Cross-Technology Interference: Detection, Avoidance, and Coexistence Mechanisms in the ISM Bands

Zegeye Mekasha Kidane[1*] and Waltenegus Dargie[2*†]

[1]Electronics Division, Max Planck Institute for Radio Astronomy, Bad Muenstereifel, 53902, Rheinland-Pfalz, Germany.

[2]Faculty of Computer Science, Technische Universität Dresden, Dresden, 01062, Sachsen, Germany.

*Corresponding authors. E-mail: zkidane@mpifr.de; waltenegus.dargie@tu-dresden.de;
†The authors contributed equally to this work.

Abstract
A large number of heterogeneous wireless networks share the unlicensed spectrum designated as the ISM (Industry, Scientific, and Medicine) radio band. These networks do not adhere to a common medium access rule and differ in their specifications considerably. As a result, when concurrently active, they cause cross-technology interference (CTI) on each other. The effect of this interference is not reciprocal, the networks using high transmission power and advanced transmission schemes often causing disproportionate disruptions to those with modest communication and computation resources. CTI corrupts packets, incurs packet retransmission cost, introduces end-to-end latency and jitter, and make networks unpredictable. The purpose of this paper is to closely examine its impact on low-power networks which are based on the IEEE 802.15.4 standard. It discusses latest developments on CTI detection, coexistence and avoidance mechanisms as well on messaging schemes which attempt to enable heterogeneous networks directly communicate with one another to coordinate packet transmission and channel assignment.

Keywords Coexistence, Cross-technology interference, heterogeneous networks, Internet of Things, wireless sensor networks

1 Introduction

The vision of the Internet of Things [1] presupposes the coexistence of and close collaboration between multiple technologies [2]. In precision agriculture, for example, wireless sensor networks and Unmanned Aerial Vehicles (UAV) can be jointly deployed to achieve highly precise sensing and efficient micro resource management [3, 4]. The nodes on the ground can collect various soil parameters whilst the UAVs assist in collecting and aggregating sensed data as well as in micro-administering resources such as herbicide. Similarly, in water quality monitoring, ground nodes can collect such parameters as pH, water temperature, turbidity, and dissolved oxygen, whilst Unmanned Surface Vehicles (USV) aggregate data from these sensors and assist in connecting disconnected regions [5]. In smart industries, where a seamless interaction between equipment, robots, and other objects may be required, the integration of multiple technologies is essential to achieve efficient, safe, and reliable operation [6, 7].

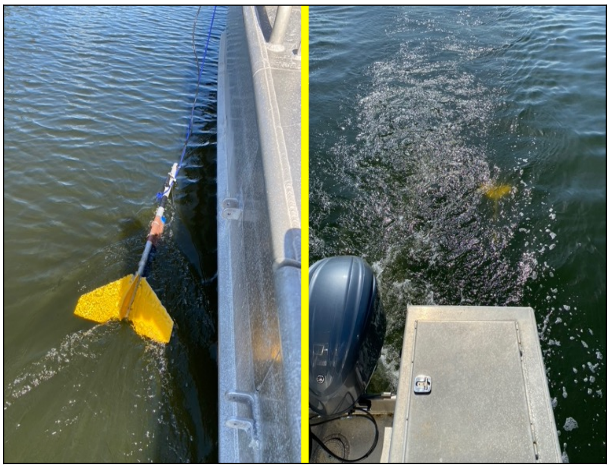


Fig. 1: Water quality monitoring at North Biscayne Bay, Miami, Florida.

For multiple technologies to coexist, issues pertaining to medium access and interference have to be resolved first. When the technologies are developed independently but share the same spectrum, they may cause interference on each other. This type of interference is called cross-technology interference, or CTI, in short [8, 9]. CTI becomes formidable when there is a significant disparity in the bandwidth and power requirements of the technologies, often those relying on low-bandwidth and low transmission power becoming victims of intense CTI. The focus of this paper is to closely examine the problem of CTI emanating from technologies sharing the ISM radio band, a license-free radio band internationally reserved for Industry, Scientific, and Medical purposes [10]. The band occupies several ranges in the radio frequency spectrum, but the one which is of particular interest to us is the range between 2.4 and 2.5 GHz with the centre frequency located at 2.45 GHz. This band has a 100 MHz bandwidth and is often employed by short-range, low-power wireless technologies.

In order to motivate the subject matters discussed in this paper, we begin by relating our experience with CTI. In the summer of 2023 we undertook multiple research expeditions with the Institute of Environment at Florida International University (FIU) on North Biscayne Bay, Miami, Florida. Twice a month, and whenever the need arises, the institute undertakes a boat tour on the bay and its surrounding areas to collect water quality parameters (pH, temperature, conductivity, dissolved oxygen, turbidity, chlorophyll, and fluorescent dissolved organic matter). A tour requires a certified captain and at least one researcher, and lasts about two hours. Fig. 1 displays the deployment of the water quality monitoring device. Recently, the quality of the water in the bay has been considerably affected by both natural and man-made causes, giving rise to the death of a substantial amount of fish and other aquatic species [11, 12]. In order to achieve a more efficient and scalable monitoring, the institute has started deploying special autonomous (unmanned) surface vessels (USV). Our expedition was intended to experimentally investigate the extent to which wireless sensor networks could be employed to monitor the water quality at a much higher spatio-temporal and scalable resolution. In this regard, an essential requirement was to establish resilient and reliable networks which operate in the presence of a rough water and extreme weather condition. Moreover, the sensor networks should be able to interact with the USVs.

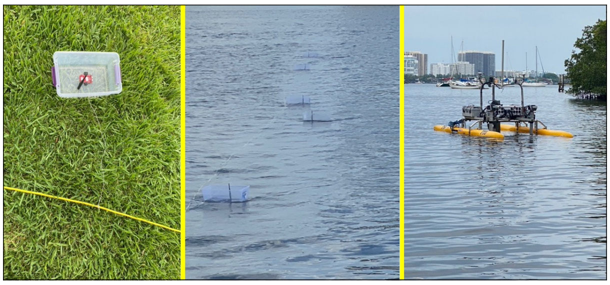


Fig. 2: Deployment of an Unmanned Surface Vehicle and a Wireless Sensor Network at North Biscayne Bay, Miami, Florida [13].

In one of these expeditions, we deployed a network of six wireless sensor nodes placed in open plastic boxes. The boxes were tied to a long rope which, in turn, was tied to a boat (Fig. 2). The nodes self-organised using the RPL protocol [14] and a 2.4 GHz radio to support distributed sensing and multi-hop communication. The distance between the nodes was about 50 m. In the absence of CTI, the nodes communicated with one another with modest packet loss, despite an appreciable water motion. Fig. 3 shows the change in the RSSI of

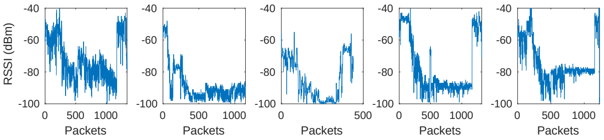


Fig. 3: Link quality fluctuation (in terms of the change in RSSI of received packets) in the absence of any CTI.

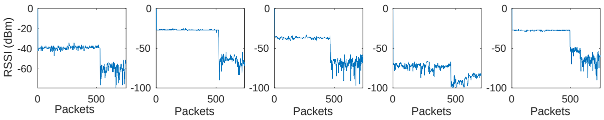


Fig. 4: Link quality fluctuation in the absence and presence of a CTI.

successfully transmitted packets, correctly mirroring the movement of the water. When, however, one of the USVs from FIU was within 300 m radius or so, communication was considerably inhibited. We tested all the available channels (there were 16 available non-overlapping channels) to minimise the effect of CTI, but the network performance remained poor. In order to separate the effect of the movement of the water on the link quality from the effect of CTI, we deployed the network along the shore of the bay and observed the link quality fluctuation both in the absence and presence of the USV. As can be seen in Fig. 4, the link quality was relatively stable until the USV entered into the interference zone of the network; afterwards, the network transited into an unstable state, followed by a complete disconnection of all the links. The USV was a product of SeaRobotics Corporation[1] and employed the IEEE 802.11b standard to interact with its remote control station.

Our second experience was on one of the lakes on FIU's Main Campus. This time, we collaborated with the team of the Motion, Robotics, and Automation Lab to jointly deploy a wireless sensor network and a USV on the lake. Additionally, one sensor node was deployed on the boat itself. Both this node and the nodes deployed on the surface of the lake communicated with a node placed outside the lake (ref. to Fig. 5). The present USV had a more complex setup than the one deployed on North Biscayne Bay. It communicated with

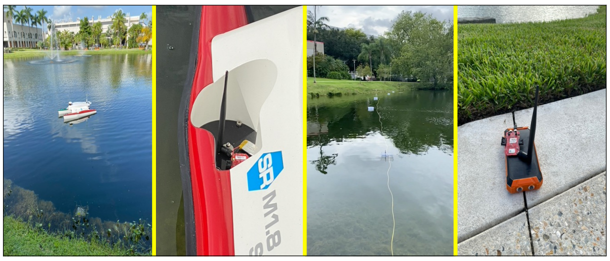


Fig. 5: Deployment of an Unmanned Surface Vehicle and a Wireless Sensor Network at one of the Lakes on Florida International University main campus.

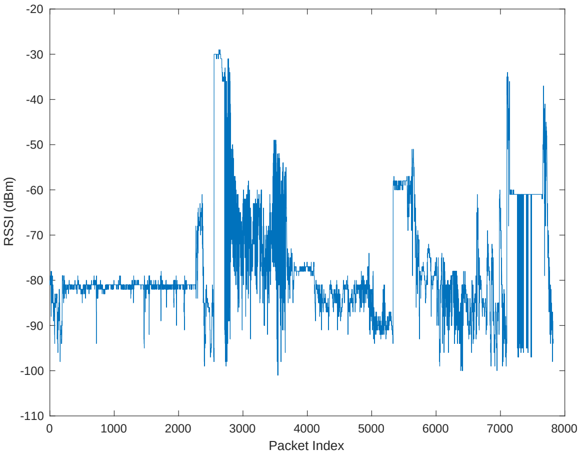


Fig. 6: Link quality fluctuation in the presence of CTI (Deployment on a lake on FIU's Main Campus).

the remote control station using a proprietary and powerful transceiver, operating in the 4.9-5.8 GHz band, but in addition, the control station was remotely controlled by a human agent using the IEEE 802.11b standard. When the USV navigated autonomously, both the node deployed on the boat and on the lake experienced no interference and the link quality was, by and large, stable; as soon as a human agent interacted with the boat using the IEEE 802.11b interface, all the nodes experienced a significant CTI. The nodes which was affected the worst was the one carried by the autonomous boat. Fig. 6 shows the link quality of this node, as reflected by the RSSI of the packets it received from the base station.

[1] https://www.searobotics.com/

As the first contribution of this paper, our survey includes latest developments on coexistence and CTI avoidance mechanisms. In particular, we review state-of-the-art dealing with Cross-Technology Communication (CTC), which enables heterogeneous networks to exchange information about communication timing and channel occupation. As the second contribution, our paper focuses on protocols and algorithms involving actual implementation and deployment as opposed to those based on simulation. As the third contribution, our survey provides a more complete picture of CTI, addressing spectrum occupation, modulation, emerging networks, interference detection, coexistence and avoidance mechanisms, as well as the impact of CTI on the performance and energy-consumption of low-power networks.

The remainder of this paper is organized as follows: Section 2, provides a brief summary of the body of work which is similar to ours. Section 3 introduces CTI and discusses competing standards. Section 4 discusses CTI detection strategies. Sections 5 and 6 review avoidance and coexistence strategies, respectively. Section 7 presents medium access and system support strategies for low-power (IoT) networks dealing with CTI. In Section 8, the impact of CTI on low-power networks will be discussed. Finally, in Section 9, concluding remarks will be made and open issues will be highlighted.

2 Related Work

In the recent past, multiple survey papers have been published with the focus on cross-technology interference. In [15], the authors survey papers which address cross technology interference between ZigBee, WiFi, and Bluetooth technologies. The authors' main focus was on interference avoidance mechanisms. In [16], the authors survey papers on cross-technology communication (CTC), which enables heterogeneous technologies to coordinate communication and channel assignment. The authors compare the performance of different approaches in terms of throughput, reliability, hardware modification, and concurrency. By contrast, the present paper provides a more comprehensive understanding of CTI and proposed approaches to deal with it. A comprehensive and well-structured review of the role of machine learning in improving the performance of IEEE 802.11 family networks is presented in [17]. The authors identify four distinct features which can take advantage of latest developments in machine learning: coexistence in core WiFi networks, distributed adaptation in emerging WiFi networks (WiFi-6 and WiFi-7), multi-hop networks, and connectivity management. As far as coexistence is concerned, the authors' focus was limited to the coexistence of WiFi networks with LTE networks. Our paper complements theirs by reviewing papers dealing with the coexistence of low-power (IEEE 802.15.4) networks with WiFi and Bluetooth technologies.

3 Cross-Technology Interference

The first step to mitigate CTI is to understand its causes. This concern has to be approached in two ways. The first is to understand the networks which produce the interference; the second is to understand the underlying communication standards and specifications based on which the networks operate. A decade or so ago, the devices which typically produced and were affected by CTI were low-power, low-range, or low-rate devices and networks, such as cordless telephones, microwave ovens, wireless battery chargers, Bluetooth devices, and local area networks. Though these devices and networks can still be a concern, the most formidable challenges come from emerging autonomous systems whose operation and interaction regions are much wider. These devices typically rely on a high transmission power and large antennas; and employ advanced modulation and medium access techniques to ensure safe and reliable operations. For example, low-altitude enterprise Unmanned Aerial Vehicles (UAV) produced by DJI[2] employ long-range proprietary controllers operating in the 2.4 and 5.8 GHz radio bands and switch between these bands using time-slotted and frequency hopping strategies to deal with CTI; in doing so, they themselves produce a considerable CTI to nearby low-power IoT devices and networks.

[2] https://www.dji.com

Coexisting wireless device comparison				
Technology	IEEE 802.15.4	IEEE 802.15.1	IEEE 802.11 b/g/n	Commercial drone (UAV) Technology
Number of Channels	16	79	11/13/14	Use 802.11 channels
Data rate	250 Kbps	1 Mbps	11 Mbps, 54 Mbps	90-100 Mbps
Band width	2 MHz	15 MHz	20 MHz	80 MHz
Transmit Power	0 dBm	1-20 dBm	10-20 dBm	10 mW-1 W
Transmit range[m]	1-100	1-10	1-100	100-500
Power consumption	Very Low	Low	High	Very High
Throughput	20-250 Kbps	720 Kbps	11 Mbps	90 Mbps
Channel allocation	11-26	1-79	1-13	NA
Method of Channel Access	CSMA/CA DCS, Scheduling	Master Slave scheme, AFH	CSMA/CA, DCS	NA
Operating Frequency	2.4 GHz	2.4 GHz	2.4 GHz	2.4 GHz, 5.8 GHz, 433 MHz, 915 MHz
Frequency Modulation	Orthogonal-PSK, BPSK	GFSK	OFDM, DSSS,CCK	BPSK, OFDM, OTFS
Coexistence	CCA based energy detection	FH, spread spectrum	CCA based energy detection	spectrum overlay multiple access (SOMA),TDMA
Encryption	AES-BC (CTR)	E0-SC	RC4-SC(WEP), AES-BC	AES, ARIA, HMAC, ECDSA
Data protection	16-bit CRC	16-bit CRC	32-bit CRC	CRC
Interference Avoidance Method	Fixed Collision avoidance, Frequency Hopping, TSCH	Frequency Hopping	Collision avoidance	Frequency Hopping
Signal On-air time	[576, 4256] us	366 us	[194, 542] us	[1, 3] minutes
Minimum packet interval	2.8 ms or 192 us	NA	$\geq$ 28 us	0.38 ms
Peak to average power ratio	$\leq$ 1.3	$\leq$ 1.3	$\geq$1.9	$\geq$2

Table 1: Comparison of coexisting ISM frequency band technologies.

3.1 Standards

Most of the wireless links which potentially cause and are affected by CTI in the ISM radio band are those based on the IEEE 802.11 and IEEE 802.15 standards. More specifically, in the former, we have the IEEE 802.11 b/g/n/ax/be/ba networks (commonly known as WiFi networks), whereas in the latter, we have IEEE 802.15.1 (Bluetooth), 802.15.3 (high-rate PAN), IEEE 802.15.4 (low-rate PAN), and IEEE 802.15.5 (Mesh) networks. The IEEE 802.15.4 standard defines 27 channels, each having a bandwidth of 2 MHz (refer to Table 1). Of these, 16 channels (designated Channels 11-26) are in the 2.4 GHz frequency band; Channels 1 to 10 are in the 915 MHz frequency band; and Channel 0 is in the 868 MHz frequency band. Equation 1 is used to determine the centre frequencies of Channels 11 to 26. Similarly, Bluetooth has 79 channels, each having a bandwidth of 1 MHz; and IEEE 802.11/b/g/n wireless local area networks have 14 available channels. Of these, only 11 are legally available in the US and only 13 are available in Europe. Nevertheless, most existing networks use only 3 of these (Channels 1, 6 and 11) to avoid adjacent channel interference. Channel 1 potentially interferes with Channels 11, 12, 13 and 14 of the IEEE 802.15.4 ISM band; Channel 6 potentially interferes with Channels 16, 17, 18, and 19 of the IEEE 802.15.4 ISM band; and Channel 11, overlaps with Channels 21 to 24. All available Bluetooth channels overlap with IEEE 802.15.4 channels, although, as independent studies show, interference from Bluetooth technologies is not appreciable [18, 19].

The spectral assignment of the IEEE 802.15.4 channels is given as:

$$F_c(n) = 2405 + 5(n - 11) \tag{1}$$

where F_c is the centre frequency in MHz and $n = 11, 12, ...26$ is the channel number.

3.2 Link Quality Metrics

Recent work on interference classification relies mainly on mapping the pattern of some low-level link quality metrics to well-known classes of interference. The pattern itself can be established by sampling the values of these metrics in time and in frequency domains and across all the available channels to establish multi-dimensional distributions and to compare the distributions with the signal profiles of the different standards discussed above. This approach performs poorly when there are multiple sources of interference. More importantly, there is no generally accepted mechanism to map the metrics to any particular physical parameters. Different chip manufacturers often implement their own metrics to characterise link quality.

There are, however, some widely accepted abstract (or coarse-grained) metrics which can be employed to characterise wireless links. The reason we label them as “coarse-grained“ is that they are obtained by averaging the received power of a signal over a period of time. The IEEE 802.15.4 specification [20] defines two physical layer parameters: Energy Detection (ED) and Link Quality Indicator (LQI). ED is an approximation of the received signal's power within the bandwidth of a given channel. It is obtained by calculating the average power corresponding to 8 successive symbols. Ideally, its range is 40 dB (in some technologies, even 85 dB) within which the mapping from a received power in decibels to an ED value is linear, with an accuracy of ± 6 dB. The metric is useful for assessing background noise and for calculating LQI. Another widely employed metric is the Received Signal Strength Indicator (RSSI), which is often associated with successfully received packets. In both cases, the source of a received signal may be an interferer. Hence, both metrics may not directly correspond to the quality with which a packet is received. The LQI, on the other hand, characterises the strength and/or quality of a desirable signal. Hence, it is directly associated with the quality with which a packet was successfully received. The specification does not state how this metric should be computed, but suggests that it can be determined based on ED, a signal-to-noise ratio estimation, or a combination of both.

Both RSSI and LQI say little about lost packets, so that the exact link state at the time the packets are lost cannot be established. There are some higher-level metrics which attempt to provide an estimation of the link quality of lost packets. One of these is the Packet Reception Rate (PRR). This metric is expressed as the ratio of the number of packets successfully received in the past τ seconds to the ideal number of packets that could be transmitted in that same time. The metric can be computed using a sliding window. Taking the difference in PRR of adjacent time slots enables to estimate the short-term link stability condition, whether this condition refers to a consistently bad or consistently good state. A CTI can also be indirectly determined by characterising link quality fluctuation in terms of the number of packets successively lost or received [21]. Assuming that the transmission pattern of the interferer is statistically stable, this metric enables to estimate the average duration a wireless link is under the influence of interference [13, 22]. Fig. 7 shows the histogram of successively lost packets when a node carried by a UAV transmitted packets in burst to a ground node. As can be seen, the histogram can be modelled as an exponential probability density function having the form: $f_x(x) = \lambda e^{-\lambda x}$, where x is the number of packets lost in succession and λ encodes the rate at which the graph decreases. Once $f_x(x)$ is estimated, it is possible to compute the average number of packets lost in succession: $E[x] = \int x.f_x(x)$. With this and the knowledge of packet length and the node's transmission rate, it is possible to determine the average duration of interference. This approach assumes that the main cause of packet loss is CTI.

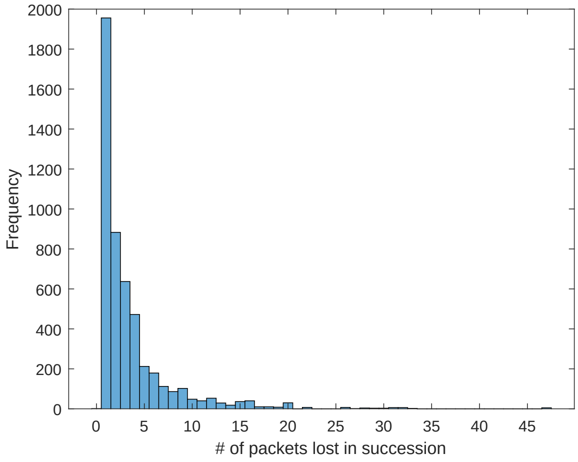


Fig. 7: Histogram of a successively lost packet when a node carried by a UAV interacts with a ground wireless sensor node

3.3 Wireless Links Models

Characterising wireless links is a classical problem. In cellular (mobile) networks, for example, models of wireless links are useful for radio management (for adapting transmission power, time-slots appropriation, handover, etc.). In such networks, both transmitters and receivers establish channel state information (CSI) by scanning the available channels at an appreciably high rate; then various features of this information are extracted to determine the characteristics of the wireless links and to carry out some compensatory or adaptive measures. Low-power networks do not have sufficient resources to perform elaborate computation. Consequently, they often rely on offline, light-weight link models to achieve the same goals.

Besides CTI, the quality of a wireless link may be affected by several external factors, including surrounding temperature, heavy rain, humidity, and shadowing [23]. In order to distinguish a CTI from link quality deterioration arising from factors inherent to the deployment setting, some researchers have proposed models to account for the contribution of the latter (which are thought to be more persistent). For example, in the context of a joint deployment consisting of a UAV and a wireless sensor network, Dragulinescu et al. identified six types of propagation environments [24]: free space, rural area, suburban, urban, dense urban and highly dense urban, though their study specifically addresses rural and free space. In both cases, the authors further distinguish between aerial and terrestrial channels, the former models the characteristic of a channel established between a UAV and a ground node, whereas the latter models the characteristics of a channel established between two ground nodes. Likewise, an air-to-air channel models the characteristics of a channel established between two or more UAVs or a UAV and a satellite. Habib et al. [25], Kim et al. [26], and Dargie et al. [27] likewise propose additional models to characterise signal propagation involving different water bodies (sea, river, lake).

4 Detection

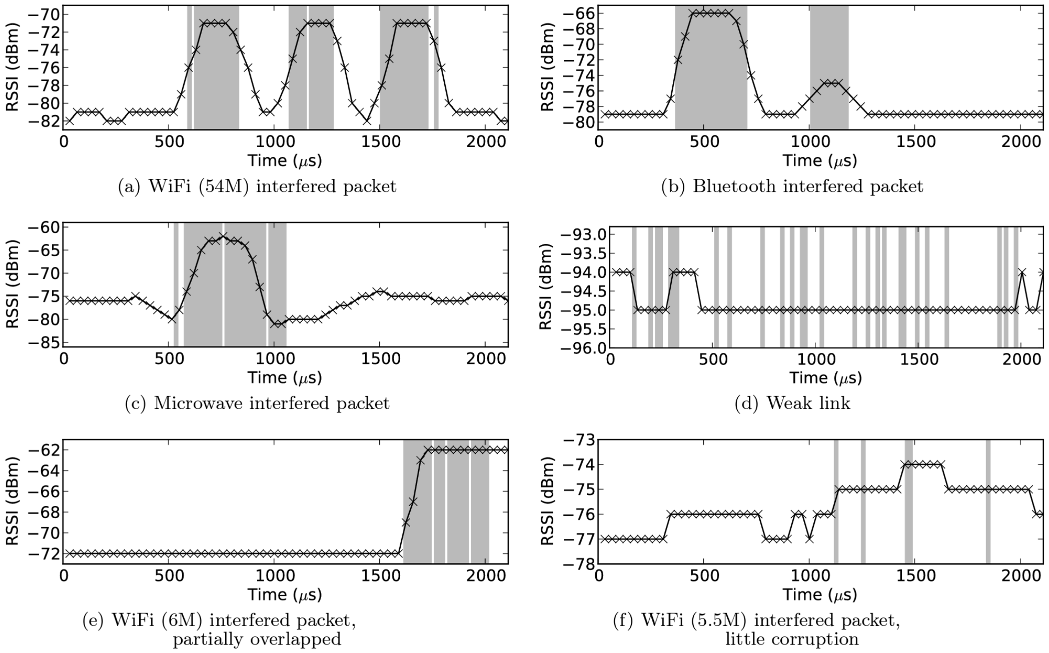
Detecting the causes and the characteristics of a CTI is crucial to effectively deal with it. A spectrum analysis is required to establish a complete information, but this involves, among others, Fast Fourier Transform (FFT), which is costly, both in terms of the resources it demands and the time it takes. All other approaches are at best approximations. One of the most frequently employed approaches consists of energy detection, in which a receiver scans all the available channels, probing the power at its radio front end. Finally, it compares some statistical aspects of the power (such as mean, max, min, average, zero-crossing, etc.) with some existing patterns to determine CTI and its potential sources. This approach requires a fast scan time, an appreciable local memory to save the sampled power and reference profiles, as well as some computation. Hence, its reliability depends on the available resources and the extent to which the reference models represent the underlying reality.

One way of establishing a reference model for a particular source of a CTI is mapping its interaction pattern to the standard to which it complies. A standard is by definition a set of rules. In all communication standards, the specific steps communicating partners take to exchange packets using a shared medium are well-defined. For instance, in most wireless standards, packet transmission is preceded by the transmission of preambles to enable signal detection and synchronization. The length and transmission duration of the preambles vary from standard to standard. Similarly, when a transmitter occupies a medium, the rules to which it complies can be inferred from its manner of packet transmission. For instance, in IEEE 801.11a an idle duration of 16 us (inter-frame space) will be experienced between the transmission of a data packet and the reception of an ACK packet; whereas this duration is 10 us in IEEE 802.11n (2.4 GHz) networks. Similar approaches map energy distributions to known traffic patterns. For example, Qin et al. [28] observe that WiFi frames are highly clustered and there are small idle leaks within the frame clusters and large white space between frame clusters.

There are other approaches which rely on low-level features, but they presuppose knowledge of the data encoding and modulation of corrupted packets. In IEEE 802.15.4, the data to be transmitted is first grouped into 4-bit symbols, each of which is then converted into a predefined 32-bit long pseudo-random noise sequence [29]. The bits (so called chips) are further grouped into even and odd chips and are modulated using Offset Quadrature Phase-Shift Keying (O-QPSK) – the even chips modulated as In-phase (I) component of the carrier, and the odd chips, as Quadrature (Q) component of the carrier. There is a time offset between the Q-phase chips and the I-phase chips, so as to enable a continuous phase change. Since the message is encoded in the pattern of the phase-shift, the wave shape and amplitude of the carrier is intact. This enables the reliable detection of the modulated signal in the presence of appreciable noise. During packet reception, demodulation and low-level source decoding take place in the first place, inside the radio chip. In most cases bit-by-bit analysis of received packets is not possible, as this is done by a hardware component. Therefore, the lowest-level information available is in the form of 4-bit symbols [30].

In [30] and [8], the authors closely investigate the symbols of corrupted packets to discover distinct interference patterns which can be traced back to specific causes. The authors distinguish between lost packets and corrupted packets. In the first, a receiver fails to detect packet preambles and subsequent headers which enables it to successfully decode the packet; whereas in the second, a packet is actually received but its CRC flags an error. In [30], when a receiver receives a corrupted packet, it requests a retransmission and carries out a symbol-by-symbol comparison to localise the corrupted symbols and establish a pattern. The authors observe that different interference sources leave distinct patterns. Interestingly, corrupted symbols are likely to be received with a relatively high energy (i.e., high RSSI values). The authors trained a supervised model with these and additional low-level features to classify different sources of a CTI. Fig. 8 shows the CTI patterns of different causes based on the analysis of corrupted symbols of received packets. Similarly, Hithnawi et al. [8] purport that interference errors occur in bursts and can be localized to short intervals. By contrast, corrupted bits due to random channel variation are randomly scattered. To characterise error burstiness due to CTI, the authors artificially induced interference using different technologies and analysed the traces of corrupted symbols, counting the frequency of symbol error bursts of various length, for each interferer technology; variable packet length, power level, and distance.

Similarly, in [31], the interference patterns of WiFi networks on IEEE 802.15.4 networks is studied experimentally. In the presence of 20 active WiFi APs deployed in the basement of a school building, two sensor nodes exchanged packets every 30 ms at a transmission rate of 250 kbps and using a variable transmission power, ranging from -65 to -27 dBm. The packet size was 127 bytes. To compensate for the effect of CTI, the transmitter's power was adjusted every 10 seconds, from the minimum to the maximum level. Likewise, the transmitter and the receiver simultaneously switched to a different channel every 600 s, beginning from Channel 11 to Channel 25. The entire experiment lasted 8 hours. The experiment results reveal that the CTI patterns of the channels overlapping with Channel 1, 6, 11 of the WiFi network had similar patterns: The duration and interval between corrupted symbols suggest that CTI having a short duration but occurring in short intervals was experienced more frequently than CTI having a long duration or occurring in long intervals. The authors attribute this to short and frequent WiFi data transmissions.



(a) WiFi (54M) interfered packet

(b) Bluetooth interfered packet

(c) Microwave interfered packet

(d) Weak link

(e) WiFi (6M) interfered packet, partially overlapped

(f) WiFi (5.5M) interfered packet, little corruption

Fig. 8: Determining the sources of cross-technology interference by establishing the pattern of corrupted symbols in received packets [30].

CTI Detection			
Research Papers	Research aim	Detection method	Technical features
[32–35]	Identification of bad radio channels	Blacklisting channels with low PDR and RSSI burst	Establishing reliable wireless links
[8, 30, 31]	Interference classification	Symbol-level correlation of corrupted packets using correlation and soft values	Mitigation of short-duration WiFi interference in long-duration ZigBee communications
[36–38]	Signal modelling and interference detection	Using deep learning and transfer learning for multi-channel spectral representation	RF emission detection, classification, and spectro-temporal localization
[39]	Channel state analysis, interference characterisation/classification	Interference detection; ranking of the relative strength of interference	Interference duration estimation
[40]	Interference and intrusion detection	Use of Random Forest Machine Learning to classify interference	Analyse of received In-phase (I) and Quadrature-phase (Q) samples

Table 2: Review of CTI detection mechanisms

Croce et al. [38] employ an Artificial Neural Network (ANN) and a Hidden Markov Model (HMM) to detect CTI during the reception of a WiFi frame. The models enable to differentiate between different sources of interference (IEEE 802.15.4, LTE, microwave, and IEEE 802.11). The authors argue that, whereas for WiFi standard frames the error probability varies during frame reception in different frame fields (PHY, MAC headers, and payloads), errors due to CTI appear randomly when the demodulator attempts to receive exogenous interfering signals. Based on their probability of occurrence, patterns (sequence of occurrence), and time intervals, the errors are classified into different sources. The error analysis in a WiFi receiver has been carried out by demodulating a sequence of completely random bits. The demodulated bits are interpreted according to the format of a WiFi frame. The authors trained and tested their models using an of-the-shelf WiFi network interface card (NIC) and two types of IEEE 802.15.4-compliant transceivers (CC2420[3] and MRF24J40[4]). The later produced controlled interference, a single source producing interference on the WiFi link at Channels 11, 10 or 8 with different interference transmitter power levels at a time. Two different approaches were used for classifying the interference sources acting on the targeted WiFi receiver. The first approach was based on the receiver behaviour in a fixed time interval (a few tens of ms) corresponding to a few samples of the error vectors. The second approach was based on a given error burst delimited by the channel busy register (a single frame radiation period). In this case, idle times between consecutive error burst were not considered for classification. The authors claim that with 95% accuracy they were able to determine the source and timing of interference.

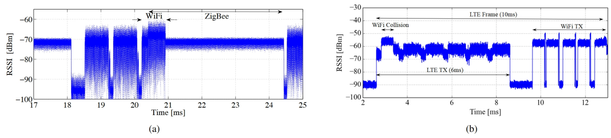


Fig. 9: Interference between technologies: (a) RSSI detected WiFi-ZigBee Power Signal and (b) WiFi-LTE collision [38]

Nguyen et al. [37] propose a wide band, real time, Spectro-Temporal RF Identification system to detect, classify, and locate Radio Frequency (RF) emissions in time and frequency using RF samples of 100 MHz bandwidth spectrum. The systems combines a one-stage object detection deep learning network with the YOLO object detection algorithm [41]. Accordingly, wide-band RF samples are transformed into a 2D time-frequency image based on which individual and overlapping RF emissions are identified, localized, and classified. The transformation of the raw RF samples to visual data follows after the I/Q data stream are divided into equal chunks and N-point FFT is applied to each chunk. The authors report a detection accuracy of 99%.

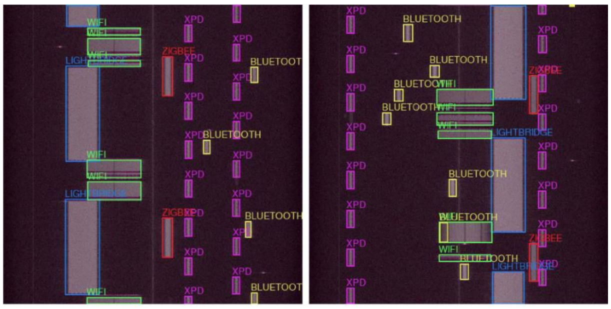


Fig. 10: Different wireless devices RF detection in congested environment[37]

Table 2 summarises some of the CTI detection approaches we reviewed in this section.

In [42, 43], the authors compare different lightweight machine learning classification models, observing that RSSI signal traces with bandwidth in the order of a few kHz lead to a poor representation of the signal envelope and undermine the classification accuracy of single signal bursts. Alternative to RSSI, the authors propose to directly detect the envelop of a received signal. The authors demonstrated that this can be carried out with off-the-shelf IEEE 802.1.4-compatible devices. According to the authors, the spectral features of the envelop reveal rich insights which are useful for training different machine learning models. This approach not only enables the detection and classification of interference sources, but also is able to resolve multiple sources when they cause interference at the same time.

[3] https://www.ti.com/product/CC2420. Last visited: 01 October 2024, 11:42 AM CET.

[4] https://ww1.microchip.com/downloads/en/DeviceDoc/39776C.pdf. Last visited: 01 October 2024, 11:44 Am CET.

5 Avoidance

Even though avoidance strategies are in essence coexistence strategies, we discuss them separately because they commonly rely on dynamic channel selection. Of course, CTI avoidance can also take place in space and time as well. The former requires the adaptation of some aspects of the physical layer (transmission power, antenna selection, antenna positioning, antenna orientation, etc.) which incurs either a considerable performance penalty to all the networks concerned (but, particularly, to the low-power networks) or restriction on their mobility. The latter, too, requires some form of coordination, the estimation of the optimal length of a time frame and the number of time slots as well as time synchronization. Discussion on these aspects is differed to Section 7. Dynamic channel selection (frequency hopping) overcomes all these restrictions, but consists of identifying the best channel; determining the timing of channel hopping; and a strategy to convey channel transition between communicating partners. According to Incel et al. [44], proposed approaches supporting dynamic channel selection in IEEE 802.15.4 networks can be classified based on 7 principal aspects. These are:

1. The purpose of channel selection.
2. The channel assignment strategy.
3. The presence or absence of a control channel.
4. Centralised vs. decentralised approach.
5. Whether all the nodes in the networks communicate using a single channel or whether the use of multiple channels is supported.
6. The medium access mechanism.
7. Whether the strategy supports packet broadcasting.

To these aspects we identify one additional feature, namely, whether channel selection is carried out by a transmitter or a receiver. Most existing approaches are transmitter-initiated, distributed, and enable the use of multiple channels. In Section 7 we shall discuss in detail the Time-Slotted Channel Hopping (TSCH) protocol – one of the protocols in low-power networks which are integrated in the IEEE 802.15.4 specification – and some variants of it.

Tytgat et al. [45] propose a receiver-initiated dynamic channel selection intending to optimise the total average packet error rate (PER) in the network. The authors attempt to achieve this goal – even though nodes make local decisions – by defining a metric which aims to identify a channel with the lowest average measured channel power. The authors compare this metric with three competitive metrics, namely,

- "activity": ranks CTI based on averaged, minimum, and maximum measured channel powers, thus: (avg - min)/(max - min).
- "min": selects the channel wherein the minimum measured channel power is the lowest as a receiving channel.
- "max": selects the channel wherein the maximum measured power is the lowest at a receiving channel. .

Channel ranking is carried out at runtime, with each node sampling the interference levels on the different channels. According to the authors, packet error rate (PER) is minimised when each individual node selects the channel with the estimated least average PER. Nodes wishing to communicate with this node, should discover its receiving channel, in the same way WiFi devises identify the channel at which an access point listens or a Bluetooth slave device following the hopping sequence of its master.

Channel blacklisting [32–34] facilitates channel selection in the presence of persistent CTI. Iyer et al. [35] carried out interference detection, classification, and channel recommendation (blacklisting) based on the offline evaluation of various WiFi and Bluetooth traffic channel utilisation characteristics and their impact on low-power IEEE 802.15.4 networks. Interference patterns are established by classifying RSSI bursts using predetermined RSSI intervals, persistent duration, and variance (a clustering component groups together RSSI bursts which are likely to come from the same CTI source). In a subsequent step, the patterns are mapped to different network traffic models using a k-mean classification. This results in distinguishing between different data traffics (WiFi beacons, periodic and non-periodic channel traffic) and in estimating the number of sources transmitting periodic signals (WiFi access points).

The authors evaluated their approach using a network of 85 sensor nodes, each node generating 1 packet per minute over a two-hour duration. Interference avoidance has been carried out by ranking the channels according to their RSSI patters. The experiment results suggest that an improvement of a 30% average throughput can be achieved in comparison to other interference avoidance techniques. This achievement was mainly due to the blacklisting of channels which were likely to suffer from CTI arising from nearby WiFi networks.

More recently, researchers have started to employ machine learning to model and mitigate the impact of CTI. In [46], the authors propose a convolutional neutral network (CNN) to transform a noisy spectrogram into a clean range profile for radar sensors. The model was trained with different real world radar signals (with and without interference and captured by NXP TEF810X 77 GHz radar transceiver [47]) representing different range profiles. The authors introduce two metrics to evaluate the performance of their model, namely, the probability of false alarm and the mean absolute error. The former is tested by measuring the receiver operating characteristics curve at various threshold and the later measures the error between the range profile amplitude of targets computed from a level signal and a predicted target signal. In [48], a recurrent neutral network (RNN) is proposed to mitigate interference between Frequency Modulated Continuous Wave (FMCW) [49] and OFDM radar signals. Since radar signals vary over time, the model is augmented with multi-layer gated recurrent unit (GRU) cells [50] to deal with gradient vanishing arising from signals disappearing with increasing time steps. Moreover, in order to maintain the relationship between the entire time steps, the authors add an attention block [51] to the RNN layer. The authors assumed up to 5 targets and 8 interference sources to be experienced at the same time and considered three types of interference (Chirp Sequence, triangle FMCW, and multiple frequency shift keying). In [52], the authors employ different CNN models to mitigate CTI in satellite-to-ground links. The proposed model is trained to identify the sources of received signals (signal of interest) and to classify the modulation schemes with which these signals are modulated (the model is trained to discriminate between the standard DBB-S2 modulation schemes, namely, QPSK, 8-APSK, 16-APSK and 32-APSK). The model was trained with a video stream modulated by a GNU radio, and transmitted using a USRP-N210 [53]. Three different jamming signals – Continuous Wave Interference (CW), Multi Continuous Interference (MC), and Chirp Interference (C)– were used to generate interference:

$$\begin{aligned} CW &= e^{j2\pi f_i t} \\ MC &= e^{j2\pi f_j t} + e^{j2\pi f_k t} \\ C &= e^{j2\pi\left(\frac{f_l - f_m}{2T}t^2 + f_m t\right)} \end{aligned} \tag{2}$$

where $f_i \dots f_m$ are sweeping frequencies and T the sweeping period, respectively. Fig. 11 displays different scalogram plots illustrating the characterisation of clean and noisy signal of interest.

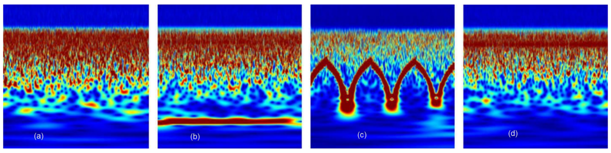


Fig. 11: A scalogram plot of the RFI data set from [52]. (a): The original signal of interest with no interference; (b): The signal of interest(SoI) with multi-continuous wave interference; (c): The signal of interest with chirp interference; (d) The signal of interest with continuous wave interference.

6 Coexistence

When multiple wireless technologies concurrently operate in the same frequency band without significantly affecting their performance or the performance of the other technologies, this condition is known as "coexistence". Garroppo et al. [19] carried out a controlled experiment to investigate the extent to which IEEE 802.11 b/g/n, IEEE 802.15.1, and IEEE 802.15.4 specifications enable coexistence.

Accordingly, the WiFi devices operate on Channel 6; the Zigbee, on Channel 18; and the Bluetooth, spanning the 2.4 GHz band. As mentioned in Section 3, the three most frequently used non-overlapping WiFi channels are 1, 6, and 11. In the 802.15.4 specification, Channel 18 is totally

CTI Avoidance			
Research Papers	Research aim	Avoidance method	Technical features
[30, 35, 54]	Interference detection and mitigation	Apply supervised and unsupervised Deep Learning to classify interference patterns	Exploitation of knowledge of modulation schemes and bit corruption patterns.
[46]	Interference classification and mitigation	A fully convolutional neural network to discriminate between different modulation schemes	Produce clean radar signal from corrupted signal.
[48]	Interference mitigation for radar signals	Use of recurrent neutral networks (RNN) to recover corrupted Frequency Modulated Continuous Wave (FMCW) radar signals	Increase the capacity of detecting radar targets in the presence of strong ambient noise (Interference)
[45]	Performance improvement in the presence of strong CTI	Multichannel protocol for supporting time-slotted and frequency hopping medium access	Analysis and experimental verification of frequency-based interference avoidance mechanism
[55, 56]	Overcoming the limitations of TSCH and CSMA/CA-based schedulers	Adaptive channel hopping based on single-hop neighborhood coordination in multi-radio communication	Minimise the effect of interference and maximise network performance in the presence of concurrent networks

Table 3: Review of CTI avoidance mechanisms.

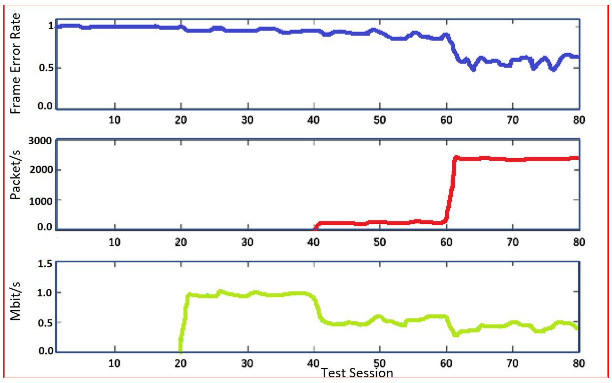


Fig. 12: Patterns of interference when three technologies operate concurrently. Bluetooth (bottom), WiFi (Centre), and IEEE 802.15.4 (top). FIR stands for Frame Error Rate. 1-FER = 1 is equivalent to no frame error rate; 1-FER= 0.5, 50% frame error rate; 1-FER = 0, 100% frame error rate .

overlapped with the 802.11 b/g Channel 6. In the beginning, the WiFi and the Bluetooth devices were inactive while two ZigBee devices[5] exchanged packets undisturbed. During this time almost all the packets were delivered successfully. After the 20th session, the Bluetooth devices become active and started to exchange packets at 1 Mbps rate. This time the ZigBee devices started to experience moderate packet loss. After the 40th session, the WiFi devices became active, thus causing the other devices to experience appreciable packet losses. The authors gradually increased the WiFi devices' packet transmission rate and by the time they reached 2500 packets per second, the performances of the ZigBee and the Bluetooth devices were severely constrained, the devices most affected were the Bluetooth devices,

[5] When the context is clear we refer to networks the nodes of which rely on IEEE 802.15.4 compatible radios as low-power networks.

as can be seen in Fig.12. Moreover, the experiment results suggest that Bluetooth and ZigBee coexist without appreciably affecting each other's performance.

Advanced coexistence strategies closely examine opportunities at the physical layer to enable concurrent transmission. For outdoor deployments, the two most important technologies which require coexistence are those based on the IEEE 802.15.4 and IEEE 802.11 b/g/n standards. Medium access in these technologies is based on a clear channel assessment (CCA) which, theoretically, should enable these technologies to share a common medium fairly. However, due to a significant disparity in their transmission power and radio sensitivity, the latter often fail to sense the activities of the former (their default threshold power is much higher than the nominal transmission power of 802.15.4 devices). Even if low-power activities were possible to detect, medium sharing on the basis of CCA alone is not advantageous to WiFi networks due to a big disparity in data rate. Low-power networks achieve much smaller bit rates and significantly longer transmission time, so that their medium occupation time to transmit a single packet will be deemed unfair.

One of the most closely investigated features for enabling coexistence is spectrum reuse. Specifically, WiFi technologies employ OFDM due to its several advantages, including efficient use of a spectrum, resilience to frequency selective fading, and computation efficiency. In OFDM, a channel is divided into multiple orthogonal subcarriers, some of which are used to modulate data and some, as pilot tones. The latter are used to convey a predefined data sequence which is used to determine the difference, or error, between an ideal signal and a received signal. In other words, pilot tones are used for synchronisation and easy signal detection. Each of the data subcarriers can be modulated using BPSK, QPSK, 16-QAM or 64-QAM. One interesting aspects is that, it is possible to selectively avoid using some of these data subcarriers, so that the spectrum occupied by them can be available for the low-power networks to concurrently transmit packets. Intelligent channel assignment is required on both sides. WiFi devices need to determine the subcarriers overlapping with some of the IEEE 802.15.4 channels in order to free them, whereas the low-power devices need to scan the available spectrum to determine the best channels for concurrent transmission.

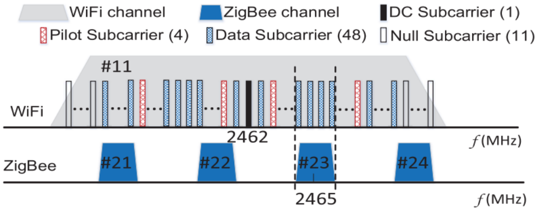


Fig. 13: Overlapping OFDM data subcarriers which can be freed for concurrent transmission by IEEE 802.15.4 low-power networks [57].

More recently, researchers have started to explore mechanisms which enable direct communications between heterogeneous networks in order to coordinate channel assignments. The approaches are collectively known as cross-technology communication (CTC) [58, 59]. Here as well, knowledge of frame structure, medium access mechanism, modulation, channel state information, etc. is exploited to enable direct communication. The prevailing idea is the following: A WiFi device having ample resources senses the presence of a low-power device in the vicinity and encodes a hint as regards its channel utilisation and transmission strategy in its outgoing packets in such a way that the low-power device is able to decode the hint to either adapt its transmission timing or select a complementary channel to avoid CTI [58].

In [59], at a WiFi transmitter a message is deliberately generated, so that when it undergoes the entire modulation and frame structuring, it can be received, demodulated, and decoded as a legitimate IEEE 802.15.4 packet. Accordingly, the message is first encoded into a set of Quadrature Amplitude Modulation (QAM) constellation points. Secondly, the points are modulated into 48 data sub-carriers using OFDM. Thirdly, the modulated subcarriers are combined using the Inverse Fast Fourier Transform (IFFT). Fourthly, the time-domain OFDM symbol is prefixed by the cyclic prefix (CP), which is a necessary part of the OFDM symbol to offset the multi-path channel effect. Having thus generating a sequence of WiFi symbols, a packet is transmitted by the WiFi RF radio. On the receiver side, the WiFi header, preamble, and trailer will be regarded as noise and, therefore, will be ignored; the payload, however, will be received, demodulated, and decoded. The process is certainly error prone, but the approach relies on the receiver's (IEEE 802.15.4) capability to detect and decode even corrupted symbols.

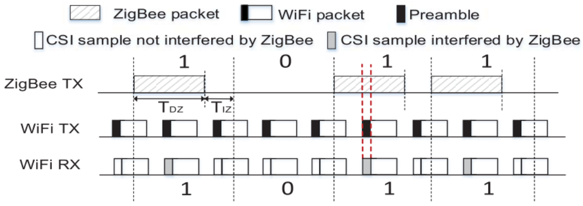


Fig. 14: Superimposing IEEE 802.15.4 packets on WiFi packets to create a desirable CSI in order to implicitly enable a direct cross-technology communication [57].

In [57], the authors exploit Channel State Information (CSI) to enable a low-power device to transmit a coordination message to a resource-rich WiFi device. CSI enables a WiFi receiver to measure the channel status for each OFDM subcarrier during packet reception. Measurement includes phase shift and amplitude variations of a received signal from a reference signal (RSSI is sampled at ca. 31 KHz and phase shift detection is made at 4 MHz [60]). For the low-power device to successfully transmit a coordination message, it has to overlap its packets with the packet of a nearby WiFi transmitter, so that the superposition of the two signals at the WiFi receiver produces the desired CSI. The idea is illustrated in Fig. 14. In the figure, the low-power device wishes to transmit the bit stream 1101 and estimates the transmission pattern of the nearby WiFi transmitter with whose packet it overlaps its own packets, destining them to a common receiver. When the overlap is successful, this will be encoded by the receiver as "1", otherwise, as "0". In the meantime, the WiFi device will also successfully intercept the packet from its peer, taking into account the channel state information. In [59], the authors combine CTC with forward error correction to achieve reliable data dissemination from a WiFi Access Point (AP) to a ZigBee network in the presence of a considerable packet loss.

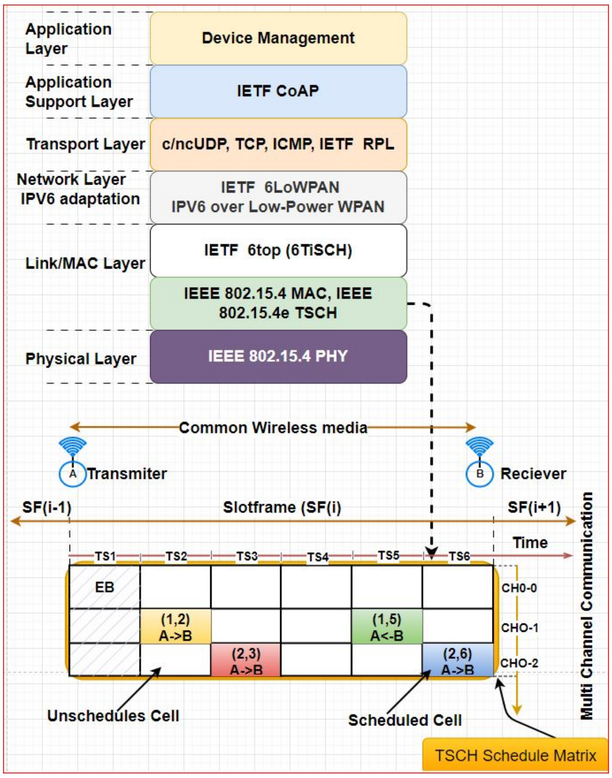


Fig. 15

Two IoT nodes communicating over the 6TiSCH protocol stack.[6]

The proposed solution explores chip-level error patterns and attempts to correct emulation errors by assuming that some errors are more likely to occur than others. The authors claim that chips in some positions of a symbol are more prone to error than others. Accordingly, the authors leverage the cyclic-shift feature of Pseudo Random (PN) sequence and combine parts of correct chips in different sequences into a complete and correct symbol without even accessing the chip information hidden by the hardware.

[6] *c/cn UDP: Compressed /not compressed user data gram protocol
*CoAP: Constrained Application protocol
*ICMP: Internet Control Massage Protocol
*TCP: Transmission Control Protocol,
*Ts: Time Slot , SF : Slot Frame,
*CHO : Channel offset, EB: Enhanced Beacon, Cell (CHO,TS)

7 System Support

The problem of CTI is well-known amongst system software and protocol developers for low-power networks [61]. The two widely used run-time environments, namely, CONTIKI [62] and RIOT [63], provide system support (message propagation, distributed time synchronisation, beacon propagation, scheduling) for easy implementation and configuration of CTI-aware protocols. The 6LoWPAN [64] protocol stack (Fig. 15) likewise accommodates protocols which aim to mitigate CTI. In the next subsection, we concisely present one of the most widely employed medium access protocols, which was initially proposed to deal with CTI in industrial IoT [6].

7.1 Time-Slotted Channel Hopping

Time-Slotted Channel Hopping (TSCH) is one of the most widely used medium access protocols in low-power wireless networks. Initially proposed to mitigate multi-path fading and interference due to electromagnetic noise [65] in industries, it has now become a part of the IEEE 802.15.4 specification and implementations exist for the CONTIKI and RIOI platforms. As its name suggests, TSCH combines the two well-known multiple access techniques, namely, Time Division Multiple Access (TDMA) and Frequency Division Multiple Access (FDMA). The protocol presupposes time synchronisation but gives allowance to some degree of synchronisation error, which is inevitable in resource-constrained devices.

Packet transmission in TSCH takes place in fixed time slots and time slots are organised into frames. The length of a slot is not fixed, as it depends on many factors (including the size of the network) [65], nevertheless, in the literature a slot length is typically between 10 and 20 ms [66], 10 ms being the most widely adopted. An illustration of a unicast communication between a transmitter and a receiver pair (RX ↔ TX) (assuming a slot length of 10 ms) is depicted in Fig. 16. Referring to the table at the bottom in Fig. 15, the rows signify the channel offsets, whereas the columns, the slot offsets. Similarly, a cell in the table describes a specific medium access configuration or schedule.

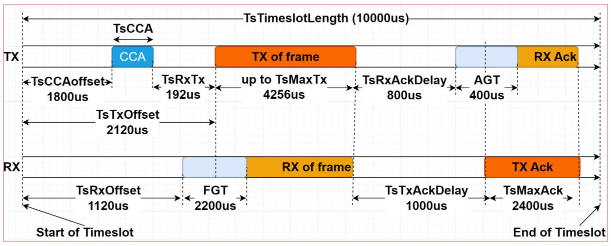


Fig. 16

Packet transmission between two IoT nodes using the TSCH protocol.[7]

7.1.1 Packet Reception

Initially, a receiving node is either in a sleep or an idle state. Packet reception begins when it turns on the radio and prepares for receiving a packet. The transition (TsRxOffset) consists of determining that the medium is free. If it is, the receiver listens for a duration of Frame Guard Time (FGT), waiting for to a valid frame to arrive. If the channel's state does not change after this time, (i.e., the radio does not detect a signal power exceeding a threshold value), it transits back to an idle or a sleep state (depending on the dynamic power management policy); otherwise, it begins receiving a packet. Following a successful reception, it transits to a transmission state. The transition takes some time (TsTxAckDelay) as the receiver switches the radio from a receiving to a transmission mode and prepares an acknowledgement packet.

7.1.2 Packet Transmission

A transmitter transits from a sleep or an idle state to a transmit state. The transition consists of making the packet ready for transmission (adding link layer headers to the data frame, performing encryption if security is required, copying the data frame to the radio buffer, and performing clear channel assessment). The time allocated for the

[7] *CCA: Clear Channel Assessment,
*Rx: Receiver,
*Tx: Transmitter,
*Ts: Timeslot,
*TsCCA: Duration of CCA
*TsCCAOffset: Time to start the CCA operation,
*TsRxTx: Transition time to frame transmission,
*TsRxAckDelay: Transition time to ACK reception,
*TsTxAckDelay: Transition time to ACK transmit,
*TxMaxAck: Maximum duration of ACK,
*AGT : ACK Guard Time ,
*FGT: Frame Guard Time

transition (TsTxOffset) must be long enough to make a packet ready for transmission, including the time needed for queuing and for the transmission of a preamble and the Start of Frame Delimiter (SFD). Similarly, the transmission duration of the frame that follows the SFD must be equal or smaller than the duration required to transmit the longest frame. The maximum frame length in IEEE 802.15.4 is 128 bytes. Once a packet transmission is over, the node transits to a receive state to await an acknowledgement. The time allocated for the transition is TsRxAckDelay. A minimum amount of time (AGT) must expire to determine whether a packet transmission was a success or a failure.

TSCH deals with interference by relying on channel hopping, using channel offset schedules [55]. However, the offset schedule is pseudo-random in that a predefined and globally shared sequence of channels is employed to determine the jump sequence between channels. Equation (3) describes the jumping function:

$$C_{ch} = C_{map}[ASN + CH_{off}]mod\ N_{ch}. \tag{3}$$

where C_{ch} is the new mapped channel, ASN stands for Absolute slot number, CH_{off} is the channel offset of the communication link between two participant nodes, N_{ch} is the length of the channel hopping sequence; and C_{map} is the channel mapping function. TSCH performs well when the network size is relatively small (relative to the available channels) and the interference magnitude is modest. It is, however, vulnerable to selective external interference such as jamming attacks, as it lacks the capacity to (1) learn the characteristics of the perceived interference and (2) adapt its hopping pattern in accordance with the channel condition. Secondly, the number of active transmission links in the network must be at most N_{ch} to avoid packet collision arising with thin the same network.

7.2 TSCH Variants

Channel hopping in multi-channel multi-radio wireless mesh network has been studied in [67] using spectrum efficiency gain as a performance metric. As can be observed in Fig. 15, each packet transmission (and retransmission), takes place in different channel. The channel is selected randomly based on a pseudo-random pattern. The study suggests that the approach reduces interference and improves reliability. Nevertheless, the approach performs well when the interference arises from within the same network. A similar study is carried out in [68] using an adaptive frequency channel hopping based on a Model-free and a Model-based schemes. The former assumes that statistics pertaining to channel dynamics are available at design time, whereas the latter typically employs machine learning to establish and react to channel dynamics [69]. Hence, each node in a network is regarded as a learning agent which gradually estimates channel dynamics based on its short-term experience. As a result, the node inclines to favour those channels with higher success rate for its future transmission [68].

Javan et al. [68] model CTI as a non-stationary random variable and the task of identifying the next best transmission channel, as a Dynamic Multi-Armed Bernoulli Bandit (Dynamic MABB) process [70]. The authors then propose an online learning algorithm with tracking ability for computing the best adaptive hopping policy. The work in [71] attempts to detect and model multiple sources of periodic interference in time-slotted medium access protocols, with the end goal being estimating both the channels and the length of the time windows of future transmissions. The task is formulated as a Multi Hypothesis Tracking problem (MHT) [72].

In [33], the authors integrate channel blacklisting with TSCH to mitigate CTI. The proposed approach is decentralised and enables any pair of receiver/transmitter nodes to negotiate a local blacklist, based on the estimation of packet delivery ratio. The channel quality estimation itself is modelled as a multiarmed bandit problem. Dynamic channel selection is carried out by combining three key algorithms: The first algorithm (which is centrally executed and its results are used by a path computation element) is responsible for computing and disseminating the TSCH schedule (channel offsets). This is the basis for all subsequent dynamic channel selections. The second algorithm enables nodes to exchange information about blacklisted channels by piggybacking blacklisting information into data and ACK frames. The third algorithm identifies channels suffering from CTI and blacklists them and maintains the list containing blacklisted channels.

8 Impacts of Interference

CTI is disruptive. It corrupts packets and inhibits medium access. If packet retransmission is not required, the cost of CTI will be manifested mainly in terms of poor packet reception ratio and high latency. If retransmission is required, the cost will be manifested mainly in terms of high energy cost, short network lifetime, and latency, among others. In order to estimate the energy cost of retransmission, one has to first estimate the transmission and reception cost of a single packet. Nominal values can be obtained from the radio data-sheet once the type of the radio is known, but often this alone is not sufficient because the transmission of a packet involves multiple layers, the management of which varies from operating system to operating system. In the following subsections, we present some experimental studies which highlight the cost of CTI in terms of energy and loss of performance.

8.1 Energy

Stefano et al. [73] investigate the energy cost of various activities using OpenMote B platforms [74] and the OpenWSN runtime environment [75]. The runtime environment includes a complete implementation of the 6TiSCH protocol stack (refer Figure 15), including TSCH as its medium access protocol. (A similar investigation is carried out using the CONTIKI operating system somewhere else [76]). The OpenMote B platform is based on the CC2538 system-on-chip, which, in turn, integrates an IEEE 802.15.4-compliant 2.4 GHz radio. To measure the current flowing into various sub-components, the authors employed an oscilloscope and disabled all LEDs to exclude their power consumption from further consideration. Thus, the power consumption of a node was segmented into a transmission cost, a receiving cost, a listening cost, and a computation (idle) cost. A transmission cost includes the cost of transmitting a data packet and receiving an acknowledgement packet. Similarly, a receiving cost includes the cost of receiving a data packet and transmitting an acknowledgement packet. As can be seen in Figure 17, tracing the power consumption (current drain) of a single node enables to estimate the beginning and end of a TSCH time slot − for the experiment, a time slot had a duration of 20 ms − by considering the receiving and transmitting characteristics of the node. But more importantly, the study clearly shows that the transmission and receiving cost by far dominate the power consumption of all other activities, suggesting that upon experiencing a collusion due to CTI, the cost of packet retransmission is high.

8.2 Network Performance

Packet loss and packet delivery latency are two of the most important performance losses resulting from CTI. The latter consists of extended medium access time, extended routing time (packet reaches its destination via multiple links), retransmission delay, and delay due to congestion.

Liang et al. [77] experimentally investigated the impact of CTI on the performance (packet loss and latency) of IEEE 802.15.4 networks when operating in the vicinity of 801.11b and 802.11g networks. A series of experiments were conducted in a quasi-isolated environment (the basement of a big building), thus ensuring that the predominant CTI was from within the experiment setup. The major contribution of this work is the employment of a special narrow band radio (RFMD ML2724) which enabled the interception of RF transmission originating from IEEE 802.15.4 transmitters. The radio enables the bit-by-bit decoding of the RF signal to determine the exact location and patterns of bit errors resulting from CTI. In other words, when placed near an 802.15.4 receiver, the narrow band radio enables to experience the impact of the CTI which the low-power receiver is subjected to. The radio can be tuned to a central frequency between 2400 and 2485 MHz and generates an analog voltage directly proportional to an RF signal energy with a 2 MHz bandwidth. For their experiments, the authors chose Channel 22 for the IEEE 802.15.4 network and Channel 11 for the 802.11b/g networks. A low-power transmitter broadcast packets having 128 byte size to multiple receivers at 75 ms interval. The narrow band radio as well as the low-power receivers kept record of lost packets, packets with CRC errors, and packets which were received successfully. Based on the

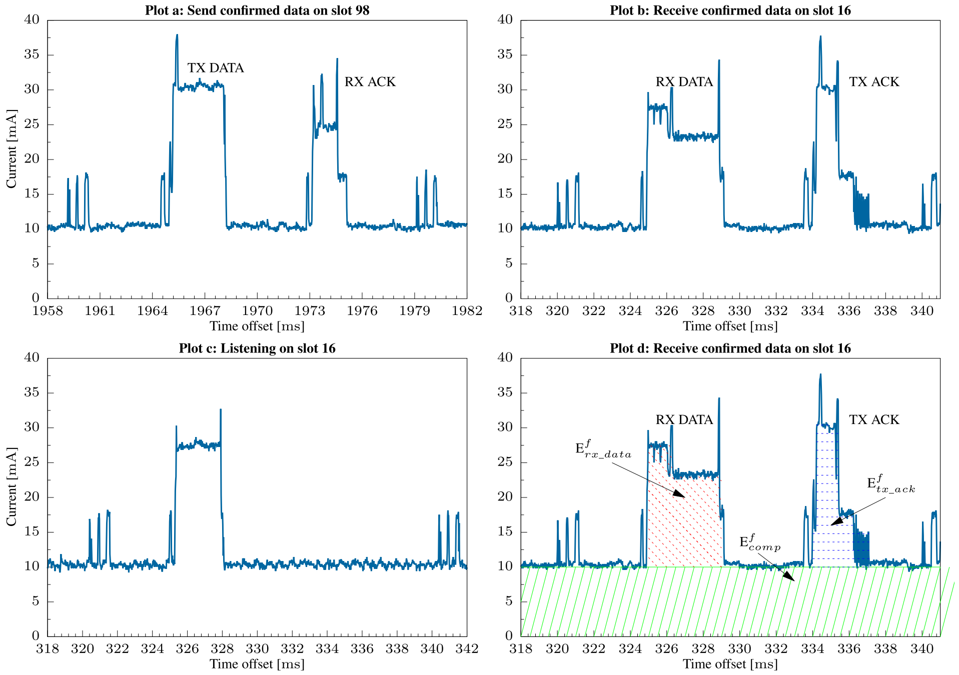


Fig. 17: Power consumption for the different TSCH cells, (a) A slot wherein a data packet is transmitted and an ACK packet is received. (b) A slot wherein a data packet is received and an ACK packet is transmitted. (c) An idle time slot. (d) Dissection of overall consumption into the cost of different activities [73].

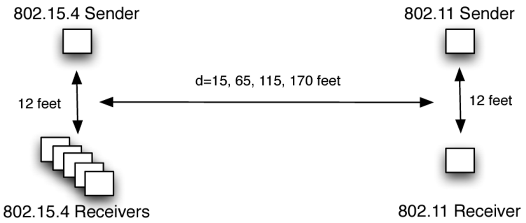


Fig. 18: Experimental setup of two heterogeneous networks operating in a self-induced CTI [77].

analysis of these statistics, the authors made the following observation:

- Packets originating from 802.11b networks had a much higher impact on the overall 802.15.4 packet reception rate than those originating from IEEE 802.11g networks – the authors attributed this to the higher transmission rate (i.e., lowers channel occupation time) of 802.11g networks.
- The number of lost packets was larger than the number of packets received with bit errors. This suggests that the synchronisation header (SHD) – a combination of the preamble and Start-of-Frame Delimiter (SFD) – was more vulnerable to 802.11 interference. This is particularly the case when the cause of the CTI was the IEEE 802.11b network.
- Packet transmission latency increased by as much as 13% to 40% in the presence of 802.11g and 802.11b traffic, respectively.
- By contrast, the WiFi networks suffer a modest amount of packet loss when the transmission power of the IEEE 802.15.4 transmitter was at its highest and its distance to the 802.11 network was approximately 15 feet.

Hithnawi [8] carried out a series of experiments similar to that of Liang et al., but arrived at a slightly different conclusion. For their experiments, the authors chose an anechoic chamber having dimensions: 7 m × 4 m × 4 m. An IEEE 802.15.4 transmitter transmits variable sized packets (20, 40, 100 bytes) at variable transmission power levels (0 dBm, -3 dBm, and -10 dBm) and intervals. At the same time a nearby WiFi device was interacting with a router in different configurations: accessing the medium with and without a clear channel assessment; and transmitting TCP and UDP packets at different intervals and with a transmission power which was gradually adjusted from -20 dBm to 20 dBm. The authors observed that configuring the WiFi network to perform with or without clear channel assessment had little impact on the reduction of CTI or its impact, as the networks (802.11 b/g) failed to detect the activities of the nearby low-power networks. On the other hand, the traffic pattern and size of the WiFi networks had a considerable impact. Thus, when their traffic was modest, it made no appreciable impact on the performance of the low-power networks; but when the traffic was dense and frequent (packets transmitted every 7 ms), it reduced the performance of the low-power networks by up to 20%.

9 Conclusion

The joint deployment of heterogeneous wireless networks is presenting a great opportunity to support a wide range of critical applications. In industrial IoT, wireless sensors, mobile robots, and other objects can seamlessly interact to facilitate safe and efficient operations. In water quality monitoring, Unmanned Aerial Vehicles, Unmanned Surface Vehicles, and wireless sensor networks can be deployed to monitor the quality of an extensive water body. Because of the safe operation of the mobile robots, the UAVs, and the USVs is critical not only to fulfill the purpose for which they are deployed but also because of their cost and the damage they may cause in case of error in their navigation plan, often they require highly reliable links. For these reasons, they rely on wireless links that afford them with high transmission power and wide bandwidth. By contrast, most existing sensing networks are low-power networks. Consequently, when such heterogeneous networks operate in close proximity to each other sharing a common spectrum, a cross-technology interference ensues and the impact of this interference is not reciprocal.

In this paper we reviewed various strategies to detect and deal with cross-technology interference. The detection strategies range from high-level strategies which attempt to statistically model network traffic and estimate traffic patterns and interval to enable packet scheduling to low-level signal processing which attempt to take advantage of knowledge of modulation and channel coding to analyse patterns of symbol corruption and bit errors. Similarly, the coexistence strategies strive to enable concurrent operations by employed high-level as well as low-level strategies. More recently, researchers have also started investigating ways for enabling direct communication between heterogeneous networks to coordinate channel assignment and mitigate cross-technology interference.

In this paper we have not investigated the cost of managing cross-technology interference. This is rather important considering the fact that some of the strategies are low-level and require a considerable computation. For example, some of the strategies aiming to enable direct cross-technology communication, rely on knowledge of the communication pattern of active networks to overlap packets and, thereby, convey a message on signals superimposed by the heterogeneous networks. This requires precise timing and fine-grained estimation. Our plan for the future is to address such issues and to quantitatively compare the performance of some of the proposed approaches.

Conflict of Interest

On behalf of all authors, the corresponding author states that there is no conflict of interest.

References

[1] Sundmaeker, H., Guillemin, P., Friess, P., Woelfflé, S., *et al.*: Vision and challenges for realising the internet of things. Cluster of European research projects on the internet of things, European Commision **3**(3), 34–36 (2010)

[2] Dargie, W., Poellabauer, C.: Fundamentals of Wireless Sensor Networks: Theory and Practice. John Wiley & Sons, ??? (2010)

[3] Primicerio, J., Di Gennaro, S.F., Fiorillo, E., Genesio, L., Lugato, E., Matese, A., Vaccari, F.P.: A flexible unmanned aerial vehicle for

precision agriculture. Precision Agriculture **13**(4), 517–523 (2012)

[4] Boursianis, A.D., Papadopoulou, M.S., Diamantoulakis, P., Liopa-Tsakalidi, A., Barouchas, P., Salahas, G., Karagiannidis, G., Wan, S., Goudos, S.K.: Internet of things (iot) and agricultural unmanned aerial vehicles (uavs) in smart farming: A comprehensive review. Internet of Things **18**, 100187 (2022)

[5] Dunbabin, M., Grinham, A., Udy, J.: An autonomous surface vehicle for water quality monitoring. In: Australasian Conference on Robotics and Automation (ACRA), pp. 2–4 (2009). Citeseer

[6] Sisinni, E., Saifullah, A., Han, S., Jennehag, U., Gidlund, M.: Industrial internet of things: Challenges, opportunities, and directions. IEEE transactions on industrial informatics **14**(11), 4724–4734 (2018)

[7] Dargie, W., Wen, J., Panes-Ruiz, L.A., Riemenschneider, L., Ibarlucea, B., Cuniberti, G.: Monitoring toxic gases using nanotechnology and wireless sensor networks. IEEE Sensors Journal (2023)

[8] Hithnawi, A., Shafagh, H., Duquennoy, S.: Understanding the impact of cross technology interference on ieee 802.15. 4. In: Proceedings of the 9th ACM International Workshop on Wireless Network Testbeds, Experimental Evaluation and Characterization, pp. 49–56 (2014)

[9] Gollakota, S., Adib, F., Katabi, D., Seshan, S.: Clearing the rf smog: making 802.11 n robust to cross-technology interference. In: Proceedings of the ACM SIGCOMM 2011 Conference, pp. 170–181 (2011)

[10] Tuch, B.: Development of wavelan®, an ism band wireless lan. AT& T Technical Journal **72**(4), 27–37 (1993)

[11] Carbonell, A., Joykutty, L., Velde, B.: Seagrass fatalities in north biscayne bay, south florida due to increases in nutrients and macroalgae in its environment. Journal of Student Research **10**(3) (2021)

[12] Bradbury, M.: Site prioritization and the reproduction of inequity in the restoration of biscayne bay. The Canadian Geographer/Le Géographe canadien **67**(1), 92–105 (2023)

[13] Dargie, W., Kidane, Z.M.: Mitigating cross-technology interference in low-power wireless networks. In: 2024 33rd International Conference on Computer Communications and Networks (ICCCN), pp. 1–8 (2024). IEEE

[14] Clausen, T., Herberg, U., Philipp, M.: A critical evaluation of the ipv6 routing protocol for low power and lossy networks (rpl). In: 2011 IEEE 7th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), pp. 365–372 (2011). IEEE

[15] Vikram Kulkarni, K.V.L.N., Sahoo, S.K.: A survey on interference avoiding methods for wireless sensor networks working in the 2.4 ghz frequency band. Journal of Engineering Science and Technology (13), 59–81 (2020)

[16] He, Y., Guo, X., Zheng, X., Yu, Z., Zhang, J., Jiang, H., Na, X., Zhang, J.: Cross-technology communication for the internet of things: A survey. ACM Comput. Surv. **55**(5) (2022) https://doi.org/10.1145/3530049

[17] Szott, S., Kosek-Szott, K., Gawłowicz, P., Gómez, J.T., Bellalta, B., Zubow, A., Dressler, F.: Wi-fi meets ml: A survey on improving ieee 802.11 performance with machine learning. IEEE Communications Surveys & Tutorials **24**(3), 1843–1893 (2022) https://doi.org/10.1109/COMST.2022.3179242

[18] Shin, S.Y., Park, H.S., Choi, S., Kwon, W.H.: Packet error rate analysis of zigbee under wlan and bluetooth interferences. IEEE Transactions on Wireless communications **6**(8), 2825–2830 (2007)

[19] Garroppo, R.G., Gazzarrini, L., Giordano, S., Tavanti, L.: Experimental assessment of the coexistence of wi-fi, zigbee, and bluetooth

devices. In: 2011 IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks, pp. 1–9 (2011). https://doi.org/10.1109/WoWMoM.2011.5986182

[20] Adams, J.T.: An introduction to ieee std 802.15. 4. In: 2006 IEEE Aerospace Conference, p. 8 (2006). IEEE

[21] Wen, J., Dargie, W.: Evaluation of the quality of aerial links in low-power wireless sensor networks. IEEE Sensors Journal **21**(12), 13924–13934 (2021)

[22] Dargie, W., Wen, J.: A link quality estimation model for a joint deployment of unmanned aerial vehicles and wireless sensor networks. In: 2021 International Conference on Computer Communications and Networks (ICCCN), pp. 1–9 (2021). IEEE

[23] Dargie, W.: Estimation of motion statistics from statistics of received power in low-power iot sensing nodes. IEEE Sensors Letters **8**(12) (2024)

[24] Dragulinescu, A.-M., Halunga, S., Zamfirescu, C.: Unmanned vehicles' placement optimisation for internet of things and internet of unmanned vehicles. Sensors **21**(21) (2021) https://doi.org/10.3390/s21216984

[25] Habib, A., Moh, S.: Wireless channel models for over-the-sea communication: A comparative study. Applied Sciences **9**(3) (2019) https://doi.org/10.3390/app9030443

[26] Kim, M., Lee, J.: Outage probability of uav communications in the presence of interference. In: 2018 IEEE Global Communications Conference (GLOBECOM), pp. 1–6 (2018). https://doi.org/10.1109/GLOCOM.2018.8647521

[27] Dargie, W., Padrao, P., Bobadilla, L., Poellabauer, C.: Link quality fluctuation in wireless networks deployed on the surface of different water bodies. IEEE Sensors Journal **24**(23), 39789–39797 (2024)

[28] Qin, Z., Sun, Y., Hu, J., Zhou, W., Liu, J.: Enhancing efficient link performance in zigbee under cross-technology interference. Mobile Networks and Applications **25**, 68–81 (2020)

[29] Hithnawi, A., Li, S., Shafagh, H., Gross, J., Duquennoy, S.: Crosszig: combating cross-technology interference in low-power wireless networks. In: 2016 15th ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN), pp. 1–12 (2016). Ieee

[30] Hermans, F., Rensfelt, O., Voigt, T., Ngai, E., Nordén, L.-Å., Gunningberg, P.: Sonic: Classifying interference in 802.15. 4 sensor networks. In: Proceedings of the 12th International Conference on Information Processing in Sensor Networks, pp. 55–66 (2013)

[31] Yang, P., Yan, Y., Li, X.-Y., Zhang, Y., Tao, Y., You, L.: Taming cross-technology interference for wi-fi and zigbee coexistence networks. IEEE Transactions on Mobile Computing **15**(4), 1009–1021 (2016) https://doi.org/10.1109/TMC.2015.2442252

[32] Kotsiou, V., Papadopoulos, G.Z., Zorbas, D., Chatzimisios, P., Theoleyre, F.: Blacklisting-based channel hopping approaches in low-power and lossy networks. IEEE Communications Magazine **57**(2), 48–53 (2019)

[33] Gomes, P.H., Watteyne, T., Krishnamachari, B.: MABO-TSCH: Multi-hop And Blacklist-based Optimized Time Synchronized Channel Hopping. Transactions on emerging telecommunications technologies (2017)

[34] Zorbas, D., Papadopoulos, G.Z., Douligeris, C.: Local or global radio channel blacklisting for ieee 802.15. 4-tsch networks? In: 2018 IEEE International Conference on Communications (ICC), pp. 1–6 (2018). IEEE

[35] Iyer, V., Hermans, F., Voigt, T.: Detecting and avoiding multiple sources of interference in the 2.4 ghz spectrum. In: Abdelzaher, T., Pereira, N., Tovar, E. (eds.) Wireless Sensor Networks, pp. 35–51. Springer, Cham (2015)

[36] Pulkkinen, T., Nurminen, J.K., Nurmi, P.: Understanding wifi cross-technology interference detection in the real world. In:

2020 IEEE 40th International Conference on Distributed Computing Systems (ICDCS), pp. 954–964 (2020). https://doi.org/10.1109/ICDCS47774.2020.00061

[37] Nguyen, H.N., Vomvas, M., Vo-Huu, T.D., Noubir, G.: Wrist- wideband, real-time, spectro-temporal rf identification system using deep learning. IEEE Transactions on Mobile Computing **23**(2), 1550–1567 (2024) https://doi.org/10.1109/TMC.2023.3240971

[38] Croce, D., Garlisi, D., Giuliano, F., Inzerillo, N., Tinnirello, I.: Learning from errors: Detecting cross-technology interference in wifi networks. IEEE Transactions on Cognitive Communications and Networking **4**(2), 347–356 (2018) https://doi.org/10.1109/TCCN.2018.2816068

[39] Uy, C.H., Bernier, C., Charbonnier, S.: Design of a low complexity interference detector for lpwa networks. In: 2019 IEEE International Instrumentation and Measurement Technology Conference (I2MTC), pp. 1–6 (2019). https://doi.org/10.1109/I2MTC.2019.8827022

[40] O'Mahony, G.D., Harris, P.J., Murphy, C.C.: Detecting interference in wireless sensor network received samples: A machine learning approach. In: 2020 IEEE 6th World Forum on Internet of Things (WF-IoT), pp. 1–6 (2020). https://doi.org/10.1109/WF-IoT48130.2020.9221332

[41] Jiang, P., Ergu, D., Liu, F., Cai, Y., Ma, B.: A review of yolo algorithm developments. Procedia computer science **199**, 1066–1073 (2022)

[42] Grimaldi, S., Mahmood, A., Hassan, S.A., Gidlund, M., Hancke, G.P.: Autonomous interference mapping for industrial internet of things networks over unlicensed bands: Identifying cross-technology interference. IEEE Industrial Electronics Magazine **15**(1), 67–78 (2021) https://doi.org/10.1109/MIE.2020.3007568

[43] Grimaldi, S., Mahmood, A., Gidlund, M.: Real-time interference identification via supervised learning: Embedding coexistence awareness in iot devices. IEEE Access **7**, 835–850 (2019) https://doi.org/10.1109/ACCESS.2018.2885893

[44] Incel, O.D.: A survey on multi-channel communication in wireless sensor networks. Computer Networks **55**(13), 3081–3099 (2011)

[45] Tytgat, L., Yaron, O., Pollin, S., Moerman, I., Demeester, P.: Analysis and experimental verification of frequency-based interference avoidance mechanisms in ieee 802.15. 4. IEEE/ACM Transactions on Networking **23**(2), 369–382 (2014)

[46] Ristea, N.-C., Anghel, A., Ionescu, R.T.: Fully convolutional neural networks for automotive radar interference mitigation. In: 2020 IEEE 92nd Vehicular Technology Conference (VTC2020-Fall), pp. 1–5 (2020). https://doi.org/10.1109/VTC2020-Fall49728.2020.9348690

[47] Ng, H.J., Feger, R., Wagner, C., Stelzer, A.: A fully-integrated 77-ghz radar transceiver using two programmable pseudo-random sequences. In: 2014 11th European Radar Conference, pp. 293–296 (2014). IEEE

[48] Mun, J., Ha, S., Lee, J.: Automotive radar signal interference mitigation using rnn with self attention. In: ICASSP 2020 - 2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), pp. 3802–3806 (2020). https://doi.org/10.1109/ICASSP40776.2020.9053013

[49] Wang, G., Munoz-Ferreras, J.-M., Gu, C., Li, C., Gomez-Garcia, R.: Application of linear-frequency-modulated continuous-wave (lfmcw) radars for tracking of vital signs. IEEE transactions on microwave theory and techniques **62**(6), 1387–1399 (2014)

[50] Turkoglu, M.O., D'Aronco, S., Wegner, J.D., Schindler, K.: Gating revisited: Deep multilayer rnns that can be trained. IEEE Transactions on Pattern Analysis and Machine Intelligence **44**(8), 4081–4092 (2021)

[51] Shen, T., Zhou, T., Long, G., Jiang, J.,

Pan, S., Zhang, C.: Disan: Directional self-attention network for rnn/cnn-free language understanding. In: Proceedings of the AAAI Conference on Artificial Intelligence, vol. 32 (2018)

[52] Ujan, S., Navidi, N., Jr Landry, R.: An efficient radio frequency interference (rfi) recognition and characterization using end-to-end transfer learning. Applied Sciences **10**(19) (2020) https://doi.org/10.3390/app10196885

[53] Wyglinski, A.M., Orofino, D.P., Ettus, M.N., Rondeau, T.W.: Revolutionizing software defined radio: case studies in hardware, software, and education. IEEE Communications magazine **54**(1), 68–75 (2016)

[54] Oyedare, T., Shah, V.K., Jakubisin, D.J., Reed, J.H.: Interference suppression using deep learning: Current approaches and open challenges. IEEE Access **10**, 66238–66266 (2022) https://doi.org/10.1109/ACCESS.2022.3185124

[55] Yung-Fu Chen, A.A.: Qf-mac: Adaptive, local channel hopping for interference avoidance in wireless meshes. arXiv:2212.08161 **2**(2) (2023)

[56] Krueger, L., Steenbrink, L., Timm-Giel, A.: Avoiding local interference in ieee 802.15.4 tsch networks using a scheduling function with distributed blacklists. In: Mobile Communication - Technologies and Applications; 24. ITG-Symposium, pp. 1–6 (2019)

[57] Guo, X., He, Y., Zheng, X., Yu, L., Gnawali, O.: Zigfi: Harnessing channel state information for cross-technology communication. IEEE/ACM Transactions on Networking **28**(1), 301–311 (2020)

[58] Kim, S.M., He, T.: Freebee: Cross-technology communication via free side-channel. In: Proceedings of the 21st Annual International Conference on Mobile Computing and Networking, pp. 317–330 (2015)

[59] Chen, Y., Wang, S., Li, Z., He, T.: Reliable physical-layer cross-technology communication with emulation error correction. IEEE/ACM Transactions on Networking **28**(2), 612–624 (2020)

[60] Li, Z., He, T.: Webee: Physical-layer cross-technology communication via emulation. In: Proceedings of the 23rd Annual International Conference on Mobile Computing and Networking, pp. 2–14 (2017)

[61] Silva, M., Cerdeira, D., Pinto, S., Gomes, T.: Operating systems for internet of things low-end devices: Analysis and benchmarking. IEEE Internet of Things Journal **6**(6), 10375–10383 (2019)

[62] Oikonomou, G., Duquennoy, S., Elsts, A., Eriksson, J., Tanaka, Y., Tsiftes, N.: The contiki-ng open source operating system for next generation iot devices. SoftwareX **18**, 101089 (2022)

[63] Baccelli, E., Hahm, O., Günes, M., Wählisch, M., Schmidt, T.C.: Riot os: Towards an os for the internet of things. In: 2013 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), pp. 79–80 (2013). IEEE

[64] Mulligan, G.: The 6lowpan architecture. In: Proceedings of the 4th Workshop on Embedded Networked Sensors, pp. 78–82 (2007)

[65] Ieee standard for low-rate wireless networks. IEEE Std 802.15.4-2015 (Revision of IEEE Std 802.15.4-2011), 1–709 (2016) https://doi.org/10.1109/IEEESTD.2016.7460875

[66] Scanzio, S., Vakili, M.G., Cena, G., Demartini, C.G., Montrucchio, B., Valenzano, A., Zunino, C.: Wireless sensor networks and tsch: A compromise between reliability, power consumption, and latency. IEEE Access **8**, 167042–167058 (2020) https://doi.org/10.1109/ACCESS.2020.3022434

[67] Tan, X.J., Wang, J., Yuan, Y.: Difference-set-based channel hopping for minimum-delay blind rendezvous in multi-radio cognitive radio networks. IEEE Transactions on Vehicular Technology **68**(5), 4918–4932 (2019) https://doi.org/10.1109/TVT.2019.2906455

[68] Javan, N.T., Sabaei, M., Hakami, V.: Adaptive channel hopping for ieee 802.15.4 tsch-based networks: A dynamic bernoulli bandit approach. IEEE Sensors Journal **21**(20), 23667–23681 (2021) https://doi.org/10.1109/JSEN.2021.3110720

[69] Aoudia, F.A., Hoydis, J.: Model-free training of end-to-end communication systems. IEEE Journal on Selected Areas in Communications **37**(11), 2503–2516 (2019) https://doi.org/10.1109/JSAC.2019.2933891

[70] Gupta, N., Granmo, O.-C., Agrawala, A.: Thompson sampling for dynamic multi-armed bandits. In: 2011 10th International Conference on Machine Learning and Applications and Workshops, vol. 1, pp. 484–489 (2011). IEEE

[71] Karoliny, J., Blazek, T., Ademaj, F., Springer, A., Bernhard, H.-P.: Time slotted multiple-hypothesis interference tracking in wireless networks. IEEE Internet of Things Journal **10**(2), 1028–1041 (2023) https://doi.org/10.1109/JIOT.2022.3204820

[72] Blackman, S.S.: Multiple hypothesis tracking for multiple target tracking. IEEE Aerospace and Electronic Systems Magazine **19**(1), 5–18 (2004)

[73] Scanzio, S., Vakili, M.G., Cena, G., Demartini, C.G., Montrucchio, B., Valenzano, A., Zunino, C.: Wireless sensor networks and tsch: A compromise between reliability, power consumption, and latency. IEEE Access **8**, 167042–167058 (2020) https://doi.org/10.1109/ACCESS.2020.3022434

[74] Vilajosana, X., Tuset, P., Watteyne, T., Pister, K.: Openmote: Open-source prototyping platform for the industrial iot. In: Ad Hoc Networks: 7th International Conference, AdHocHets 2015, San Remo, Italy, September 1-2, 2015. Proceedings 7, pp. 211–222 (2015). Springer

[75] Watteyne, T., Vilajosana, X., Kerkez, B., Chraim, F., Weekly, K., Wang, Q., Glaser, S., Pister, K.: Openwsn: a standards-based low-power wireless development environment. Transactions on Emerging Telecommunications Technologies **23**(5), 480–493 (2012)

[76] Sordi, M.A., K. Rayel, O., Moritz, G.L., Rebelatto, J.L.: Towards improving tsch energy efficiency: An analytical approach to a practical implementation. Sensors **20**(21) (2020) https://doi.org/10.3390/s20216047

[77] Liang, C.-J.M., Priyantha, N.B., Liu, J., Terzis, A.: Surviving wi-fi interference in low power zigbee networks. In: Proceedings of the 8th ACM Conference on Embedded Networked Sensor Systems. SenSys '10, pp. 309–322. Association for Computing Machinery, New York, NY, USA (2010). https://doi.org/10.1145/1869983.1870014 . https://doi.org/10.1145/1869983.1870014