Poster Abstract: Exploiting Physical Layer Information to Mitigate Cross-Technology Interference Effects on Low-Power Wireless Networks

Anwar Hithnawi
Institute for Pervasive Computing
ETH Zurich
hithnawi@inf.ethz.ch

ABSTRACT

The proliferation of a wide range of wireless devices operating in the crowded 2.4 GHz ISM band is becoming a major challenge for emerging low-power wireless networks in indoor applications. Recent studies show that *Cross Technology Interference* (CTI) can significantly reduce the overall delivery ratio of such networks. CTI subsequently decreases the network performance and drains their scarce resources of radio spectrum and energy. In this work, we present the design and preliminary evaluation results of an energy-efficient packet recovery mechanism that exploits (i) physical layer information available by 802.15.4-compliant radios and (ii) time diversity of wireless channel, to mitigate cross technology interference effects on low-power wireless networks.

1. INTRODUCTION

Cross Technology Interference (CTI), a consequence of frequency overlap of different technologies operating in the same RF spectrum, is emerging as major problem for the performance of 802.15.4 networks which transmit at the relatively low power. Low-power wireless networks are subject to intrusive transmissions from high-power interference sources, such as microwave ovens, cordless phones and baby monitors, and low-power interference sources, such as IEEE 802.11 and bluetooth. Classical approaches to mitigate the impact of interference tend to hop away to interference free channels. However, technologies operating in the ISM band differ in the width of occupied sub-bands (see Fig. 1), the regularity, and time duration of accessing the ISM frequency spectrum. In this paper, we depart from classical mitigation approaches that are typically customized for a certain CTI source and require knowledge of the interference source to boost network performance. Instead, we focus on a general mitigation approach that allows for stable performance independent of the particular interference patterns of the interferer. It is based on a packet recovery mechanism that aims at minimizing the number of retransmissions by exploiting partially correctly received bits within the interfered frames. In our work, we first examine the interference patterns induced on 802.15.4 receivers by three prominent technologies operating in the 2.4 GHz ISM band. The presence of interference introduces a temporary increase in the received signal strength which can be quantified and correlated to the error bursts introduced by the interference source. Given these observations, we propose a packet recovery mechanism to mitigate the impact of CTI on low-power networks.

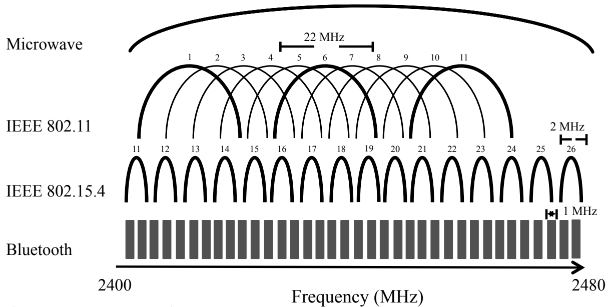

Figure 1: Microwave oven, IEEE 802.11, IEEE 802.15.4 and bluetooth RF channels in the 2.4 GHz ISM band.

2. BACKGROUND AND RELATED WORK

Transmission over wireless links is susceptible to various sources of distortions which can result in bit-errors and packet losses. Classical link-layer reliability mechanisms, such as channel coding and *Automatic Repeat reQuest* (ARQ), were designed to recover from time-variable error conditions, where errors are characterized by being randomly distributed over the transmitted data. Errors due to interference are, on the other hand, characterized by being bursty [2]. Hence, distortions can affect multiple consecutive bytes which is beyond the recovery capabilities of most lightweight FEC protocols. Furthermore, classical ARQ protocols are inefficient in the presence of an active interference source, as an immediate retransmission is most likely disturbed by the same source of interference. Hence, research in interference mitigation has refocused from link-layer reliability mechanisms to rely on active spectrum sampling. Liang et al. [1] and Hauer et al. [3] propose link-layer-based approaches to improve the delivery rate in low-power wireless networks exposed to WiFi interference. Liang et al. suggest the use of cyclic error-correcting codes to help decoding corrupted packet payloads. This approach may not be efficient for other interference sources, such as bluetooth and microwave which introduce long error bursts. Our approach is inspired by Hauer et al. work, which correlates WiFi traffic to the positioning of bit-errors. We generalize this concept to mitigate CTI and propose a new recovery mechanism. Furthermore, our approach differs from these approaches by not being customized to a certain interference pattern. Moreover, it is compatible to existing link-layer protocols and does not

SenSys'13, Nov 11-15, 2013, Rome, Italy
ACM 978-1-4503-2027-6/13/11.

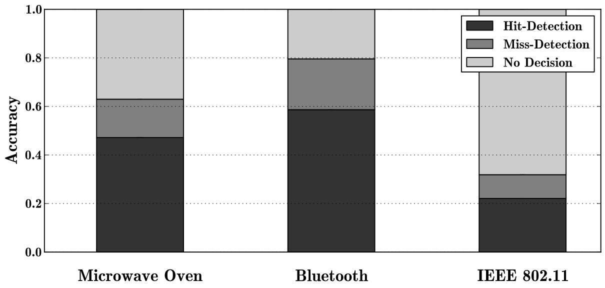

Figure 2: Accuracy of the error-burst detection algorithm with the presence of bluetooth, microwave oven and IEEE 802.11 interference.

introduce overhead to interference free communication as it is triggered upon detection of interference.

3. PRELIMINARY DESIGN AND EVALUATION

Basic design: Our recovery mechanism operates in two modes, passive and recovery. Having two modes allows to avoid imposing additional computational overhead to the interference free communication. The system runs mainly in the passive mode which monitors the *Link Quality Indication* (LQI) value of corrupted frames to detect interference using a simple threshold mechanism. Upon detection of interference, the system switches to recovery mode where for each received frame, we capture RSSI changes by sampling the received signal at a frequency of 30 kHz, roughly at one byte of granularity. The sampled RSSI readings are then fed to the detection algorithm, which localizes error bursts within the frame. The correctly decoded bytes are buffered and used to reconstruct the original frame from a subsequent interfered retransmission. The design of the error-burst detection algorithm is based on the following observations of CTI patterns on low-power wireless links: *(i)* radio interference introduces a temporary increase in the RSSI that can be quantified; *(ii)* coherence time of low-power wireless links is longer than the transmission time of a maximum 802.15.4 frame. The RSSI is stable with an average standard deviation less than 1 dBm for links without bursts [4]; *(iii)* weak links are characterized by stable RSSI near the cusp of reception sensitivity, consequently slight variations can cause packet losses [4]; *(iv)* error bursts can be projected to RSSI variations by marking the corresponding byte of surging RSSI reading. For a given packet and its sampled $RSSI_{[0..n]}$ values, we mark $Byte_i$ as a corrupted byte if $RSSI_i - RSSI_{min} > threshold$. Hereby, we define the *threshold* as the maximum RSSI range of intermediate links in a short time; *(v)* a safety margin of one byte at the edges (start/end) of detected bursts is marked as corrupted. This is due to possible delays associated with accessing the radio registers over the SPI bus; *(vi)* the majority of bytes within an interfered packet are correct but discarded due to the bit-by-bit correct transmission enforcement by CRC (see Fig. 3).

Preliminary evaluation: For the preliminary evaluation, we analyzed interference patterns on 802.15.4 frames using traces from the SoNIC project [2]. The log traces cover the impact of cross technology interference from microwave oven, bluetooth, and IEEE 802.11. The traces are collected in an anechoic chamber to study interference patterns in a controlled environment. The log traces capture RSSI variations at a rate of 30 kHz. We evaluated the detection algorithm and compared the result with ground truth data. We count hit-detection in case of correct detection or false positive. Otherwise, we count a miss-detection. Fig. 2 depicts the performance of the detection algorithm where overall links are considered for each of the CTI sources. Fig. 3 highlights the percentage of correctly decoded bytes after applying the detection algorithm. Correctly detected bytes from the corrupted frames are added to correctly received bytes and depicted as useful bytes. With the presence of microwave and bluetooth interference, respectively 41% and 40% of the correctly received bits within CRC-failed frames are correctly decoded. For WiFi, 17% of the data is correctly decoded. In the considered traces, WiFi source traffic saturates the channel. Thus, this represents the worst case scenario.

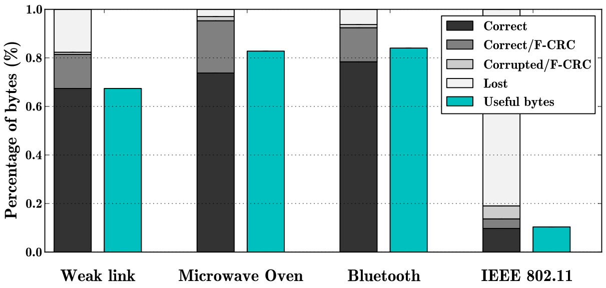

Figure 3: Percentage of bytes within 802.15.4 packets correctly received, correct within failed-CRC packet, corrupted within failed-CRC packet, and lost. Percentage of correctly decoded bytes after applying error-burst detection algorithm depicted as useful bytes.

4. SUMMARY AND FUTURE WORK

In this paper, we present a lightweight packet recovery mechanism that increases loss resilience in low-power wireless networks in presence of CTI, by exploiting observed variations of the RSSI readings at reception time from the physical-layer to reconstruct corrupted packets. Motivated by initial results we outline our future work by: *(i)* thoroughly evaluating the recovery mechanism in uncontrolled environments with presence of various interference sources. *(ii)* evaluating the impact of the recovery mechanism for different prominent low-power MAC protocols.

5. REFERENCES

[1] C. Liang, N. Priyantha, J. Liu, A. Terzis. Surviving Wi-Fi Interference in low Power ZigBee Networks. In *ACM SenSys*, pages 309–322, 2010.

[2] F. Hermans, O. Rensfelt, T. Voigt, E. Ngai, L. Norden, P. Gunningberg. SoNIC: Classifying Interference in 802.15.4 Sensor Networks. In *ACM/IEEE IPSN*, pages 55–66, 2013.

[3] J. Hauer, A. Willig, A. Wolisz. Mitigating the Effects of RF Interference through RSSI-Based Error Recovery. In *Springer-Verlag EWSN*, pages 224–239, 2010.

[4] K. Srinivasan, M. Kazandjieva, and S. Agarwal, P. Levis. The β-factor: Measuring Wireless Link Burstiness. In *ACM SenSys*, pages 29–42, 2008.