Understanding the Impact of Cross Technology Interference on IEEE 802.15.4

Anwar Hithnawi, Hossein Shafagh
Department of Computer Science
ETH Zurich, Switzerland
{hithnawi, shafagh}@inf.ethz.ch

Simon Duquennoy
SICS Swedish ICT AB
Kista, Sweden
simonduq@sics.se

ABSTRACT

Over the last few decades, we witnessed notable progress in wireless communication. This has led to rapid emergence of heterogeneous wireless technologies that share the RF spectrum in an un-coordinated way. Such a coexistence introduces high uncertainty and complexity to the medium, affecting reliability and availability of wireless networks. This problem aggravates for technologies operating in the lightly regulated, yet crowded ISM bands. To address coexistence of different technologies in the scarce RF spectrum, provide proper interference-aware protocols, and mitigation schemes, we need to develop a good understanding of the interaction patterns of these technologies. In this paper, we provide a thorough study of the implications of Cross Technology Interference (CTI) on the particularly vulnerable low-power IEEE 802.15.4 wireless networks. We identify the underlying vulnerabilities that hamper 802.15.4 to withstand CTI. We show that the uncertainty that CTI induces on the wireless channel is not completely stochastic; CTI exhibits distinct patterns that can be exploited by interference-aware protocols.

Categories and Subject Descriptors

C.2.1 [**Computer-Communication Networks**]: Network Architecture and Design—*Wireless communication*

Keywords

IEEE 802.15.4; Cross Technology Interference; Low-power Wireless Communication

1. INTRODUCTION

Over the last few years, there has been a surge on the number of new wireless devices being used [2]. The wireless medium, through its promises of ubiquity, mobility, and connectivity, fosters an increasing demand for integrating wireless interfaces to appliances. The resulting coexistence leads to spectrum exhaustion, which translates into reliability and connectivity issues. This problem aggravates for technologies operating in the lightly regulated, yet crowded unlicensed ISM bands. The ISM bands proliferate with heterogeneous devices including WiFi (IEEE 802.11), Bluetooth, 2.4 GHz cordless phones, microwave ovens, surveillance cameras, game controllers[1], and 2.4 GHz RFID. These technologies differ widely in terms of emitted power levels, persistence in accessing the wireless medium, and in the width of occupied sub-bands, as illustrated in Figure 1.

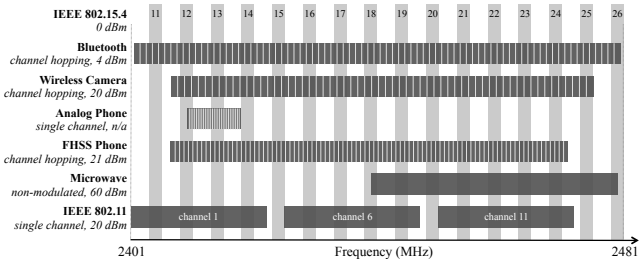


Figure 1: RF channels of IEEE 802.15.4 and the set of prevalent RF interferers in the 2.4 GHz ISM band studied in this paper.

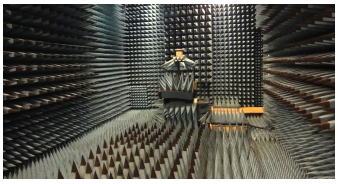
At the same time, low-power wireless communication is taking its momentum as the key technical driver for applications such as healthcare systems, smart environments, home automation, monitoring and tracking, and the *Internet of Things* (IoT). Many of these applications expect underlying wireless networks to be reliable and fast, yet require devices to be battery-based and have energy efficiency as a priority. This implies lower radio transmission power, which hampers low-power wireless communication devices to withstand RF interference.

Our goal in this work is to develop a detailed understanding of the interaction between IEEE 802.15.4 and a set of prevalent RF interferers and to recognize the key factors to the harmful coexistence of these technologies. We expose a 802.15.4 network consisting of a pair of 802.15.4 nodes in a controlled environment to a set of RF interferers. We focus on a set of RF technologies that are pervasive in indoor environments: IEEE 802.15.1 (Bluetooth), wireless surveillance cameras such as baby monitors, analog and FHSS cordless phones, microwave ovens, and IEEE 802.11 (WiFi). The set of considered interferers are selected to represent common underlying properties adopted by most of the nowadays used wireless devices. Our considered set consists of low/high power interferers, narrow/wide band interferers,

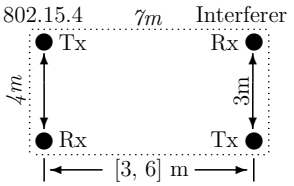
[1]For example, the Xbox 360 S wireless controller.

ACM WiNTECH '14 Maui, Hawaii USA

http://dx.doi.org/10.1145/2643230.2643235.



(a) Anechoic room



(b) Setup

Figure 2: Experiment setup for the CTI impact study in an anechoic room.

analog/digital interferers, channel hopping/fixed frequency interferers, CSMA and non-CSMA interferers. We intend to empirically recognize the interference impact and patterns given the presence of different wireless communication paradigms. We analyze the impact of CTI on 802.15.4 at different layers: *(a)* Physical layer: investigation of characteristics captured from off-the-shelf 802.15.4 radio chips, through fast RSSI sampling and other indicators; *(b)* MAC layer: effects on Clear Channel Assessment and CSMA backoff; *(c)* Upper layers payload: study of features such as error patterns, error bursts, and interspaces between consecutive errors. We make the collected traces for our CTI study of more than 2.3 million transmitted packets publicly available[2] to the research community for further investigations.

Our results show how different technologies affect 802.15.4 distinctly in aspects such as corruption rate, backoff mechanism, position of corrupted symbols, etc. This knowledge can be exploited by interference mitigation mechanisms for a better resilience against CTI. This is an essential step towards enabling reliable low-power wireless networks to coexist in the shared spectrum.

The remainder of this paper is structured as follows: Section 2 briefly reviews IEEE 802.15.4. Section 3 describes our experiment setup and configurations. Section 4 discusses the impact of interaction between high/low-power interferers and 802.15.4 networks. The CTI patterns induced on the wireless channel and data transmitted over the interfered channels are explained in Section 5. Section 6 presents related work on mitigating and studying the impact of CTI. We conclude this study in Section 7.

2. IEEE 802.15.4 BACKGROUND

We briefly review relevant aspects of the IEEE 802.15.4 standard to our work.

IEEE 802.15.4 CSMA/CA: Similar to 802.11, most of 802.15.4 nodes employ contention-based CSMA/CA MAC. Nodes can apply different adaptation of radio duty cycling on top of CSMA/CA to increase energy efficiency. Once a node has a packet to transmit, it enters the transmission mode. It waits for a random back-off period to assure that the channel is free. For this, it relies on *Clear Channel Assessment* (CCA). The determination of CCA considers *Energy Detection* (ED) or/and detection of 802.15.4 modulated signal in the channel. If CCA declares the channel to be free, the transmission is carried out, otherwise it defers the transmission for a random backoff time. The successful reception of a data packet, i.e., it passes the CRC check, is confirmed through an explicit ACK frame from the receiver.

IEEE 802.15.4 modulation and spreading:

[2]CTI study traces collected in anechoic room: `http://www.inf.ethz.ch/~hanwar/CTI_Study_Traces/`

RF Technology	Abbr.	TX Power (dBm)	Bandwidth (MHz)
IEEE 802.15.4	–	0	2
Bluetooth (Class 2)	BL	4	1 (FH)
Wireless Camera	CAM	20	1.125 (FH)
Analog Phone	AN-P	n/a	0.1
FHSS Phone	FH-P	21	0.8 (FH)
Microwave Oven	MW	60	-
IEEE 802.11	WiFi	20	20

Table 1: Characteristics of considered RF technologies in our study.

For devices operating in the 2.4 GHz band, the IEEE 802.15.4 standard [5] defines the *Offset Quadrature Phase-Shift Keying* (O-QPSK) modulation scheme with a half pulse shaping. In order to increase the resistance against noise, *Direct-Sequence Spread Sequence* (DSSS) is employed. The transmitter's radio transforms binary data to modulated analog signals by adapting spreading and modulation. The data is first grouped in 4-bit symbols, which are mapped to one of the 16 *Pseudo-random Noise* (PN) sequences that are 32-bit long. Each bit in a PN sequence is referred to as a chip, which is then modulated to the carrier signal using O-QPSK.

For demodulation, the receiver's radio converts each half-sine pulse signal into a chip. The radio performs soft decisions at the chip level, providing PN sequences with non-binary values ranging from 0 to 1 [4]. The de-spreading is performed by mapping the PN sequence to the symbol with the highest correlation. The redundancy induced by spreading allows correct decoding of the received symbol, even if few chips were not correctly decoded which increases the immunity to noise.

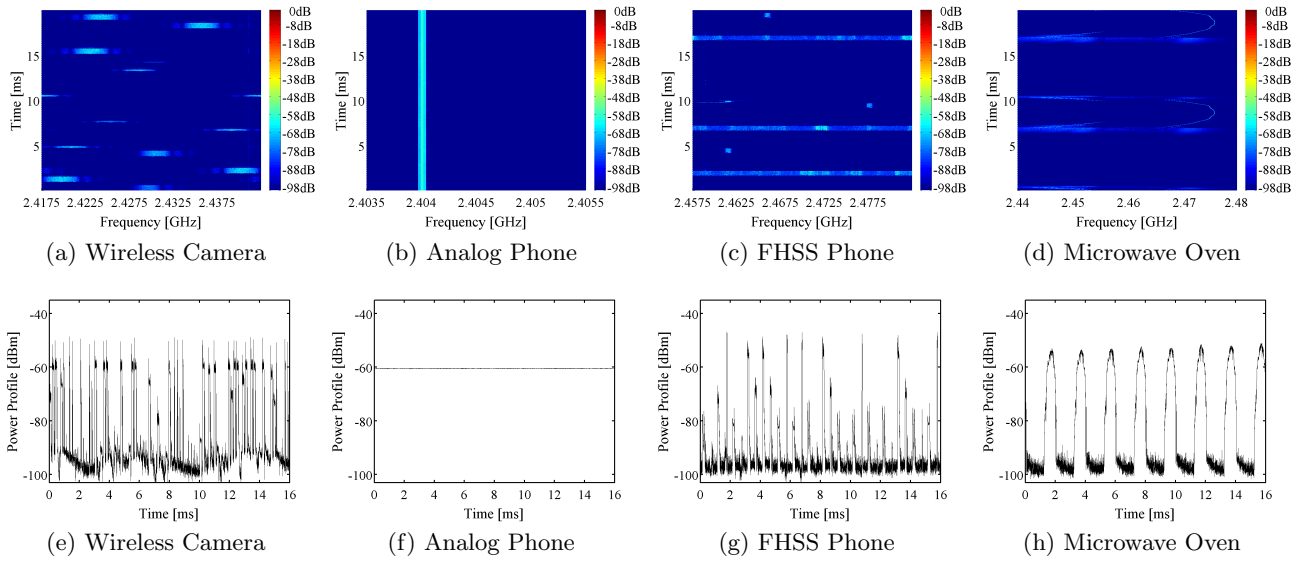
IEEE 802.15.4 channels: 802.15.4 transmission occurs in one of the 27 non-overlapping allocated channels. Out of these, 16 (from 11 to 26) are allocated in the 2.4 GHz band, each with 2 MHz bandwidth and 5 MHz channel spacing. The remaining 11 channels are allocated in sub-GHz bands.

3. EXPERIMENTAL SETUP

In order to characterize the effects of CTI on 802.15.4, we subject a 802.15.4 network to a set of different interference sources and collect a large amount of data on communication and channel observations.

Hardware setup. We run our experiments in an anechoic chamber, with dimensions 7 m x 4 m x 4 m (length, width, height), in order to have full control on the source of errors and to isolate the impact of surrounding interference sources and to identify the mere impact of each of these interfering technologies. We consider a simple network setup, as depicted in Figure 2(b), which consists of one transmitter and one receiver for both 802.15.4 and the considered interfering technology, i.e., a pair of 802.15.4 nodes and a pair of interferer nodes. We alternate the transmission power of the 802.15.4 nodes to feature attenuation levels of weak signals and emulate greater distances. We use the Tmote Sky [17] sensor nodes as 802.15.4 transmitter and receiver. Tmote Sky nodes feature CC2420 radios [4] which are compliant with the IEEE 802.15.4 standard and are widely used radio interfaces. The nodes have an integrated omni-directional inverted-F microstrip antenna.

Interfering technologies. We consider technologies with low and high emitting powers consisting of the following interference sources: WiFi, Bluetooth, FHSS, and analog



(a) Wireless Camera (b) Analog Phone (c) FHSS Phone (d) Microwave Oven

(e) Wireless Camera (f) Analog Phone (g) FHSS Phone (h) Microwave Oven

Figure 3: Characteristics of high-power interferers in the ISM band, in form of spectrograms in first row and power-profiles in the second row.

cordless phones, microwave ovens, and surveillance cameras, e.g., baby monitors (see Table 1). We use the software defined radio USRP N210 [26] to monitor a 25-MHz RF bandwidth at a given time. We round the scan in 4 tuning steps to cover 80 MHz of the 2.4 GHz band starting from 2.40 to 2.48 GHz. Figure 3 shows the spectograms and power-profiles which we recorded for a subset of the considered RF technologies. The technologies and devices we use, are described in more detail in Section 4.

Communication scenarios. As we aim at exploring low-level interference effects as precisely as possible, we eliminate all network protocol overheads by writing our receiver and sender applications to directly interface the CC2420 driver in the Contiki OS [6]. We use the three following communication scenarios: *(a)* **CCA-enabled:** transmissions at 100 ms interval, conditioned by a CCA[3] with exponential back-off period, and followed by an acknowledgment (ACK) frame; *(b)* **CCA-disabled:** transmissions at 100 ms interval, without CCA, ACK enabled; *(c)* **Saturated:** transmissions at 8 ms interval, without CCA nor ACK. In the first two scenarios, the transmission interval is constrained to 100 ms because of the time needed to log fast RSSI sampling information over the serial line. The third scenario disables fast RSSI sampling to reduce this interval and allows us to study the correlation among packets sent consecutively. The first two experiments run for 1600 packets, the third for 3200 packets. We fill the packet's payload with one of the 802.15.4 symbols, and periodically iterate over all 16 supported symbols.

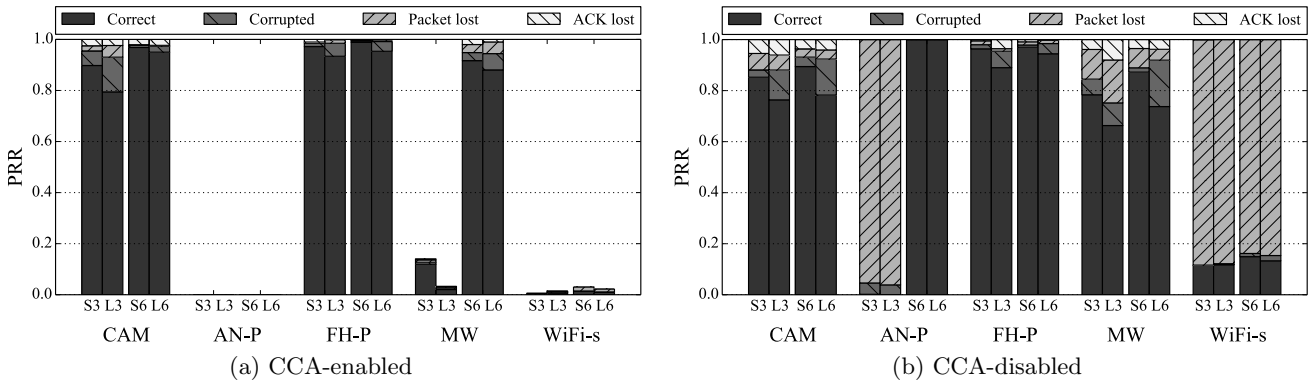
In all three scenarios, we run a series of experiments where we vary the packet sizes among 20, 40, 100 bytes, and the power level among high (0 dBm), medium (-3 dBm) and low (-10 dBm). We recognize three types of packet reception, packets that are correctly received (passed CRC check), packets that got corrupted, hence have at least one corrupted symbol (failed the CRC check), and packets that are lost, sent but never received (corruption affected the PHY header or synchronization header). In all experiments, in case we have pre-knowledge information on the exact used frequency ranges of the interferer (see spectrograms in Figure 3), the transmitter and receiver are configured to communicate over one or two channels that overlap with that of the interferers. For the technologies that affect a wide range of channels, such as for microwave oven and FHSS interferers, we loop over every second channel of 802.15.4 to broaden our scope of analysis and not to miss hopping specific channel effects.

Measurements. The transmitter logs the number of retransmission attempts (if enabled) and the noise level for each sent packet. For each received packet, the receiver logs the following information: noise level, link quality indicator (LQI), checksum value, received packet content, and the received signal strength during the packet reception associated to each received packet. We modified the CC2420 driver in Contiki to: *(a)* instruct the radio to pass packets with failed CRCs rather than discard them, to enable us processing erroneous packets; *(b)* capture RSSI values at a rate of one sample per symbol (one reading each 16 μs). Upon the detection of an incoming packet the *start of frame delimiter* (SFD) pin is set to 1, which triggers an interrupt. In this interrupt, we capture the variations of the RSSI during the reception of a packet. The sampling is performed until the last symbol of the packet is received and the SFD pin is set back to 0.

4. IMPACT OF CTI ON 802.15.4

In the following subsections, we provide an overview on the characteristics of each of the considered interferers, their overlapping spectral ranges with 802.15.4, and their direct impact on the 802.15.4 performance. The spectrum allocation of every technology considered is illustrated in Figure 1. Figure 4 shows the *Packet Reception Rate* (PRR) of the 802.15.4 nodes with different interferers placed at distances 3 and 6 m.

[3]CCA considers energy detection mode with threshold set to -45 dbm.



(a) CCA-enabled (b) CCA-disabled

Figure 4: PRR for CCA-enabled and CCA-disabled traffic types for distances 3 and 6 m. The saturated traffic type follows the same trends as CCA-disabled, hence not shown here. Empty space in CCA-enabled traffic indicates no traffic due to busy medium, i.e., backoff. Bluetooth's and non-saturated WiFi's impact on the communication are almost neglectable.

4.1 IEEE 802.11

IEEE 802.11 is the most pervasive wireless technology in indoor environments. The 802.11 b/g/n transmission occurs in one of the 14 overlapping channels spreading over the 2.4 GHz ISM band. Each channel has a width of 20 MHz, where most of these channels are overlapping with four of the 802.15.4 channels. At the physical layer, 802.11 supports a large set of modulation and coding schemes that trade performance with interference and noise tolerance. The communication signal is spread over the 20 MHz channel using DSSS or OFDM. Most 802.11 devices support power level ranges of -20 dBm to 20 dBm and commonly communicate at the highest transmission power of 20 dBm.

We evaluate the interference caused by 802.11 using a Netgear WNR3500L router and a laptop that supports IEEE 802.11 b/g/n in the 2.4 GHz ISM band. In our experiments, the router acts as an access point forwarding TCP/UDP traffic to the laptop which acts as a client. We use the network tool `iperf` [15] to generate saturated TCP traffic and non-saturated UDP traffic that resemble file download and VoIP, respectively. We configure the router to use channel 11, and study the interference impact on two 802.15.4 channels: channel 22 as fully overlapped with the WiFi channel 11 and channel 24 which is partially overlapped with WiFi channel 11.

As shown in Figure 4, for all the considered configuration scenarios, the exchanged saturated TCP (WiFi-s) caused PRR to drop to below 20%. This can be attributed to the aggressive way of WiFi transmitting at a 100x higher power than the 802.15.4 nodes. Although 802.11 employs CSMA, the amount and regularity of the energy emitted by the 802.15.4 node is not sufficient to defer 802.11 communication. In the saturated TCP case the WiFi access point transmits nearly continuously, and as a result the 802.15.4 node backs off or experiences severe packet losses. It is notable to highlight that the air time of 802.11 b/g/n packets is significantly shorter than the air time of 802.15.4 packets (about 0.54 ms for 802.11 g maximum packet length, 4.2 ms for 802.15.4 maximum packet length). The exchange of non-saturated UDP traffic, on the other hand, has negligible impact on the performance of 802.15.4 nodes. Therefore, we only show the saturated TCP case in Figure 4.

4.2 Frequency Hopping Bluetooth

Bluetooth uses the adaptive frequency hopping technique across a 79 MHz bandwidth in the 2.4 GHz ISM band, with each channel occupying a bandwidth of 1 MHz. The hopping occurs at a rate of 1600 hops/sec, hence it occupies a channel for 625 μs. Bluetooth defines different communication classes, which specify the transmission power, resulting into different communication ranges. However, the most common Bluetooth devices are the battery-powered Class 2, transmitting at 4 dBm which is higher than 802.15.4 devices (-25 dBm to 0 dbm) [5]. To evaluate the interference generated by Bluetooth on 802.15.4, we use two HTC Desire phones transferring a large file. At both considered distances, Bluetooth did not have notable impact on the performance of 802.15.4 nodes. Due to space constraints, we leave out the PRR plot considering Bluetooth interference. Note, this observation cannot be generalized to other Bluetooth classes, as in a previous study [7], we observed a performance reduction of 20% caused by Bluetooth Class 1 devices.

4.3 Wireless Camera

As for a wireless camera, we use the Philips SCD 603 digital video baby monitor. It comprises a 2.4 GHz wireless camera and a wireless video receiver. The wireless camera communicates with the wireless video receiver using frequency hopping over 61 channels, where each channel has a width of 1.125 MHz.

The camera's spectrogram (Figure 3(a)) shows the frequency hopping nature of the wireless camera. Most of the hopping occurs in the frequency range [2.42-2.45] GHz. This matches our observations on the PRR, as 802.15.4 channels interleaved in this range were affected the most. This could be due to the underlying spread sequence concentrating on this region of the spectrum. In case the camera experiences degradation in the quality, it could switch to another spread sequence that affects another region of the spectrum. In our analysis, we consider 802.15.4's channel 16 which falls in the above mentioned frequency range. At both considered distances between interferers and the 802.15.4 nodes, we measure the performance of the 802.15.4 nodes with camera being ON and OFF. For the CCA-enabled traffic, as shown

in Figure 4(a), we observe more than 20% corrupted or lost packets for long data packets at distance 3 m, resulting into retransmissions. The frequency hopping nature of the interfering signal makes its effect less intrusive, specifically due to the relatively narrow band of 802.15.4, which makes it less impaired by frequency hopping.

4.4 Analog Cordless Phone

We experiment with the Vtech GZ2456 cordless handset system. The phone base, according to the device manual [3], transmits in the frequency range [2410.2 - 2418.9] MHz, and receives in the frequency range [912.75 - 917.10] MHz. However, our experiments show that the phone base transmits in the 900 MHz band and receives in the 2.4 GHz band, which contradicts the manual description. The phone handset accordingly transmits and receives using the reverse order of frequency ranges. The phone picks a default channel out of 30 supported channels in the specified frequency range. It does not support automatic channel selection. However, channel switching can be configured manually by the user.

The spectrogram and power-profile of the analog cordless phone are illustrated in the Figures 3(b) and 3(f), respectively. The frequency profile shows that the analog phone occupies a narrow channel (about 0.1 MHz) at a time. Based on the phone frequency profile, we select the 802.15.4 channel 13 centered at 2.415 GHz which overlaps analog phone's communication.

As shown in Figure 4(a), 802.15.4 nodes while employing CCA could not communicate when subjected to analog phone interference, for both considered locations. This is due to the phone continuously transmitting, as seen in the corresponding power profile, depicted in Figure 3(f). As a result, the 802.15.4 transmitter backs off continuously due to the channel being occupied. In our previous work [7], we observed the same behavior even at a distance of 16 m.

In our experiment with CCA disabled, we force 802.15.4 transmission to occur regardless of ambient noise. Interestingly, at a distance of 6 m, as shown in Figure 4(b), most of the packets are received correctly. In this particular case, the default CCA-threshold based backoff cancels all transmissions, although communication is obviously still possible. We elaborate more on this behavior and possible workarounds in Section 5.

4.5 Digital FHSS Cordless Phone

We experiment with the Uniden DCT6485-3HS cordless handset system. The phone base and handset communicate using frequency hopping over 90 channels of 800 kHz width in the range [2407.5 - 2472] MHz. As shown in Figure 4, the FHSS phone affects 802.15.4 similarly as the wireless camera, however less destructive. This is attributed to the fact that both technologies employ the same underlying signal spreading scheme, i.e., frequency hopping, only with slight changes in channel width (cf. Table 1) and hopping rates.

4.6 Microwave Oven

We use a residential microwave oven, the Clatronic MWG 758. We heat a cup of water in the microwave to emulate an interference typical to that emitted by these appliances. As depicted in the spectrogram and power profile Figures 3(d) and 3(h), the oven radiation distinctly affects the second half of the 2.4 GHz band and the generated noise exhibits a temporal periodic ON-OFF pattern ($\sim$ 5 ms ON, $\sim$ 15 ms OFF). This confirms the observations in [11, 23]. Note that there is still a level of emitted noise in the OFF period that can cause harm to communication parties in close proximity.

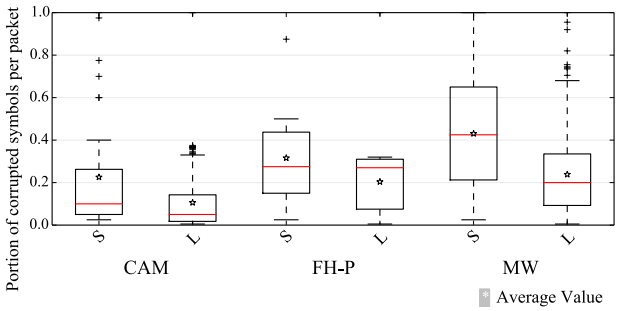


Figure 5: Portion of corrupted symbols in a packet, for the CCA-disabled traffic at distance 6 m for packets with length 100 byte (L) and 20 byte (S).

In the CCA enabled case, as shown in Figure 4(a), short packets at distance 6 m experience slightly fewer losses. This can be attributed to the ON and OFF temporal characteristics of the microwave oven. For distance 3 m, the communication is reduced down to below 20%. As we move the microwave away from 802.15.4 nodes the PRR improves to reach 90%. For the CCA disabled case, we observe about 20% to 35% corrupted or lost packets, as shown in Figure 4(b). More interestingly, for distance 3 m a severe performance reduction is not observed, as with CCA enabled.

5. INTERFERENCE ANALYSIS

This section provides a detailed analysis of packet errors and the temporal channel impairments induced by interference at the finest level of granularity, i.e., symbol level. We distinguish between two forms of accessing the wireless medium by RF interferers:

(a) Persistent form: technologies adopting this form consistently emit energy, thus monopolizing the medium completely. Analog cordless phones, as considered in our study, but also analog wireless cameras, and DSSS cordless phones, adopt such behavior [23]. This form of interference can cause a complete loss of connectivity to the affected nodes, as the medium is constantly detected as busy.

(b) Non-persistent form: other interferers are non-persistent. This implies they exhibit a time-variant ON and OFF pattern of energy emission. This is due to the underlying access mechanisms, such as frequency hopping, continual inter-frame spacing (e.g., SIFS, DIFS), and back-off slots, or periodic ON and OFF cycles of noise radiation, as for the microwave oven. This translates to exchanged packets being either correctly received (the shorter the transmission time, the higher the chances) or being partially corrupted, where the interfering signal overlaps a portion of the packet.

In the following, we analyze corrupted packets with a focus on the key features that can potentially aid link-layer recovery mechanisms.

Rate of corruption in a packet: *To what extent do non-persistent interferers corrupt a packet?* The air time of 802.15.4 packets is in the order of a few milliseconds, which is often a sufficient time interval to overlap non-persistent interfering signals. This results into having portions of the

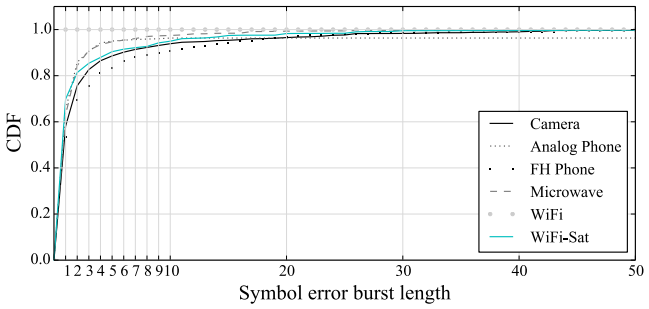


Figure 6: CDF of symbol error burst lengths considering all corrupted packets.

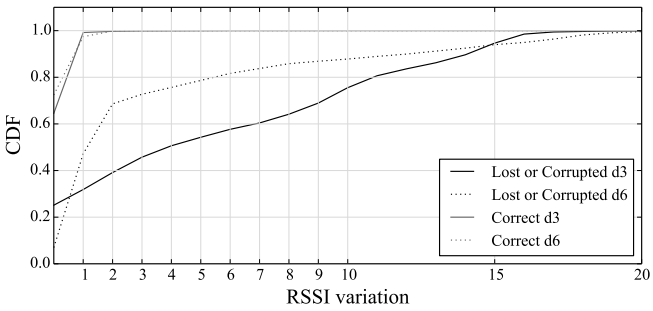


Figure 7: RSSI analysis based on RSSI samples during packet reception for two distances, 3 (d3) and 6 m (d6), aggregated for all technologies sending at highest transmission power.

packets being corrupted, in a way that varies with the time characteristics of the interferer. This insight is potentially helpful for error coding and packet recovery mechanisms.

We explore this aspect further by processing corrupted packets in our traces. Figure 5 shows the portion of corrupted symbols in every packet for the wireless camera, the FHSS phone, and microwave oven. As a result of the technologies being non-persistent, many packets experience corruption over only a minority of their symbols. This is particularly pronounced for long packets: For 100-byte packets, on average less than 25% of the received symbols are corrupted. Such packets could benefit from link-layer mechanisms that rely on PHY hints to support identifying and recovering corrupted symbols.

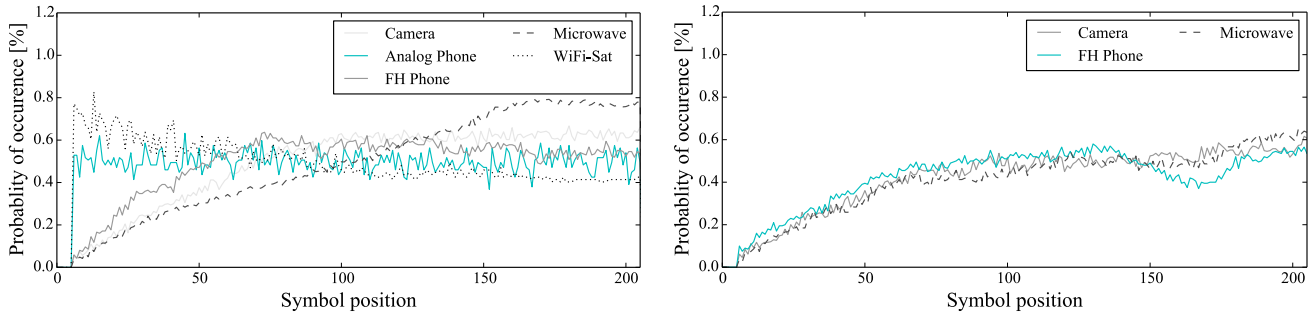
Error burstiness: *To what extent do errors occur in groups, affecting consecutive symbols and consecutive packets?* There is a common assumption that interference errors occur in bursts, thus localized in short intervals, while corrupted bits due to channel variation are randomly scattered. To identify the level of error burstiness due to CTI, we process our traces and count the frequency of symbol error bursts of length n ($n \in [1 \dots 50]$) with respect to each interferer technology across all packet lengths, power levels and distances. Note, we make our observation at the symbol level, losing information on the error burstiness in the underlying 32-bit sequence (PN) and making our notion of burst to be corresponding to symbol time of 16 μs.

Figure 6 shows the distribution of intra-packet burst lengths. The majority of the error burst lengths we processed in our traces are of length 1 for all considered technologies. This can be attributed to symbol level consideration. We observe 20-30% error bursts that range in length from 2 to 10. The wireless camera and the FH phone show a higher tendency of having error bursts of varied lengths. We leave out the discussion of the interspacing between symbol errors within a packet and across packets due to space constraints.

Error position: *Where in the packet do most of symbol errors occur?* For this, we look at the distribution of corrupted symbols over the received 802.15.4 packets. We count for each symbol position how often it was corrupted. We run this over aggregated data of both of the considered distances and transmission powers for the packet size 100 byte. Figures 8(a) and 8(b) show the probabilities of symbol corruption at different positions in a packet for both communication scenarios with CCA disabled and CCA enabled, respectively. For CCA enabled we observe less corruptions in the header information. For saturated WiFi, we observe a higher chance of corruption in the beginning of a packet, which aligns with the observations of Liang et al. [10]. For persistent interferers such as the analog phone, all positions are affected with similar probability. This changes for channel hopping technologies, i.e., the FH phone and the wireless camera. There we observe that the later positions have a higher chance to be corrupted. For microwave, we noticed that the probability increases with the symbol index until index 150 where it stabilizes. This could be attributed to the ON and OFF pattern of microwave and the fact the later positions are affected similar from the ON state.

Intra-packet channel variations: *How do RSSI readings vary within the span of a packet reception time?* We conduct an analysis to expose statistical differences in the level of RSSI readings during packet reception between interfered, non-interfered, and as in previous work [7] for weak signal losses. In this context, we check the level of surge on the RSSI readings during packet reception. Figure 7 shows the CDF of RSSI variations for interfered and non-interfered packets. Our observations confirm that RSSI readings vary within 2 dBm range for the time span of one 802.15.4 frame, considering no interference during packet reception, as the coherence time is larger than one 802.15.4 packet air time [20]. This is mainly why radio chips restrict RSSI readings to few symbols (in case of CC2420, over the 8 first symbols following the SFD field). This, consequently leads to missing to capture interference effects. The implication of this is that per packet RSSI and LQI readings are not reflecting the impact of interference. Indeed both LQI and RSSI provide indications of good and stable channel in most of the interfered packets, similar observations have been reported for 802.11 in [25]. This can be exploited to detect RF activity, diagnose packet losses and trigger interference-aware protocols. Other than detecting interference activity, the induced power level on the channel is important for other considerations, such as physical proximity to the interferer [8, 14]

CCA deferrals and energy detection: *To what extent can we rely on rigid CCA given CTI presence?* Using our traces from the saturated experiments (CCA disabled), we investigate the relation between the RSSI sampled by the sender before transmission and the actual success of packet transmissions. Doing so, we know, for every transmission, whether a node using CCA would have backed off or not (assuming a threshold of -45 dBm) and whether such back off would have been helpful or not. Figure 9 summarizes



(a) CCA-disabled (b) CCA-enabled

Figure 8: Symbol error distribution for corrupted 802.15.4 packets (aggregated for packet length 100 byte) interfering with wireless camera, analog phone, FHSS phone, microwave oven, and saturated WiFi.

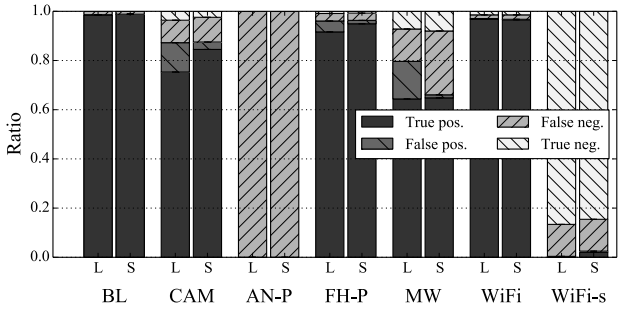


Figure 9: Ratio of successful or failed back-off decisions with CCA-disabled traffic at distance 6 m with the highest transmission power for 100 byte (L) and 20 byte (S) packets. Distinction between channel free and transmission ok (true positive), channel free but transmission either corrupted or lost (false positive), channel busy but transmission successful (false negative), and channel busy with either corrupted or lost transmission (true negative).

all possible 4 cases: no backoff followed by success (true positive) or failure (false positive), or backoff followed by success (false negative) or failure (true negative).

In the case of the analog phone, as indicated in Section 4.4, the backoff mechanism is extremely inefficient, consistently leading to false negatives (unnecessary backoff). In the WiFi saturated case, on the other hand, the backoff procedure is efficient, avoiding more than 80% of the transmissions that would have failed anyway. For the frequency hopping technologies (Bluetooth, wireless camera, FHSS phone) as well as for the non-saturated WiFi, the channel is sparsely occupied, and the backoff threshold operates as intended: few backoffs, and successful transmissions. The microwave oven, with its periodic ON-OFF pattern, is more challenging and presents cases where the backoff is either too conservative or too aggressive.

This analysis shows that (1) a single RSSI threshold cannot suit all setups and (2) even for a given setup, a threshold can trigger both false negatives and false positives, e.g., in the case of microwave oven. This indicates that careful RSSI threshold tuning on a per-technology basis or mechanisms smarter than a simple thresholding may help mitigating interference efficiently.

6. RELATED WORK

Wireless interference has gained much attention in recent wireless communication research. Work in this area falls under two broad categories: The first category deals with the impact of the RF interference on wireless networks, and the second deals with recent efforts to mitigate RF interference,

Interference impact: Studying the RF interference sources in the ISM bands has gained large interest from the wireless research community. Petrova et al. [22], Pollin et al. [24], and Sikora et al. [9] have performed experimental studies to quantify the impact of interference from 802.11, Bluetooth, and microwave oven on the performance of 802.15.4 networks. These studies focused on reporting the impact on performance metrics such as throughput and packet reception ratios, however without exploring low-level effects of interference. Liang et al. [10] studied the interplay between 802.11 and 802.15.4 networks and their patterns at bit-level granularity focusing on bit-error positions. They recognize symmetric and asymmetric interference regions. Boano et el. [11] studied interference patterns with the focus on the coarse samples of the RSSI for the purpose of emulating interference patterns in testbeds. To the best of our knowledge, our work is the first CTI study that aims at providing detailed understanding of the interaction between 802.15.4 devices and a set of prevalent RF interferers, and recognizing key factors to the harmful coexistence of these technologies.

Interference mitigation: The recognizable impact of RF interference on the performance of wireless networks has motivated researchers to look at solutions to mitigate interference. The most widely adapted mitigation solution is to avert interferer frequencies by employing spectrum sensing to identify interference-free channels [13, 21, 1]. Such approaches are resource hungry for 802.15.4 networks. Moreover, the spectrum is crowded with wireless devices which makes it hard to find interference-free channels. Classifying interference sources is possible by employing signal processing classifiers [1, 19] or featuring distinct interferers' patterns on corrupted packets [12]. It is, however, not yet clear how the interference classifiers can be utilized in an automated

way to mitigate interference, given the diversity of interference technologies.

Another direction of research focuses on the recovery from symbol corruption, by utilizing resilience coding schemes that are robust to bursty errors. For instance, reed solomon coding can be employed to mitigate the 802.11 impact on 802.15.4 networks, as suggested by Liang et al. [10]. Furthermore, partial packet recovery mechanisms are used to exploit the temporal effects of interference induced on the PHY hints, such as variations in soft errors (softPHY) [18] or RSSI variations [7, 16] to determine boundaries of the interfered fractions on the received corrupted packets. Recent research efforts utilize advancements in MIMO for interference cancellation [23] and to facilitate spectral usage efficiency and harmonize coexistence across different technologies. However, such advancements are not yet feasible for 802.15.4 devices.

7. CONCLUSION

In this paper, we report and discuss results of our empirical study of the cross technology interference impacts on 802.15.4. We examine the interaction patterns between 802.15.4 and a set of prevalent high and low-power RF interferers at symbol level granularity with focus on protocol aspects, error patterns of bits transmitted over the air and the wireless link variations as perceived by the transmitter and receiver. We show that RF interferer technologies differ widely in the way they affect 802.15.4 networks. Thus, they form a strong and complex impact on the performance of a wireless network that needs to be addressed with novel solutions that exploit channel information and physical layer hints. One important outcome of this study is that there is no one-fits-all solution to mitigate the impact of CTI. We need to address this by designing measures that take into account the properties of the interferers to adaptively select a proper mitigation mechanism. Thus, we aim for the future work to design a lightweight system that passively monitors channel information and physical layer hints to classify interferers by their properties, such as periodicity, persistency level, emitted power level, etc., and consequently map it to an appropriate mitigation mechanism. This will overcome the limitations of interference source classification approaches, which can not be utilized in an automated way and leave it to the user to decide on proper countermeasures. We expect that our study will provide useful insights for designing 802.15.4 protocols that better withstand RF interference.

8. REFERENCES

[1] Cisco CleanAir Technology. `http://www.cisco.com/en/US/netsol/ns1070/`.

[2] FCC Lab: Report on Trends in Wireless Devices. `www.fcc.gov/oet/info/documents/reports/wirelessdevices.doc`.

[3] Vtech GZ2456 User Manual.

[4] *Texas Instruments. CC2420 datasheet*, 2007.

[5] Low-Rate Wireless Personal Area Networks (LR-WPANs), IEEE Std. 802.15.4., 2011.

[6] A. Dunkels, B. Gronvall, T. Voigt. Contiki - A Lightweight and Flexible Operating System for Tiny Networked Sensors. In *IEEE LCN*, 2004.

[7] A. Hithnawi. Exploiting Physical Layer Information to Mitigate Cross-Technology Interference Effects on Low-Power Wireless Networks. In *ACM SenSys*, 2013.

[8] A. Hithnawi, H. Shafagh, S. Duquennoy. Low-Power Wireless Channel Quality Estimation in the Presence of RF Smog. In *IEEE DCOSS*, 2014.

[9] A. Sikora, V.F. Groza. Coexistence of IEEE 802.15.4 with other Systems in the 2.4 GHz-ISM-Band. In *IEEE IMTC*, 2005.

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

[11] C.A. Boano, T. Voigt, C. Noda, K. Romer, M. Zuniga. JamLab: Augmenting Sensornet Testbeds with Realistic and Controlled Interference Generation. In *ACM/IEEE IPSN*, 2011.

[12] 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*, 2013.

[13] H. Rahul, N. Kushman, D. Katabi, C. Sodini, F. Edalat. Learning to Share: Narrowband-friendly Wideband Networks. In *ACM SIGCOMM*, 2008.

[14] H. Shafagh, A. Hithnawi. Come Closer - Proximity-based Authentication for the Internet of Things. In *MobiCom*, 2014.

[15] Iperf. `http://iperf.sourceforge.net/`.

[16] J. Hauer, A. Willig, A. Wolisz. Mitigating the Effects of RF Interference through RSSI-Based Error Recovery. In *EWSN*, 2010.

[17] J. Polastre, R. Szewczyk, D. Culler. Telos: Enabling Ultra-low Power Wireless Research. In *ACM/IEEE IPSN*, 2005.

[18] K. Jamieson, H. Balakrishnan. PPR: Partial Packet Recovery for Wireless Networks. In *ACM SIGCOMM*, 2007.

[19] K. Lakshminarayanan, S. Sapra, S. Seshan, P. Steenkiste. RFDump: An Architecture for Monitoring the Wireless Ether. In *ACM CoNEXT*, 2009.

[20] K. Srinivasan, M. Kazandjieva, S. Agarwal, P. Levis. The β-factor: Measuring Wireless Link Burstiness. In *ACM SenSys*, 2008.

[21] L. Yang, W. Hou, L. Cao, B. Zhao, H. Zheng. Supporting Demanding Wireless Applications with Frequency-agile Radios. In *USENIX NSDI*, 2010.

[22] M. Petrova, W. Lili, P. Mahonen, J. Riihijarvi. Interference Measurements on Performance Degradation between Colocated IEEE 802.11g/n and IEEE 802.15.4 Networks. In *IEEE LCN*, 2007.

[23] S. Gollakota, F. Adib, D. Katabi, S. Seshan. Clearing the RF Smog: Making 802.11n Robust to Cross-technology Interference. In *ACM SIGCOMM*, 2011.

[24] S. Pollin, I. Tan, B. Hodge, C. Chun, A. Bahai. Harmful Coexistence Between 802.15.4 and 802.11: A Measurement-based Study. In *CrownCom*, 2008.

[25] S. Rayanchu, A. Mishra, D. Agrawal, S. Saha, S. Banerjee. Diagnosing Wireless Packet Losses in 802.11: Separating Collision from Weak Signal. In *IEEE INFOCOM*, 2008.

[26] Universal Software Radio Peripheral, Ettus Inc. `www.ettus.com`.