Demo Abstract : Safeguarded ZigBee via WiFi Guard Band

Yoon Chae
Department of Computer Science,
George Mason University
ychae2@gmu.edu

Song Min Kim
Department of Computer Science,
George Mason University
song@gmu.edu

ABSTRACT

Low power IoT suffers from performance degradation due to severe cross-technology interference (CTI) such as WiFi. In this demo, we present a novel ZigBee system that effectively maintains high reliability even under saturated WiFi traffic. This is achieved by placing a ZigBee packet on the guard band of ongoing, ambient WiFi traffic. Guard band is designed to be kept clear of interference from other WiFi, thereby *safeguarding* the ZigBee within. Our system effectively captures WiFi (802.11b) guard band on the fly, using physical layer information accessible on commodity ZigBee RF. We demonstrate real-time guard band detection and robust ZigBee communication, showcasing a practical pathway to operating low power IoT under excessive CTI.

CCS CONCEPTS

• **Computer systems organization** → **Sensor networks**; • **Networks** → *Wireless personal area networks*;

KEYWORDS

Guard band, Cross-technology interference, ZigBee, WiFi

ACM Reference Format:
Yoon Chae and Song Min Kim. 2018. Demo Abstract : Safeguarded ZigBee via WiFi Guard Band. In *SenSys '18: Conference on Embedded Networked Sensor Systems, November 4–7, 2018, Shenzhen, China.* ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/3274783.3275180

1 INTRODUCTION

The rapid growth of the wireless body has led to severe cross-technology interference (CTI) in the 2.4GHz ISM band [4]. To tackle this, recent studies [2, 3] explore the traffic pattern and exploit the channel idle time for communication reliability. Among them, WISE [3] leverages long idle time following the WiFi burst traffic, due to exponential backoff. TIIM [2] uses machine learning based on idle time prediction. These techniques commonly adopt statistical models, inherently suffering from uncertainties (thus performance unreliability) of CTI dynamics that inevitably occur in practice, including varying traffic and user.

In this demo, we present a unique design that enables highly robust ZigBee operation naturally immune from underlying CTI dynamics. As depicted in Figure 1, by placing 2MHz ZigBee signal within the 3-5MHz WiFi guard band, ZigBee packets are essentially *safeguarded* from other WiFi in proximity. Unlike state-of-the-art designs, our technique *deterministically* identifies the idle channel (i.e., the guard band) by observing the duration and the channel of the WiFi traffic – thus achieving high reliability under CTI uncertainty.

Figure 1: Our system places ZigBee transmission (red) in the guard band of ongoing ambient WiFi (blue). This essentially safeguards ZigBee from the WiFi interference, as WiFi devices in proximity back off as per CSMA.

The system exploits physical layer information (i.e., I/Q) accessible in recent commodity ZigBee radio chips, to directly interpret WiFi (802.11b) packet header. The guard band duration obtained from the packet header strictly determines the available ZigBee packet length that can be protected by the guard band. The system is carefully designed to minimize computational overhead and energy consumption under the small budget of low-end ZigBee devices.

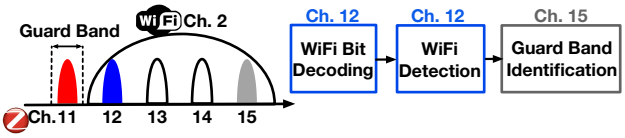


Figure 2: (left) Safeguarded ZigBee on channel 11 sits in the guard band of WiFi channel 2. (right) The guard band is captured by the three, light-weight steps.

2 SYSTEM DESIGN

Here we discuss the three core technical elements of our system: WiFi bit decoding, detection, and guard band identification, followed by the safeguarded transmission.

WiFi Bit Decoding. The key technique of our design is interpreting 802.11b WiFi signal with 22MHz bandwidth using ZigBee receiver limited to 2MHz. As shown in Figure 2, WiFi bit decoding is the first step to achieve the safeguarded ZigBee. The WiFi signal

SenSys '18, November 4–7, 2018, Shenzhen, China

ACM ISBN 978-1-4503-5952-8/18/11.
https://doi.org/10.1145/3274783.3275180

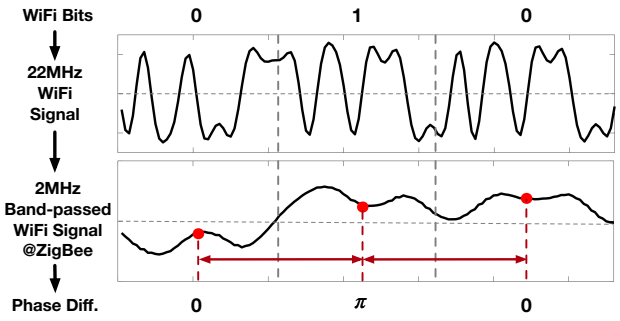


Figure 3: WiFi bits '1' and '0' are projected to phase differences 'π' and '0' at the ZigBee receiver, respectively.

flows into the ZigBee RF front-end and passes through the 2MHz low pass filter (LPF), leaving only low frequency components. Physical layer samples (i.e., I/Q) are collected at 1MHz sampling rate at ZigBee channel 12, which is the leftmost channel overlapping with the WiFi channel that yields the guard band of interest. Figure 3 illustrates that the phase difference directly indicates WiFi bits. Specifically, 'π' and '0' phase differences indicate WiFi bits '1' and '0', respectively. From this, our system is able to interpret WiFi signal.

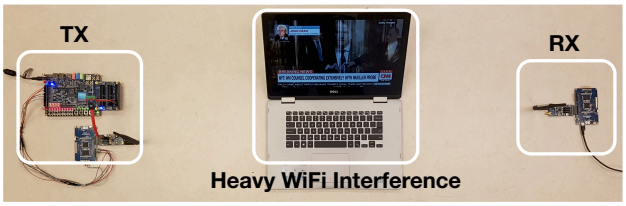
WiFi Detection. WiFi packet detection is based on the aforementioned WiFi decoding technique. That is, WiFi packets are captured by comparing the decoded input bit with the unique pattern of the WiFi preamble bits. To accomplish this in an efficient manner, our design matches 38-bit subset of the WiFi preamble, where the subset is carefully chosen so that it not only enables extremely lightweight computation of O(1) [1], but also achieves high reliability of under 3.6×10^{-10}% false positive and 4.3% false negative rates, respectively.

Guard Band Identification. The frequency (i.e., ZigBee channel) and duration of the guard band are retrieved from the channel and length of the WiFi packet. Among them, the WiFi channel is found by observing the leftmost and rightmost ZigBee channels overlapping with the WiFi channel. WiFi packet length is directly decoded from the WiFi packet header. From this, our design properly sets the length and the channel of the ZigBee packet.

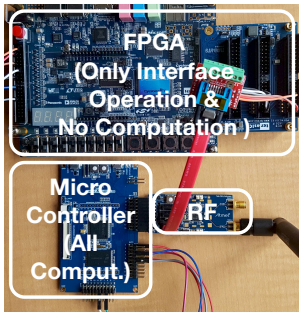
3 DEMONSTRATION

This section discusses the demonstration plan showing the safeguarded ZigBee communication under saturated interference environment. The demonstration video is available at https://youtu.be/B8guFNCw2Ns. Figure 4b shows the implementation of our system using three commercial off-the-shelf devices: (i) ZigBee RF front-end (AT86RF215), (ii) Microcontroller (SAM4SD32C), and (iii) FPGA (Cyclone V). The I/Q samples provided from the RF front-end are sent to the microcontroller, where the FPGA serves as the interface converter between the two. That is, the FPGA is not involved in any computation – the entire steps in Section 2 are performed only within the microcontroller, showing the feasibility of the design on low-end IoT devices.

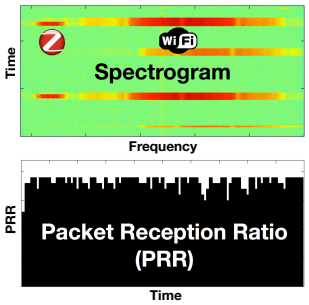
Figure 4a shows the demonstration setup. ZigBee sender (TX) and receiver (RX) pair are installed on the table, where the sender



(a) Demonstration Setting (top view)



(b) Testbed



(c) Real-time Performance

Figure 4: (a) ZigBee communication reliability under heavy WiFi traffic (PC playing YouTube video) is demonstrated. (b) Our system consists of three off-the-shelf components. (c) Spectrogram and PRR are shown for visual demonstration of the system's real-time operation and performance.

runs our design and the receiver is a legacy ZigBee. We also place a laptop nearby playing high-quality video clip on YouTube, generating heavy WiFi interference. The TX node detects ambient 802.11b packets in the air and transmits the packet over WiFi guard bands. As shown in Figure 4c, two monitors display the real-time operation of our design, through spectrogram and packet reception ratio (PRR) of the ZigBee packets. A USRP (set under the table) is used to show the spectrogram, which reflects the radio activities around the guard band and the corresponding WiFi channel. This visually demonstrates that our system indeed successfully locates the ZigBee packet within the WiFi guard band. The PRR validates that the system safeguards ZigBee communication and ensures reliability.

ACKNOWLEDGMENTS

We sincerely thank the anonymous reviewers for their valuable comments and suggestions. This work was supported in part by US NSF Grant CNS-1717059.

REFERENCES

[1] Yoon Chae, Shuai Wang, and Song Min Kim. 2018. Exploiting WiFi Guard Band for Safeguarded ZigBee. In *SenSys '18 Proceedings of the 16th ACM Conference on Embedded Network Sensor Systems*. ACM.

[2] Anwar Hithnawi, Hossein Shafagh, and Simon Duquennoy. 2015. TIIM: technology-independent interference mitigation for low-power wireless networks. In *Proceedings of the 14th International Conference on Information Processing in Sensor Networks*. ACM, 1–12.

[3] Jun Huang, Guoliang Xing, Gang Zhou, and Ruogu Zhou. 2010. Beyond co-existence: Exploiting WiFi white space for Zigbee performance assurance. In *Network Protocols (ICNP), 2010 18th IEEE International Conference on*. IEEE.

[4] Chieh-Jan Mike Liang, Nissanka Bodhi Priyantha, Jie Liu, and Andreas Terzis. 2010. Surviving wi-fi interference in low power zigbee networks. In *Proceedings of the 8th ACM Conference on Embedded Networked Sensor Systems*. ACM, 309–322.