X-Disco: Cross-technology Neighbor Discovery

Shuai Wang*, Jianlin Guo†, Pu Wang†, Kieran Parsons†, Philip Orlik†, Yukimasa Nagai‡
Takenori Sumi‡, Parth Pathak*
*George Mason University, †Mitsubishi Electric Research Laboratories (MERL),
‡Information Technology R&D Center of Mitsubishi Electric Corporation
Email: {swang42, phpathak}@gmu.edu, {guo, pwang, parsons, porlik}@merl.com,
{Nagai.Yukimasa@ds., Sumi.Takenori@dc.}MitsubishiElectric.co.jp

***Abstract*—With the explosive proliferation of wireless devices, our lives are improved by various applications supported by heterogeneous wireless technologies, such as WiFi and ZigBee. However, the coexistence of WiFi and ZigBee also results in the degradation of the network performance, which cannot be avoided if the WiFi devices are even unaware of the ambient ZigBee devices. To better accommodate the heterogeneous wireless devices, this paper presents X-Disco, the first cross-technology neighbor discovery mechanism, for a WiFi device to detect ZigBee neighbors, without modification to hardware or firmware. With the help of the recently proposed cross-technology communication, X-Disco enables a commodity WiFi device to trigger responses, containing ZigBee neighbor information, from the ambient ZigBee coordinators (including routers). Through exploring the WiFi PHY-layer information accessible by WiFi driver, X-Disco decodes the responded ZigBee messages and obtains the ZigBee neighbor information. To improve X-Disco's reliability, we also propose ZigBee neighbor validation and interruption mitigation to exclude hidden node terminals and mitigate the interference caused by the ambient WiFi traffic respectively. The evaluation of X-Disco is performed on the commodity devices (TP-Link WDR 4300 WiFi router, TelosB motes) and USRP B210. The results demonstrate X-Disco successfully detects nine ZigBee neighbors within 70ms in the office.**

I. Introduction

We have witnessed the explosive growth of IoT devices , including WiFi, ZigBee, and Bluetooth, along with various applications supported by heterogeneous wireless technologies in the past decades. As half billion ZigBee chips sold [1] and over three billion WiFi devices shipped annually [2], WiFi and ZigBee coexist densely on the 2.4 GHz ISM spectrum and physical places such as smart homes and factories, raising critical coexistence issues such as cross-technology interference (CTI) [3], [4]. To avoid such interference, cross-technology coordination [5], [6] and cooperation [7] are proposed for better accommodating WiFi and ZigBee devices. Nevertheless, the coordination across multiple wireless technologies inevitably requires wireless devices to maintain the cross-technology neighbor information. Therefore, this paper focuses on enabling a universal neighbor discovery mechanism for a WiFi device to detect the ambient ZigBee neighbors, namely cross-technology neighbor discovery.

As an essential step of establishing and maintaining a network, neighbor discovery is inherently supported in the homogeneous ZigBee [8] and WiFi networks [9]. However, discovering cross-technology neighbors is non-trivial due to two challenges: (i), WiFi and ZigBee devices cannot directly communicate with each other due to the incompatible PHY layers. (ii), developing a universal neighbor discovery mechanism across multiple wireless protocols might require significant modification on the billions of existing IoT devices [10], resulting in impractical use cases and expensive costs at scale.

This paper proposes **X-Disco**, the first software-only cross-technology neighbor discovery mechanism, to enable a WiFi device to discover the ambient ZigBee neighbors without any modification to the ZigBee devices. X-Disco achieves this by leveraging the Device and Service Discovery mechanism [8], where the ZigBee neighbor information, such as addresses, is shared per neighbor information request sent to the ZigBee coordinator [1]. At a high level, after the X-Disco device (commodity WiFi) transmits a neighbor information request via the recent proposed cross-technology communication (CTC) [11], the ZigBee coordinator reacts to that request as if that request is from a ZigBee device and replies with a message, containing all associated ZigBee devices' addresses, which are further decoded and obtained by the X-Disco device. Decoding the replied ZigBee message is uniquely inspired by our newly discovered insight: the ZigBee signal is recognizable and decodable by exploiting the special patterns extracted from FFT magnitude (accessible by driver) collected at WiFi Spectral Scan, ensuring compatibility to commodity WiFi. As fetching neighbor information from ZigBee coordinators strictly follows ZigBee Device and Service Discovery mechanism, X-Disco maintains transparency to ZigBee network. In addition, working in active mode, the ZigBee coordinators are designed to be responsive to the neighbor information request, thereby incurring minimum overhead, as no duty cycle is involved.

X-Disco is built with three new technical highlights: (i) ZigBee Symbol Extraction, (ii) ZigBee Coordinator Detection, and (iii) Neighbor Information Acquisition, where the compatibility with the hardware and protocols is the key. ZigBee Symbol Extraction ensures that ZigBee messages are reliably decoded at commodity WiFi, under the challenge where the phase information is totally discarded, to overcome the PHY-

This work was done while Shuai Wang worked at MERL as an intern.

[1]Deployed for forwarding packets in multi-hop networks, ZigBee routers are included in ZigBee coordinators since they function same in our design. Therefore, we don't distinguish ZigBee coordinators and routers.

978-1-6654-8643-9/22/$31.00 ©2022 IEEE

layer incompatibility issue. ZigBee Coordinator Detection detects ambient ZigBee coordinators, from which Neighbor Information Acquisition obtains the ZigBee neighbor information by exchanging ZigBee compatible messages, yielding 100% transparency to the ZigBee network. To the best of our knowledge, X-Disco is the first design to discover cross-technology neighbors using commodity WiFi devices. X-Disco effectively utilizes the widely deployed WiFi infrastructures to detect ambient ZigBee devices, demonstrating the pervasive application in practice at zero cost. To summarize, the contribution of this paper is three-fold:

- We design X-Disco, the first cross-technology neighbor discovery mechanism for a commodity WiFi device to detect ambient ZigBee neighbors. The full compatibility with commodity WiFi and ZigBee hardware and protocol ensures X-Disco's wide and practical deployment.
- X-Disco introduces three main techniques: ZigBee Symbol Extraction, ZigBee Coordinator Detection, and Neighbor Information Acquisition, which allow a commodity WiFi device to decode the responded ZigBee messages, detect the ambient ZigBee coordinators, and acquire the ZigBee neighbor information respectively. In addition, we propose two enhancements (ZigBee Neighbor Validation and Interruption Mitigation) to improve the reliability of X-Disco.
- X-Disco is evaluated on the commodity WiFi (TP-link WDR 4300 router), software-defined radio (USRP B210), and commodity ZigBee (Telosb motes). The results demonstrate that X-Disco successfully detects nine ZigBee neighbors within 70ms in the office.

II. Motivation

A. The Need for Cross-technology Neighbor Discovery

Numerous IoT devices with different wireless technologies densely coexist on the ISM band and the physical world to support various applications. For instance, 53 million Amazon Echo devices [12], equipped with WiFi and ZigBee transceivers, Philips Hue Smart Bulb, and Samsung SmartThings, were shipped in 2020 to support smart homes. ZigBee-based route management systems and WiFi modules are installed for smart factories [13]. In such a dense WiFi and ZigBee coexisting environment, severe ZigBee transmission loss ($\geq$50% ZigBee packets [4]), caused by the cross-technology interference from WiFi, degrades spectral efficiency and results in failures of ZigBee applications. Nevertheless, all these problems could be avoided via heterogeneous coordination [7], [5], [6], [14], if heterogeneous wireless devices are aware of each other – i.e., the neighbor information is dynamically maintained and shared across multiple wireless technologies. Therefore, we present X-Disco for commodity WiFi devices to detect the ZigBee neighbors. To minimize the deployment cost, X-Disco is designed to be a software-only approach and 100% transparency to the ZigBee network, which are inspired by the following two opportunities.

B. Opportunities

1) Cross-technology Communication: The recent advanced Cross-technology Communication designs [11], [15] enable a commodity WiFi device to send messages to a commodity ZigBee device directly. Specifically, a WiFi device emulates the target ZigBee message via carefully customizing the payload of a WiFi packet such that the corresponding transmitted WiFi signal is recognized as a legitimate ZigBee packet with the intended message by the commodity ZigBee devices. In this paper, X-Disco incorporates CTC to trigger the response from the ambient ZigBee coordinators. Meanwhile, decoding the responded ZigBee messages at commodity WiFi is inspired by the next opportunity.

2) Fine-grained PHY-layer Information at WiFi: The commodity WiFi device exposes fine-grained PHY-layer information such as Channel State Information (CSI) [16] and Fast Fourier Transformation (FFT) magnitude of the received signal [17], [18] to the WiFi driver. As a proprietary mode supported by many WiFi drivers and commodity WiFi devices [2], Spectral Scan [18], [19] continuously collects the FFT magnitude of the received signal, regardless of the signal type. That is, upon the arrival of a ZigBee signal, WiFi Spectral Scan converts that ZigBee signal into a series of FFT magnitudes, demonstrating special patterns of ZigBee signal. However, it is still quite challenging to decode the ZigBee message because ZigBee modulates information in the phase, whereas WiFi Spectral Scan only provides magnitude information without phase. In next Section, we demonstrate an overview of X-Disco, followed by insights for overcoming this challenge.

III. Overview of X-Disco and Background

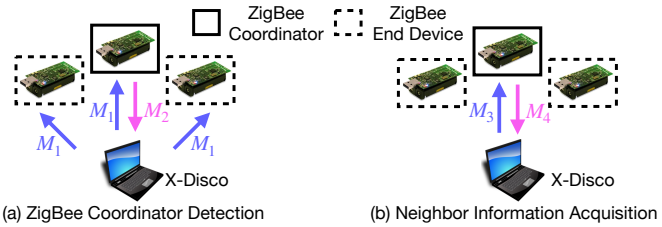


Fig. 1. Two steps in X-Disco: ZigBee Coordinator Detection and Neighbor Information Acquisition, while each step requires two messages exchanged.

A. X-Disco in a Nutshell

X-Disco is a two-step approach, containing four messages (M_1 to M_4) exchanged between an X-Disco device (commodity WiFi) and ambient ZigBee coordinators. As illustrated in Figure 1, in Step (a), the X-Disco device transmits an emulated ZigBee broadcast packet in message M_1, triggering the ZigBee coordinator to rebroadcast in the message M_2, from which the X-Disco device obtains the essential ZigBee network information for customizing a neighbor information request message in the next step. In Step (b), the X-Disco device requests the ZigBee neighbor information in the carefully customized message M_3, which triggers the ZigBee coordinator to attach the associated ZigBee devices' addresses

[2]These include ath9k, ath10k [19], and ath11k [20]) drivers, and ar92xx, ar93xx, and ar98xx chips.

in the responded message M_4. By leveraging the ZigBee Device and Service Discovery mechanism, X-Disco detects ZigBee neighbors via fetching the neighbor information from the ZigBee coordinator, with only four messages exchanged. As ZigBee coordinators are always in active mode, the exchanged messages are naturally immune to the duty-cycle related problems, thereby achieving the minimum overhead.

As the foundation of X-Disco, decoding the replied message M_2 and M_4 at commodity WiFi is very challenging because WiFi Spectral Scan does not provide any phase information, whereas ZigBee modulation relies on phase. To address this issue, we propose ZigBee Symbol Extraction, which decodes the ZigBee signal only using the FFT magnitude without phase information. To understand ZigBee Symbol Extraction, we demonstrate how the ZigBee signal is constructed at the ZigBee PHY layer and how the ZigBee signal is interpreted at WiFi Spectral Scan in next Section.

B. How ZigBee signal is interpreted at WiFi

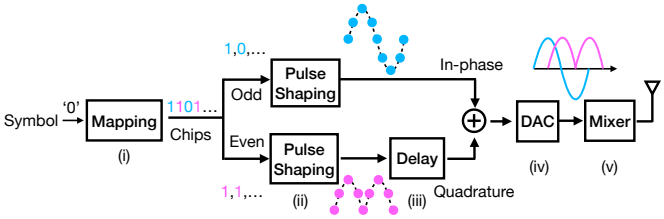


Fig. 2. PHY Layer of a ZigBee transmitter.

1) ZigBee Transmitter: The transmission of a ZigBee packet starts with assembling every four bits into one symbol ('0'-'F'), which is the basic unit to carry information in ZigBee [21]. As illustrated in Figure 2, the ZigBee PHY Layer first converts the input ZigBee symbol into a unique and pseudo-random 32-bit chip sequence [21] in Step (i), i.e., Direct Sequence Spread Spectrum (DSSS). Then, the chips '1' and '0' are shaped into positive and negative $1\mu s$ half-sine pulses in Step (ii) and (iii), where the quadrature signal, corresponding to the chips on the even indices, is delayed by half pulse duration $0.5\mu s$, compared to the in-phase signal (the chips on the odd indices). As the in-phase (I) and quadrature signal (Q) are merged, this half-pulse delay leads to complex sinusoidal waves with constant magnitude, while expressing 0/1 chips in the phase, namely Offset Quadrature Phase Shift Keying (OQPSK). Finally, in Step (iv) the digital-to-analog converter (DAC) translates the discrete I/Q signal into a continuous analog baseband signal, which is then shifted by the mixer to the ZigBee's carrier frequency (passband) and transmitted into the air in Step (v).

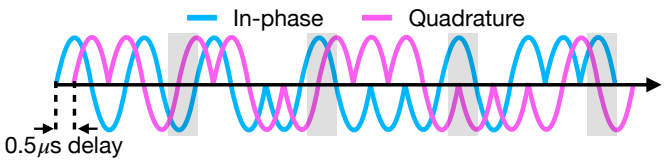


Fig. 3. In the baseband (I/Q) signal of ZigBee symbol '0', where the Quadrature is delayed by $0.5\mu s$, the four $3.2\mu s$ non-grayed segments are fed into FFT magnitude calculation while the grayed parts are discarded at WiFi Spectral Scan.

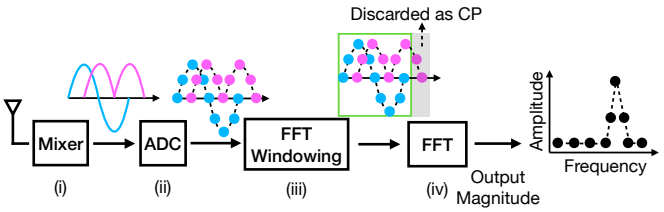


Fig. 4. Illustration of WiFi Spectral Scan.

To demonstrate the intuition of the ZigBee signal, we plot the I/Q waveform of ZigBee symbol '0' in Figure 3. The ZigBee PHY Layer converts one ZigBee symbol into 32 chips, where the In-phase and Quadrature take 16 chips each, yielding the ZigBee signal of $16\mu s$ with a constant magnitude. Since the duration of each chip is $1\mu s$, the complex ZigBee signal consists of 2MHz positive or negative half-sine waves, resulting in 2MHz bandwidth. Next, we show the architecture of WiFi Spectral Scan, which provides the fundamental insight for decoding a ZigBee message at commodity WiFi.

2) WiFi Spectral Scan: As Figure 4 depicts, in Step (i), the mixer shifts the passband signal to the baseband, which is further sampled at 20MHz by the analog-to-digital converter (ADC) in Step (ii). Then in Step (iii), FFT Windowing is performed every $4\mu s$ [3] to cut the continuously received samples into fragments of 80 samples, where the last 16 samples (e.g., grayed parts in Figure 3) are discarded as cyclic prefix (CP), designed for avoiding inter symbol interference. Finally, in Step (iv), the rest 64 samples ($3.2\mu s$ non-grayed segments in Figure 3) are fed into FFT calculation, which outputs the corresponding magnitude while the phase information is left out. Since this process does not require the received signal to be WiFi, an arbitrary signal (e.g., ZigBee) will be reflected in FFT magnitude if Spectral Scan mode is on.

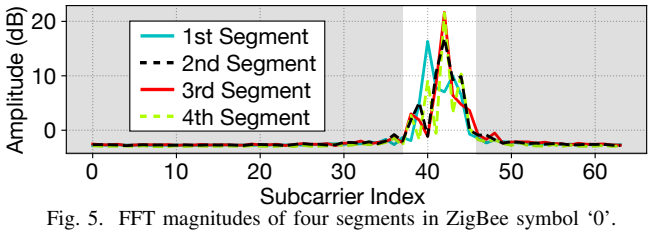


Fig. 5. FFT magnitudes of four segments in ZigBee symbol '0'.

When the signal of ZigBee symbol '0', transmitted on ZigBee channel 13 (2.415GHz), arrives at WiFi Spectral Scan working on WiFi channel 1 (2.412GHz), the mixer shifts the Zigbee signal to the center frequency of the WiFi channel, a 3MHz frequency offset is introduced in the baseband signal, yielding the overlap with WiFi subcarriers 38 to 45. Then, as depicted in Figure 3, FFT Windowing cuts the baseband signal into four non-grayed segments. As illustrated in Figure 5, the results depict an interesting insight — four FFT magnitudes demonstrate different patterns on the overlapped subcarriers. This insight is quite counter-intuitive because the four non-grayed segments have the same and constant magnitude, as explained in Section III-B1, whereas the corresponding FFT magnitudes are different.

[3]Achieved by setting **`fft_period`** to be 0 in configuration file in the WiFi ath9k driver [19].

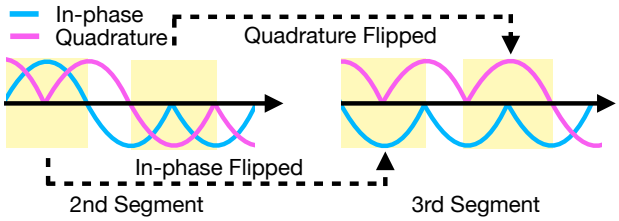


Fig. 6. The difference between the 2nd and 3rd segments of ZigBee symbol '0' comes from the flipped $1\mu s$ sinusoidal waves, marked in yellow shadow, in In-phase and Quadrature.

How to understand this insight? We use the 2nd and 3rd segments of ZigBee symbol '0' as an example to explain this insight. Due to the randomness in the Symbol-to-Chip Mapping, the 0/1 chips in a ZigBee symbols are random, as well as the corresponding positive and negative sinusoidal signals. As compared in Figure 6, the yellow marked sinusoidal waves are the flipped in the 2nd and 3rd segments. Such flip only changes the phase of the signal while the magnitude of the time domain signal is still the same. When we feed those two segments into the FFT calculation, the results reflect two segments on the frequency domain, not the time domain. According to the property of FFT, the two segments induce the same FFT magnitude, if and only if one segment is the phase-shifted version of the other. Since not all $1\mu s$ sinusoidal waves are flipped, the entire $3.2\mu s$ 2nd segment is not the phase-shifted version of the entire 3rd segment. Therefore, the FFT magnitudes of those two segments are different. Not only the FFT magnitudes of different segments in one ZigBee symbol are unique, the randomness in the Symbol-to-Chip Mapping makes different ZigBee symbols induce a unique and specific pattern in the corresponding four FFT magnitudes, indicating the feasibility of decoding the ZigBee symbol without the phase information on commodity WiFi.

IV. Design of X-Disco

Based on the insight introduced in the last Section, the detailed designs of X-Disco are demonstrated here.

A. ZigBee Symbol Extraction

Extracting the ZigBee symbol information on commodity WiFi is realized by exploring the uniqueness of the four FFT magnitudes induced by different ZigBee symbols. To simplify the notation, we define the four FFT magnitudes calculated from one ZigBee symbol to be an FFT group. At a high level, decoding the ZigBee symbol is achieved by comparing the received FFT group with the template FFT groups, which are calculated from the transmitted signals of 16 ZigBee symbols. The ZigBee symbol of the received FFT group corresponds to the template FFT group with the highest similarity.

Specifically, we denote the template FFT group of the ZigBee symbol i by $\mathbb{Z}_i$, where $i \in \{0, \cdots, F\}$. Then the FFT group is specifically defined as $\mathbb{Z}_i \triangleq [\boldsymbol{Z_{i,1}}, \boldsymbol{Z_{i,2}}, \boldsymbol{Z_{i,3}}, \boldsymbol{Z_{i,4}}]$, where $\boldsymbol{Z_{i,k}}$ represents the FFT magnitude of the k-th segment in Symbol i. With only eight WiFi subcarriers overlapped with one ZigBee channel, we define $\boldsymbol{Z_{i,k}} \triangleq [Z_{i,k}[L], Z_{i,k}[L+1], ..., Z_{i,k}[L+7]]$, where $Z_{i,k}[L]$ is the magnitude of the L-th subcarrier in $\boldsymbol{Z_{i,k}}$ and L is the index of the left most subcarrier overlapped with the ZigBee channel. Based on that, we define the similarity between the FFT groups induced by ZigBee symbol i and j as follows:

Definition 1 (Similarity): The similarity between two FFT groups $\mathbb{Z}_i$ and $\mathbb{Z}_j$ is the multiplication of the cross-correlation coefficient between each two FFT magnitudes,

$$sim(\mathbb{Z}_i, \mathbb{Z}_j) = \prod_{k=1}^{4} corr(\boldsymbol{Z_{i,k}}, \boldsymbol{Z_{j,k}}), \tag{1}$$

where $corr$ calculates the correlation coefficient between two vectors. With this definition, if any two FFT magnitudes in two ZigBee symbols are different, the similarity drops significantly.

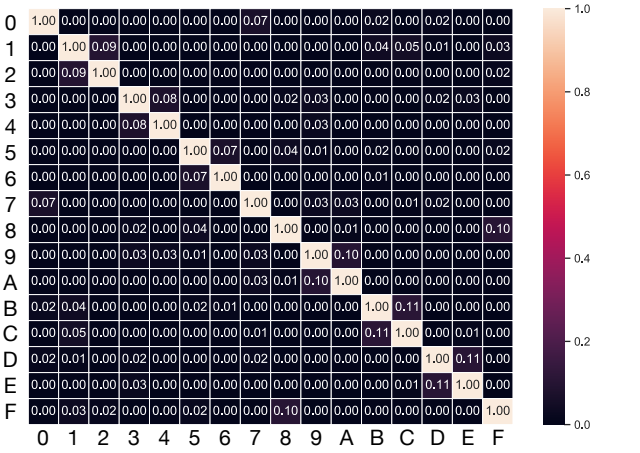


Fig. 7. Similarity between the FFT group of different ZigBee Symbols.

To demonstrate the insight of decoding ZigBee symbols without phase information, we plot the similarity between the FFT groups of arbitrary two ZigBee symbols in Figure 7. Apparently, the similarity between the template FFT groups of different ZigBee symbols is quite small, indicating that we could decode ZigBee symbols by comparing the similarity, which is purely calculated from FFT magnitude without any phase information on commodity WiFi.

In X-Disco, extracting ZigBee symbols at commodity WiFi starts with forming the four received FFT magnitudes $\boldsymbol{Y_n}, \boldsymbol{Y_{n+1}}, \boldsymbol{Y_{n+2}}$, and $\boldsymbol{Y_{n+3}}$, into an FFT group $\mathbb{Y}_n \triangleq [\boldsymbol{Y_n}, \boldsymbol{Y_{n+1}}, \boldsymbol{Y_{n+2}}, \boldsymbol{Y_{n+3}}]$. If the ZigBee symbol i's template FFT group has the highest similarity, the decoding result is the ZigBee symbol 'i'. Therefore, extracting the ZigBee symbol from the received FFT group $\mathbb{Y}_n$ is achieved by checking which template FFT group has the highest similarity:

$$\underset{i}{\operatorname{argmax}}\, sim(\mathbb{Y}_n, \mathbb{Z}_i) \tag{2}$$

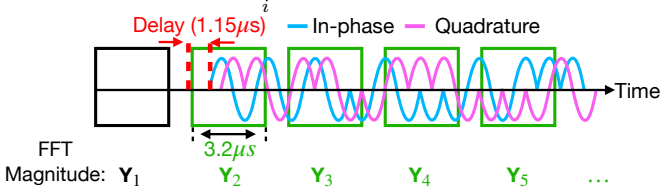


Fig. 8. The X-Disco keeps collecting the FFT magnitudes, where the $\boldsymbol{Y_2}$ to $\boldsymbol{Y_5}$ capture the ZigBee signal with a delay of 1.15 μs.

Nevertheless, directly applying Equation 2 to decode a ZigBee packet faces two practical issues. As illustrated in

Figure 8, the X-Disco device continuously collects the FFT magnitude $\boldsymbol{Y_1}$ to $\boldsymbol{Y_5}$ from Spectral Scan. Since the X-Disco device is not synchronized to the ZigBee packets, two issues occur: (i), the unknown arrival time of a ZigBee packet. For instance, in Figure 8, the first ZigBee symbol in a ZigBee packet, captured by the FFT magnitude $\boldsymbol{Y_2}$ to $\boldsymbol{Y_5}$, should be detected by X-Disco before extracting the ZigBee symbols. (ii), the unknown delay in the FFT window. The FFT magnitude $\boldsymbol{Y_2}$ is calculated from the 1.15 μs noise concatenated by the first $2.05\mu s$ ZigBee signal due to the delay. Directly comparing such received FFT group with our template FFT groups, which are calculated in the synchronized case, would degrade the similarity and the accuracy of ZigBee Symbol Extraction. To resolve these two issues, we present two new designs: ZigBee Cross-detection and Fine-grained Synchronization.

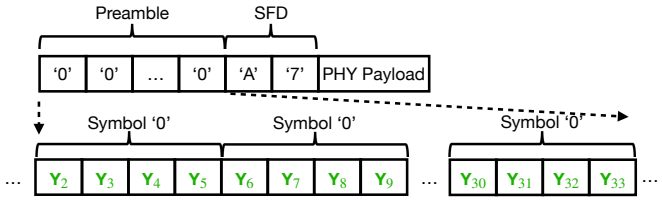


Fig. 9. The ZigBee preamble of eight symbol '0's is captured by the FFT magnitudes $\boldsymbol{Y_2}$ to $\boldsymbol{Y_{33}}$.

1) ZigBee Cross-detection: as illustrated in Figure 9, the ZigBee packet starts with eight repeated '0's as the preamble field. With this observation, detecting the arrival of a ZigBee packet at commodity WiFi is achieved by checking if the eight consecutive FFT groups are the same. Specifically, we calculate the multiplication of the similarity between the current FFT group $\mathbb{Y}_n$ and the seven following FFT groups:

$$\prod_{i=1}^{7} sim(\mathbb{Y}_n, \mathbb{Y}_{n+4i}) \tag{3}$$

If this value reaches to a threshold (e.g., 0.4 [4]), a ZigBee packet is detected. Then, we know the current FFT group $\mathbb{Y}_n$ captures the start of the ZigBee signal, and the FFT magnitude $\boldsymbol{Y_n}$ is the first FFT magnitude of the first ZigBee symbol '0' in the ZigBee preamble.

2) Fine-grained Synchronization: we note that the random delay shifts the whole ZigBee signal and changes the FFT magnitude. By leveraging the knowledge that the first eight ZigBee symbols (preamble) are known, X-Disco detects the delay via matching the delayed version of the template FFT group of ZigBee symbol '0' and the FFT group of the first received ZigBee symbol '0'. Specifically, we create the template FFT group for each of 16 ZigBee symbols with all possible delays – $\mathbb{Z}_i^d \triangleq [\boldsymbol{Z_{i,1}^d}, \boldsymbol{Z_{i,2}^d}, \boldsymbol{Z_{i,3}^d}, \boldsymbol{Z_{i,4}^d}]$, where $\boldsymbol{Z_{i,k}^d}$ represents the k-th FFT magnitude of the ZigBee symbol i with a delay of d samples. Thus, the random delay τ is detected by finding which τ maximizes the similarity between the FFT group of the first received ZigBee symbol '0' and the delayed template FFT group:

$$\underset{\tau}{\operatorname{argmax}}\, sim(\mathbb{Y}_n, \mathbb{Z}_0^\tau) \tag{4}$$

[4]0.4 provides us $\geq 96\%$ ZigBee packet detection rate in office environment.

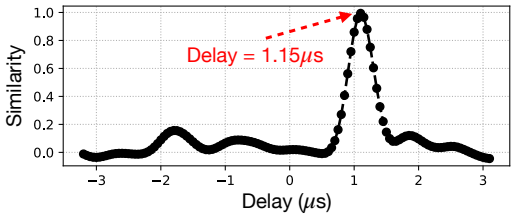


Fig. 10. The similarity between the FFT group of the first received ZigBee symbol '0' and template FFT group with all possible delays, where the negative delays indicate ZigBee signal arrives prior to the FFT calculation.

Figure 10 demonstrates the similarity between the FFT group of the ZigBee signal, depicted in Figure 8, and the delayed template FFT group. The similarity reaches the maximum at the delay of $1.15\mu s$, which is exactly the delay of the signal in Figure 8, validating the effectiveness of this design.

As the random delay is detected, the ZigBee symbols within the PHY-layer payload field, which are also shifted by the same delay, are decoded by checking which template FFT group of the delay τ is the closest to the received FFT group:

$$\underset{i}{\operatorname{argmax}}\, sim(\mathbb{Y}_n, \mathbb{Z}_i^\tau) \tag{5}$$

As a result, applying the decoding approach described in Equation 5 on all the received FFT groups, the X-Disco device decodes the entire ZigBee packet. Built on top of ZigBee Symbol Extraction, X-Disco is able to decode the ZigBee messages exchanged in ZigBee Coordinator Detection and Neighbor Information Acquisition. To achieve zero cost in deploying X-Disco into practice, we need X-Disco to be transparent to the existing ZigBee network. That is, our design should be compatible with the ZigBee protocol. Next, we introduce detailed designs to meet this goal.

B. ZigBee Coordinator Detection

Detecting the ZigBee coordinators using commodity WiFi is non-trivial because we need to maintain transparency to the existing ZigBee network. One straightforward way is to let the X-Disco device passively listen to the ZigBee channel until the periodic broadcasted ZigBee beacon packets are captured and decoded at commodity WiFi via ZigBee Symbol Extraction. Nevertheless, most ZigBee networks are non-beacon-enabled networks, which do not support beacon packets.

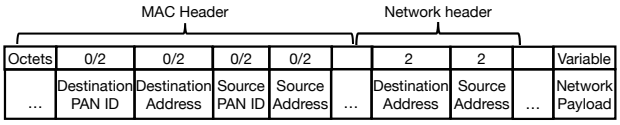


Fig. 11. In a ZigBee packet, the MAC Header and Network Header carry essential address and ID information.

In contrast to the passive listening, our proposed ZigBee Coordinator Detection actively triggers the ambient ZigBee coordinators to share their essential ZigBee network information with the commodity WiFi devices. This is achieved by leveraging the ZigBee *Passive Acknowledgement* mechanism specified in the ZigBee protocol [8], where the ZigBee coordinators would rebroadcast any received broadcast packets as a confirmation of packet reception, as opposed to explicitly

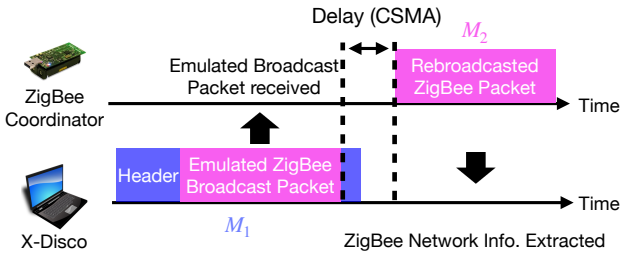


Fig. 12. The timeline of WiFi emulating a ZigBee broadcast packet in M_1, triggering a rebroadcasted packet M_2 from the ZigBee coordinator.

transmitting the MAC-layer ACK packets. It is worth mentioning that: (i), rebroadcasting packets at ZigBee coordinators indicates the existence of the ZigBee coordinators. (ii), the rebroadcasted packets encapsulate essential ZigBee network information, such as PAN IDs and addresses, in their header fields, as illustrated in Figure 11.

Our design achieves this by exchanging two messages (M_1 and M_2) between the X-Disco device and the Zigbee coordinator. As illustrated in Figure 12, the X-Disco device (commodity WiFi) sends out an emulated ZigBee broadcast packet via CTC [11] in the WiFi message M_1 and switches to the Spectral Scan mode. Upon the reception of the emulated ZigBee broadcast packet, the ZigBee coordinator rebroadcasts with a message M_2, from which the ZigBee coordinator is detected and the essential ZigBee network information is obtained by the X-Disco device.

Specifically, the X-Disco device configures each field, as illustrated in Figure 11, where the header is set to be the broadcast mode for the emulated ZigBee broadcast packet. Then, we apply CTC to transmit that customized ZigBee broadcast packet on the X-Disco device. After the ZigBee coordinator receives the emulated ZigBee broadcast packet, it fills its PAN ID and address fields into the MAC Header and the Network Header to construct the rebroadcasted packet. Eventually, running on the Spectral Scan mode, the X-Disco device applies ZigBee Symbol Extraction to obtain this encapsulated essential ZigBee network information, which is further utilized in Neighbor Information Acquisition. If there are multiple ZigBee coordinators nearby, the rebroadcasted ZigBee packets are transmitted with different delays due to CSMA, ensuring that ZigBee network information of all ambient ZigBee coordinators is collected without collision, thus the minimum overhead.

C. Neighbor Information Acquisition

IEEE_addr_req:

Octets: 2	1	1
NWKAddrOfInterest	RequestType	StartIndex

IEEE_addr_rsp:

Octets: 1	8	2	0/1	0/1	Variable
Status	IEEEAddr RemoteDev	NWKAddr RemoteDev	NumAssocDev	StartIndex	NWKAddr AssocDevList

Fig. 13. The format of `IEEE_addr_req` and `IEEE_addr_rsp` frame .

Acquiring the ZigBee neighbor information from the ambient ZigBee coordinators leverages the Device and Service Discovery in ZigBee protocol [8], which allows a ZigBee device to request the Network addresses of all the ZigBee neighbors associated with a specific ZigBee coordinator. This is realized via exchanging `IEEE_addr_req` and `IEEE_addr_rsp` messages, where the formats are described in Figure 13. By setting the "RequestType" and "StartIndex" to be 0x01 and 0x00 respectively, a ZigBee device transmits a `IEEE_addr_req` packet to trigger the ZigBee coordinator with the network address of "NWKAddrOfInterest" to respond with a `IEEE_addr_rsp` message, containing the number of the associated ZigBee devices in the "NumAssocDev" field and the network addresses of all associated ZigBee devices in the "NWKAddr AssocDevList" field.

Our Neighbor Information Acquisition also contains two messages (M_3 and M_4) exchanged between the X-Disco device and the Zigbee coordinator, as illustrated in Figure 1(b). Specifically, the X-Disco device uses the message M_3 to emulate an `IEEE_addr_req` packet, where the "NWKAddrOfInterest" is set to be the ZigBee coordinator's network address obtained in the ZigBee Coordinator Detection. After the X-Disco device transmits this emulated packet, the ZigBee coordinator responds with the corresponding `IEEE_addr_rsp` message, i.e., M_4, which is decoded via ZigBee Symbol Extraction by the X-Disco device. Then, X-Disco skips the first 42 symbols (all fields before "NumAssocDev") and obtains the number of the ZigBee neighbors from the 43rd to 44th symbols ("NumAssocDev" field). Eventually, the X-Disco device gets the network address of each ZigBee neighbor from 47th to the last symbol ("NWKAddr AssocDevList" field) in the packet, thereby completing the discovery of the ZigBee neighbors.

V. Advanced Features of X-Disco

In addition to the main design, X-Disco supports two advanced features for discovering the ZigBee neighbors in more generalized scenarios.

A. ZigBee Neighbor Validation

Sometimes, a ZigBee coordinator's associated device does not mean it is also the X-Disco device's neighbor. In other words, some of the discovered ZigBee neighbors might be the hidden terminals, as the X-Disco device might be out of these devices' coverage while they are still associated with the ZigBee coordinator. To address this situation, we leverage the Network Address and IEEE Address Conversion, which is also provided by the ZigBee Device and Service Discovery mechanism, to further validate the fetched ZigBee neighbor information. If "NWKAddrOfInterest" is the network address of the ZigBee device and "RequestType" is "0x00" in the `IEEE_addr_req` packet, as illustrated in Figure 13, only this specific ZigBee device would respond with the `IEEE_addr_rsp` packet, which contains its IEEE address in the "IEEEAddr RemoteDev" field. Given that observation, to validate if a specific ZigBee device is the X-Disco device's neighbor, the X-Disco device emulates an `IEEE_addr_req` with that specific ZigBee device's network address, obtained in Neighbor information Acquisition, and waits for a response.

That ZigBee device is a valid cross-technology neighbor if a `IEEE_addr_rsp` packet is captured by ZigBee Symbol Extraction; otherwise, not.

Another rare scenario for cross-technology neighbor discovery is an independent ZigBee device. Unlike WiFi devices, which associate and dissociate with WiFi routers frequently, it is very rare for the ZigBee devices not to associate with any ZigBee coordinators because the ZigBee devices are usually deployed in a network scale and set up manually. Therefore, X-Disco would detect the ZigBee neighbors in most of the scenarios, including smart homes and smart factories, thereby showing vast potential for wide deployment.

B. Interruption Mitigation

When we deploy X-Disco in the WiFi traffic intensive environment, the FFT magnitude collection is easily interrupted by ambient WiFi traffic. This is because the X-Disco device would switch back to the packet reception mode to start the decoding process if a WiFi packet arrives. To mitigate this interruption, we change the X-Disco device's center frequency to minimize the spectrum overlapped with ambient WiFi traffic. In specific, most 2.4GHz WiFi traffic, modulated by OFDM (802.11g and 802.11n) or CCK (802.11b), is on WiFi channels 1, 6, and 11. Such WiFi packets are so sensitive to the WiFi center frequency that even a 1MHz misalignment results in zero packet reception rate. According to our evaluation in Section VI-B, working on 2.425GHz, the X-Disco device effectively mitigates the interruption caused by the 802.11g/n (OFDM) and 802.11b (CCK) traffic.

VI. Evaluation

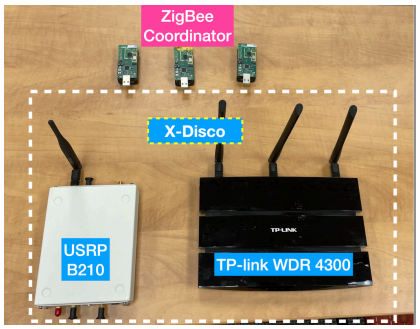
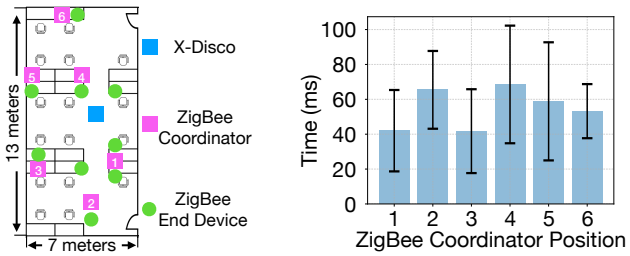


Fig. 14. Our system consists of X-Disco, implemented on USRP B210 (extracts FFT magnitude) and TP-link WDR 4300 (emulates ZigBee), and ZigBee coordinators, implemented on TelosB motes.

We build X-Disco on USRP B210 and TP-link WDR 4300 WiFi router, as illustrated in Figure 14. Implementing X-Disco on commodity WiFi devices is supported by the WiFi driver. We implement X-Disco in two parts for evaluation purposes. Specifically, we use a TP-link WiFi router to emulate the ZigBee broadcast packet and `IEEE_addr_req` packet while the USRP is for collecting FFT magnitudes of the received signal as WiFi Spectral Scan mode. Since our WiFi router does not support Spectral Scan mode, the FFT data collection is implemented at USRP. We also implement the ZigBee passive acknowledgement mechanism and `IEEE_addr_rsp` packets on TelosB motes. The primary metric to evaluate X-Disco is the time consumed for discovering all the ZigBee neighbors. We evaluate X-Disco in the office (None Line-of-sight) and the hallway (Line-of-sight). We also evaluate the advanced features of X-Disco in the office.

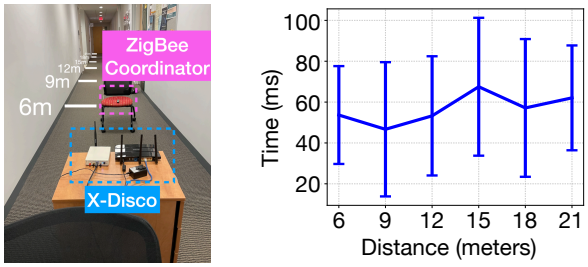
A. X-Disco Performance



(a) The NLoS Setting. (b) Performance in NLoS Scenario.

Fig. 15. Performance of discovering the ZigBee neighbors in N-LoS scenario.

As depicted in Figure 15(a), we deploy the ZigBee network in the office where eight TelosB motes marked in green circles work as the ZigBee end devices and one TelosB mote as the ZigBee coordinator is placed in six different positions for six experiments. The X-Disco device is working on 2.425GHz and all ZigBee devices are working on ZigBee channel 16 (2.43GHz). The detailed results are demonstrated in Figure 15(b). The average time to detect all nine ZigBee devices, including the ZigBee coordinator, is 42ms, 65.4ms, 41.7ms, 68.2ms, 59.2ms, and 53.7ms, when the ZigBee coordinator is placed at the positions 1 to 6. The reason the time varies for different positions is that when the ZigBee coordinator is placed at some positions (e.g., positions 2 and 4), the packet emulation does not work well since the emulated packets are sensitive to the low SNR and thus not successfully received, thereby resulting in more retransmission of emulated ZigBee packets until the response is triggered. Therefore, for those positions, X-Disco takes a longer time to obtain the ZigBee neighbor information.



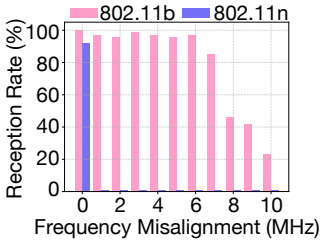
(a) The LoS Setting (b) Performance in LoS Scenario.

Fig. 16. We place the ZigBee coordinator at 6 to 21 meters from the X-Disco device in the Line-of-Sight Setting (a) and evaluate its performance over the distance (b).

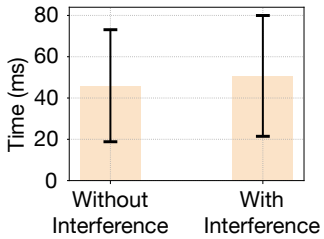
We also deploy the X-DISCO and ZigBee devices in the hallway for evaluating X-Disco in the Line-of-Sight (LoS) scenario, as illustrated in Figure 16(a), where we deploy the ZigBee coordinator at the distance of 6 to 21 meters with respect to X-Disco. Accordingly, the time consumed for fetching the neighbor information from the ZigBee coordinator is 53.7ms, 46.7ms, 53.3ms, 67.5ms, 57.1ms, and 62.1ms. In the LoS and NLoS experiments, we finish the neighbor

discovery within 70ms on average, showing the effectiveness and reliability of X-Disco.

B. Impact of WiFi traffic



(a) WiFi packet reception rate with different frequency misalignment.



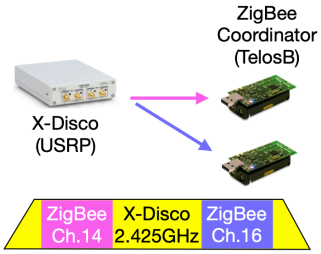
(b) Performance of X-Disco with and w/o help of interruption mitigation.

Fig. 17. Illustration of how WiFi traffic affect X-Disco.

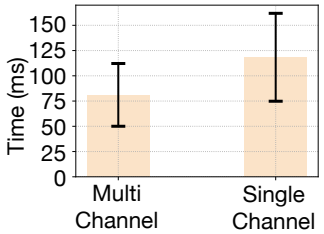
As we explained in Section V-B, we shift the center frequency of the X-Disco device to avoid the interruption caused by the ambient WiFi traffic. In this experiment, we place a WiFi transmitter and WiFi receiver at the distance of 1 meter working on the default transmission power (17dBm). We control the frequency misalignment by shifting the WiFi transmitter's center frequency by 1MHz at a time and checking the packet reception rate of the 802.11b (modulated by DBPSK) and 802.11n (modulated by OFDM) packets. As illustrated in Figure 17(a), the reception rate of 802.11n packets drops to near 0% with more than 1MHz frequency misalignment while the reception rate of 802.11b packets drops to 23% with 10MHz frequency misalignment. Therefore, we let the X-Disco device work on the 2.425GHz (middle of WiFi channels 1 and 6), which is supported by setting register "freq" [15] in ath9k driver, to avoid the interruption caused by WiFi traffic.

Based on this setting, we evaluate the performance of X-Disco with and without WiFi interference. In this experiment, we control a USRP to inject a WiFi 802.11b packet of 3.5ms every 10ms (35% channel occupation rate). As illustrated in Figure 17(b), the average time consumed to detect the ZigBee neighbors under WiFi interference is 50.1ms, which is only 4ms longer than the case without interference, indicating the effectiveness of our interruption mitigation design.

C. Multi-channel Discovery



(a) The X-Disco device discovers ZigBee neighbors on ZigBee channel 14 and 16 simultaneously.

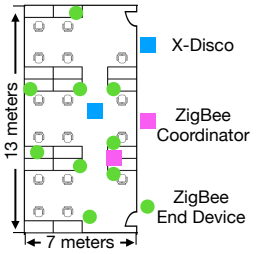


(b) Performance of X-Disco with (Multi Channel) and without (Single Channel) Multi-channel Discovery.

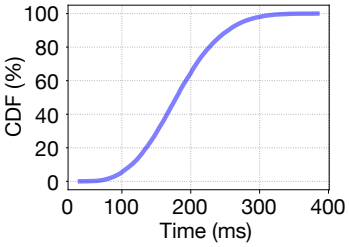
Fig. 18. Performance of X-Disco Multi-channel Discovery.

As depicted in Figure 18(a), in this experiment, we control the X-Disco device (2.425GHz) to discover the ZigBee neighbors on two ZigBee channels simultaneously. The X-Disco device emulates ZigBee broadcast packets on ZigBee channels 14 (2.42GHz) and 16 (2.43GHz), where each channel contains 9 ZigBee neighbors, via CTC [11]. Correspondingly, the FFT magnitudes capture the rebroadcasted ZigBee packets on these two channels in the subcarriers 12-19 and subcarriers 45-52, from which the ZigBee network information is extracted via ZigBee symbol extraction. Then, X-Disco emulates `IEEE_addr_req` messages on two channels and acquires the ZigBee neighbor information from the responded `IEEE_addr_rsp` packets accordingly. The distance between the X-Disco device and ZigBee coordinators is 6 meters. With multi-channel discovery, the time consumed to discover all 18 ZigBee neighbors on two channels is 79.2ms, as illustrated in Figure 18(b). In contrast, without the help of multi-channel discovery, the X-Disco device has to discover the ZigBee neighbors on channel 14 and then switches center frequency to discover the rest Zigbee neighbors on ZigBee channel 16, which costs 119.3ms on average.

D. ZigBee Neighbor Validation



(a) The setting of ZigBee neighbor validation.

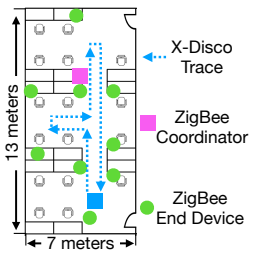


(b) CDF of time consumed for ZigBee neighbor validation.

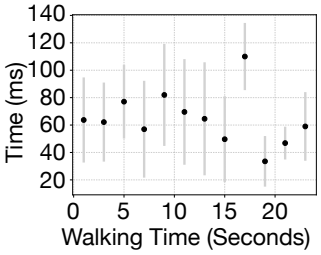
Fig. 19. We deploy X-Disco in office to evaluate the effectiveness of ZigBee neighbor validation.

To show the performance of ZigBee neighbor validation, we deploy a ZigBee network of 9 ZigBee devices in the office, as depicted in Figure 19(a). After the X-Disco device obtains the ZigBee neighbor information, it validates the neighbor one by one. We run the experiments 200 times and record the total time to discover and validate all 9 ZigBee neighbors. The detailed results are shown in Figure 19(b), where all neighbors are validated within 177ms in the 50% of experiments and all validations are finished within 382ms.

E. Mobile



(a) The mobile trace.



(b) Performance in mobile scenario.

Fig. 20. We evaluate X-Disco as walking in the office.

We also evaluate X-disco in the mobile scenario, as depicted in Figure 20(a). As we walk along the blue dotted trace with the X-Disco device at the speed of 1m/s, the X-Disco device keeps discovering the ambient ZigBee neighbors. The whole walk takes 23 seconds and the average time to discover all ZigBee neighbors is 63.7ms, 62.2ms, 77.1ms, 57ms, 82ms, 69.6ms, 64.6ms, 49.7ms, 110ms, 33.5ms, 46.8ms, and 59ms over the time, as shown in Figure 20(b).

VII. Related Work

Neighbor discovery has been widely studied in ad-hoc networks [22]. Nevertheless, in a more practical scenario, involving heterogeneous wireless technologies, the requirement of direct communication is not satisfied. We note that the recently proposed cross-technology communication designs [11], [15], [23] help a commodity WiFi device to transmit a message to a ZigBee device directly.

Based on CTC, many works improve the performance of channel coordination [5] and cooperation [7]. Two papers [10], [24] claim they focus on the cross-technology neighbors discovery. However, applying the WiFi to ZigBee CTC to assist ZigBee devices in detecting ZigBee neighbors, NewBee [24] is still for discovering homogeneous wireless neighbors. SERVOUS [10] is using ZigBee device to detect BLE neighbors while it requires modification at both ZigBee and BLE sides, incurring unaffordable costs at deploying that design into practice. Compared to SERVOUS, X-Disco is transparent to the ZigBee network, at the zero cost for installing X-Disco to the WiFi device without any modification to the existing ZigBee devices and ZigBee network.

X-Disco leverages the WiFi to ZigBee high-throughput CTC [11] to emulate ZigBee packets at commodity WiFi. For decoding the responded ZigBee packets at commodity WiFi, X-Disco utilizes the WiFi Spectral Scan mode to extract the FFT magnitude. Even though SymBee [23] and LEGO-Fi [25] are able to decode ZigBee packets at WiFi device, these designs require significant modification to WiFi PHY layer. Given the cross-technology neighbor information fetched by X-Disco, we are able to avoid the cross-technology interference [5] , demonstrating the tremendous applications of X-Disco in the future.

VIII. Conclusion

In this paper, we present X-Disco to enable a WiFi device to detect the ambient ZigBee neighbors. We demonstrate the feasibility that a commodity WiFi device is capable of decoding the ZigBee packets just using the FFT magnitude extracted from WiFi Spectral Scan. Based on that, we complete X-Disco for a commodity WiFi device to fetch the ZigBee neighbor information from the ambient ZigBee coordinators. Evaluated in the office (LoS and NLoS), X-Disco discovers nine ZigBee neighbors within 70ms, demonstrating its efficacy in discovering the cross-technology neighbors. More experiments for validating X-Disco's enhanced features and performance in mobile scenarios are performed to show the potential to deploy X-Disco into practice.

References

[1] "Zigbee increasingly dominating the world of IoT, https://www.develcoproducts.com/blog/zigbee-increasingly-dominating-the-world-of-iot/."

[2] "Global Wi-Fi Enabled Devices Shipment Forecast, 2020-2024., https://www.researchandmarkets.com/reports/5135535/global-wi-fi-enabled-devices-shipment-forecast."

[3] S. M. Kim and T. He, "Freebee: Cross-technology communication via free side-channel," in *Proceedings of the 21st MobiCom*. ACM, 2015, pp. 317–330.

[4] C.-J. M. Liang, N. B. Priyantha, J. Liu, and A. Terzis, "Surviving wi-fi interference in low power zigbee networks," in *Proceedings of the 8th ACM SenSys*, 2010, pp. 309–322.

[5] Z. Yin, Z. Li, S. M. Kim, and T. He, "Explicit channel coordination via cross-technology communication," in *Proceedings of the 16th MobiSys*, 2018, pp. 178–190.

[6] Y. Chae, S. Wang, and S. M. Kim, "Exploiting wifi guard band for safeguarded zigbee," in *Proceedings of the 16th SenSys*, 2018, pp. 172–184.

[7] W. Chen, Z. Yin, and T. He, "Global cooperation for heterogeneous networks," in *IEEE INFOCOM 2020*. IEEE, 2020, pp. 1014–1023.

[8] Z. Alliance, "ZigBee Specification, https://zigbeealliance.org/wp-content/uploads/2019/11/docs-05-3474-21-0csg-zigbee-specification.pdf," 2005.

[9] R. Cohen and B. Kapchits, "Continuous neighbor discovery in asynchronous sensor networks," *IEEE/ACM Transactions on Networking*, vol. 19, no. 1, pp. 69–79, 2010.

[10] R. Hofmann, C. A. Boano, and K. Römer, "Servous: Cross-technology neighbour discovery and rendezvous for low-power wireless devices." in *EWSN*, 2021, pp. 151–162.

[11] Z. Li and T. He, "Webee: Physical-layer cross-technology communication via emulation," in *Proceedings of the 23rd MobiCom*, 2017, pp. 2–14.

[12] "Intriguing Amazon Alexa Statistics You Need to Know in 2022, https://safeatlast.co/blog/amazon-alexa-statistics/#gref."

[13] B. Chen, J. Wan, L. Shu, P. Li, M. Mukherjee, and B. Yin, "Smart factory of industry 4.0: Key technologies, application case, and challenges," *Ieee Access*, vol. 6, pp. 6505–6519, 2017.

[14] R. Liu, Z. Yin, Jiang, and T. He, "Wibeacon: expanding ble location-based services via wifi," in *Proceedings of the 27th annual international conference on mobile computing and networking*, 2021, pp. 83–96.

[15] S. Wang, W. Jeong, J. Jung, and S. M. Kim, "X-mimo: Cross-technology multi-user mimo," in *Proceedings of the 18th Conference on Embedded Networked Sensor Systems*, 2020, pp. 218–231.

[16] X. Guo, Y. He, X. Zheng, L. Yu, and O. Gnawali, "Zigfi: Harnessing channel state information for cross-technology communication," *IEEE/ACM Transactions on Networking*, vol. 28, no. 1, pp. 301–311, 2020.

[17] S. Rayanchu, A. Patro, and S. Banerjee, "Airshark: detecting non-wifi rf devices using commodity wifi hardware," in *Proceedings of the IMC*, 2011, pp. 137–154.

[18] Z. Li and Y. Chen, "Bluefi: Physical-layer cross-technology communication from bluetooth to wifi," in *40th ICDCS*. IEEE, 2020, pp. 399–409.

[19] "ath9k spectral scan, https://wireless.wiki.kernel.org/en/users/drivers/ath9k/spectral_scan."

[20] "An open-source software using ath11k driver., https://github.com/simonwunderlich/fft_eval."

[21] "IEEE 802.15.4 Protocol," http://standards.ieee.org/getieee802/download/802.15.4-2015.pdf.

[22] M. J. McGlynn and S. A. Borbash, "Birthday protocols for low energy deployment and flexible neighbor discovery in ad hoc wireless networks," in *Proceedings of the 2nd ACM MobiHoc*, 2001, pp. 137–145.

[23] S. Wang, S. M. Kim, and T. He, "Symbol-level cross-technology communication via payload encoding," in *2018 IEEE 38th ICDCS*. IEEE, 2018, pp. 500–510.

[24] D. Gao, Z. Li, Y. Liu, and T. He, "Neighbor discovery based on cross-technology communication for mobile applications," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 10, pp. 11 179–11 191, 2020.

[25] X. Guo, Y. He, X. Zheng, Z. Yu, and Y. Liu, "Lego-fi: Transmitter-transparent ctc with cross-demapping," *IEEE Internet of Things Journal*, vol. 8, no. 8, pp. 6665–6676, 2021.