over online social networks," in *Proc. 23rd Int. Conf. Comput. Commun. Netw. (ICCCN)*, Aug. 2014, pp. 1–8.

[39] S. Guo, L. He, Y. Gu, B. Jiang, and T. He, "Opportunistic flooding in low-duty-cycle wireless sensor networks with unreliable links," *IEEE Trans. Comput.*, vol. 63, no. 11, pp. 2787–2802, Nov. 2014.

[40] K. Srinivasan et al., "The k factor: Inferring protocol performance using inter-link reception correlation," in *Proc. 16th Annu. Int. Conf. Mobile Comput. Netw.*, Sep. 2010, pp. 317–328.

[41] S. Wang, S. M. Kim, Y. Liu, G. Tan, and T. He, "CorLayer: A transparent link correlation layer for energy efficient broadcast," in *Proc. 19th Annu. Int. Conf. Mobile Comput. Netw.*, 2013, pp. 51–62.

[42] T. Zhu, Z. Zhong, T. He, and Z.-L. Zhang, "Exploring link correlation for efficient flooding in wireless sensor networks," in *Proc. USENIX NSDI*, 2010, pp. 1–15.

[43] S. Guo, S. M. Kim, T. Zhu, Y. Gu, and T. He, "Correlated flooding in low-duty-cycle wireless sensor networks," in *Proc. 19th IEEE Int. Conf. Netw. Protocols*, Oct. 2011, pp. 383–392.

[44] K. Whitehouse, A. Woo, F. Jiang, J. Polastre, and D. Culler, "Exploiting the capture effect for collision detection and recovery," in *Proc. 2nd IEEE Workshop Embedded Networked Sensors*, May 2005, pp. 45–52.

[45] F. Ferrari, M. Zimmerling, L. Mottola, and L. Thiele, "Low-power wireless bus," in *Proc. 10th ACM Conf. Embedded Netw. Sensor Syst.*, Nov. 2012, pp. 1–14.

[46] M. Doddavenkatappa et al., "Splash: Fast data dissemination with constructive interference in wireless sensor networks," in *Proc. NSDI*, 2013, pp. 269–282.

[47] A. Hagedorn, D. Starobinski, and A. Trachtenberg, "Rateless deluge: Over-the-air programming of wireless sensor networks using random linear codes," in *Proc. Int. Conf. Inf. Process. Sensor Netw. (IPSN)*, Apr. 2008, pp. 457–466.