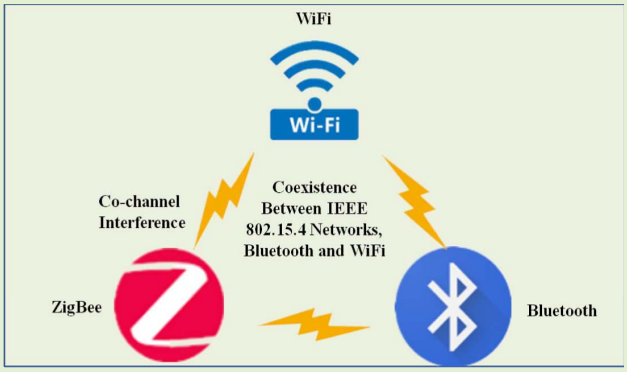
Coexistence and Interference Mitigation for WPANs and WLANs From Traditional Approaches to Deep Learning: A Review

Dong Chen, *Member, IEEE*, Yuan Zhuang, *Member, IEEE*, Jianzhu Huai, *Member, IEEE*, Xiao Sun, Xiansheng Yang, Muhammad Awais Javed, *Senior Member, IEEE*, Jason Brown, Zhengguo Sheng, *Senior Member, IEEE*, and John Thompson, *Fellow, IEEE*

***Abstract*—More and more devices, such as Bluetooth and IEEE 802.15.4 devices forming Wireless Personal Area Networks (WPANs) and IEEE 802.11 devices constituting Wireless Local Area Networks (WLANs), share the 2.4 GHz Industrial, Scientific and Medical (ISM) band in the realm of the Internet of Things (IoT) and Smart Cities. However, the coexistence of these devices could pose a real challenge—co-channel interference that would severely compromise network performances. Although the coexistence issues has been partially discussed elsewhere in some articles, there is no single review that fully summarises and compares recent research outcomes and challenges of IEEE 802.15.4 networks, Bluetooth and WLANs together. In this work, we revisit and provide a comprehensive review on the coexistence and interference mitigation for those three types of networks. We summarize the strengths and weaknesses of the current methodologies, analysis and simulation models in terms of numerous important metrics such as the packet reception ratio, latency, scalability and energy efficiency. We discover that although Bluetooth and IEEE 802.15.4 networks are both WPANs, they show quite different performances in the presence of WLANs. IEEE 802.15.4 networks are adversely impacted by WLANs, whereas WLANs are interfered by Bluetooth. When IEEE 802.15.4 networks and Bluetooth co-locate, they are unlikely to harm each other. Finally, we also discuss the future research trends and challenges especially Deep-Learning and Reinforcement-Learning-based approaches to detecting and mitigating the co-channel interference caused by WPANs and WLANs.**



***Index Terms*—Internet of Things, WPANs, WLANs, Bluetooth, IEEE 802.15.4, interference mitigation, deep learning, reinforcement learning, heterogeneous networks.**

I. Introduction

With the rapid development of communications technologies and huge demands in consumer electronics, devices such as home appliances and industrial sensors need to be accessible through wireless networks and provide enhanced services for the Internet of Things (IoT) [1]–[6], Smart Cities [7], [8] and Machine-Type Communications (MTC) [9]. Widely adopted networks enabling the proliferation of these devices are Wireless Personal Area Networks (WPANs) and Wireless Local Area Networks (WLANs). More precisely, WPANs can be formed by Bluetooth and IEEE 802.15.4 networks such as ZigBee or IPv6 over Low Power Wireless Personal Area Networks (6LoWPAN), whereas WLANs can be made up of IEEE 802.11 a/b/g/n/p/ac/ax networks depending on applications. WPANs normally support applications at short-range from 10 to 50 meters, whereas WLANs could support medium-range applications from 50 to 100 meters. Inevitably, on some occasions, WPANs and WLANs may need to coexist [10]. For example, in Smart Homes, devices such as laptops and smartphones are connected to WLANs, while some other devices such as wireless keyboards and headphones are connected to WPANs enabled by Bluetooth and the IEEE 802.15.4 Standard. Since WPANs and WLANs usually share the 2.4 GHz license-free band, this could give rise to

Manuscript received July 26, 2021; revised September 21, 2021; accepted September 28, 2021. Date of publication October 4, 2021; date of current version November 12, 2021. This work was supported by LIESMARS Special Research Funding from Wuhan University, China. The associate editor coordinating the review of this article and approving it for publication was Prof. Dongsoo Har. *(Corresponding author: Yuan Zhuang.)*

Dong Chen, Yuan Zhuang, Jianzhu Huai, Xiao Sun, and Xiansheng Yang are with the State Key Laboratory of Information Engineering in Surveying, Mapping and Remote Sensing, Wuhan University, Wuhan 430072, China (e-mail: yuan.zhuang@whu.edu.cn).

Muhammad Awais Javed is with the Department of Electrical and Computer Engineering, COMSATS University, Islamabad 45550, Pakistan.

Jason Brown is with the Department of Electronic and Computer Systems Engineering, the University of Southern Queensland, Springfield, QLD 4300, Australia.

Zhengguo Sheng is with the Department of Engineering and Design, University of Sussex, Brighton BN1 9RH, U.K.

John Thompson is with the Institute for Digital Communications, the University of Edinburgh, Edinburgh EH8 9YL, U.K.

Digital Object Identifier 10.1109/JSEN.2021.3117399

co-channel interference among those devices and compromise the network performance, thus leading to the low Quality of Service (QoS) for IoT applications.

As a result, extensive research has been conducted to investigate the coexistence issue from different perspectives with various metrics. Specifically, some studies were performed on real testbeds, aiming to find how co-channel interference might occur and how the network performance could be impacted from different distances, and a recommendation of a four-meter offset between ZigBee and WLAN devices can be made to engineers and researchers to alleviate interference when deploying WPANs and WLANs in a close range [11]–[13]. Moreover, some studies [14], [15] used simulation models such as Network Simulator-2 (NS-2) and Optimized Network Engineering Tools (OPNET) to mimic the adverse impacts caused by co-channel interference. The simulation results were compared with analytical results obtained from theoretical models, and both results showed a good agreement.

Besides the coexistence analysis, many studies have been proposed to mitigate co-channel interference. A busy tone [16] is created from an adjacent channel next to the current one that a WPAN occupies, to defer WLAN transmissions, while the WPANs continue to transmit packets. A more widely adopted approach is to firstly detect a free channel first and then shift to that channel to avoid interference [11]. In addition, some other studies used transmission parameters such as channel access time to alleviate co-channel interference. It was found that the average exponential back-off time of an IEEE 802.11 device to access the channel is longer than the transmission time of a Bluetooth packet, so Bluetooth can use the IEEE 802.11 back-off time to complete a packet transmission without WLAN interference [17].

A. The Existing Review Papers on Coexistence and Interference Mitigation Between WPANs and WLANs

To date, there already exist a number of articles reviewing the coexistence of IEEE 802.15.4 networks and WLANs. Specifically, Yang *et al.* [18] provided a detailed review on the coexistence between IEEE 802.15.4 and IEEE 802.11 networks with an emphasis on the severity of the coexistence, coexistence model analysis and co-channel interference mitigation. Metrics such as the Packet Error Rate (PER) and Signal-to-Interference plus Noise Ratio (SINR), and models such as interference channel models and path fading models are used to evaluate the coexistence scenarios. Saranya and Pugazendi [19] presented a review on the co-existence mechanisms of WPANs and WLANs devices. This review firstly introduces the IEEE 802.15.4 and IEEE 802.11 Standards, then discusses a few scenarios in which ZigBee and WLAN devices mutually interfere with each other, and finally presents three interference mitigation methods in terms of distributed adaptation, media access control and scheduling. Hayajneh *et al.* [20] reviewed the coexistence and interference mitigation for Wireless Body Area Networks (WBAN). This work comprehensively discusses the coexistence issues among IEEE 802.15.6, IEEE 802.15.4 networks and low-power WLANs. The adverse effects of WLANs on IEEE 802.15.6 and IEEE 802.15.4 networks are briefly discussed. The authors also provide a mathematical analysis and simulation results on the coexistence paradigms including IEEE 802.15.6, low-power WLANs and WLANs.

Movassaghi *et al.* [21] also reviewed on WBANs. This review mainly discusses IEEE 802.15.6 and IEEE 802.15.4j networks and concludes that the distance between IEEE 802.15.6 networks and WLANs should be up to three meters while 10 WBANs coexist in the same scenario to avoid interference, which is recommended by the IEEE 802.15.6 task group. Ferro and Potorti [22] reviewed the Bluetooth and WLAN standards in terms of network topology, capacity, power consumption and QoS support, among which medium access control, data link types and topology are well defined by the standards, whereas power consumption, QoS and security are still open issues. In particular, the coexistence between Bluetooth and WLANs is briefly discussed regarding to two interference mitigation schemes: the Adaptive Frequency Hopping (AFH) scheme [23], [24] and transmit power control. Latré *et al.* [25] analyzed IEEE 802.15.4-based WBANs and suggested that low transmission power be used for each node to alleviate co-channel interference. Naik *et al.* [26] discussed coexistence issues for different technologies under the unlicensed 5 GHz band such as Long Term Evolution (LTE) and WLANs, Radar and WLANs, Dedicated Short-Range Communication (DSRC) and WLANs because the 2.4 GHz band has become significantly saturated.

Although the above articles have reviewed on the coexistence scenarios for IEEE 802.15.4 networks and WLANs, and for Bluetooth and WLANs, separately, there is no up-to-date review paper discussing and summarizing coexistence issues between WPANs (IEEE 802.15.4 networks and Bluetooth) and WLANs in one single article. To make our review comprehensible to the reader who has no prior expertise in the coexistence of WPANs and WLANs, we provide a tutorial on the basic concepts and describe each corresponding issue in detail. The goal of this review is to provide interested readers who wish to design new networks using the IEEE 802.15.4, Bluetooth and WLAN standards with a comprehensive understanding of various aspects of the severity and solutions of the coexistence between WPANs and WLANs, so the readers can use this paper as a primer for more in-depth research. In particular, IEEE 802.11 networks, Wi-Fi and WLANs are used interchangeably throughout the paper. The co-channel interference only refers to the interference caused by heterogeneous devices. The reason why we focus on co-channel interference in 2.4 GHz rather than 5 GHz is because WLANs could work on either the 2.4 GHz or 5 GHz band, but the majority of IEEE 802.15.4 networks and Bluetooth piconets in smart homes or apartments still work on the 2.4 GHz band. On the 5 GHz band, WLANs could co-locate with many other wireless networks such as LTE, Radar and DSRC as described in [26].

TABLE I
ACRONYMS USED THROUGHOUT THE PAPER

AFH	Adaptive Frequency Hopping	ISOMDMS	Interference Source Oriented Master Delay Scheduling
AP	Access Point	6LoWPAN	IPv6 over Low Power Personal Area Networks
ARQN	ARQ Number	LIFS	Long Inter-frame Spacing
ARQ	Automatic Repeat Request	LQI	Link Quality Indicator
ACL	Asynchronous Connection Link	LTE	Long Term Evolution
AWGN	Additive White Gaussian Noise	LBS	Location-Based Services
BE	Back-off Exponent	MSDU	MAC Service Data Unit
BO	Beacon Order	MMSE	Minimum Mean Squared Error
BPSK	Binary Phase-Shift Keying	MTC	Machine-Type Device
BIAS	Backoff Interference Awareness Scheduling	MC	Markov Chains
BI	Beacon Interval	NB	Number of Back-offs
BER	Bit Error Rate	NAV	Network Allocation Vector
CCA	Channel Clearance Assessment	NBP	Narrow Band Protection
CFP	Contention Free Period	NLS	Non-linear Least Square
CAP	Contention Access	NS-2/3	Network Simulator-Version 2/3
CW	Contention Window	NFC	Near Field Communications
CBT	Cooperative Busy Tone	O-QPSK	Offset Quadrature Phase-Shift Keying
CDF	Cumulative Distribution Functions	OPNET	Optimised Network Engineering Tools
DIFS	DCF Interframe Space	PCF	Point Coordination Function
DSSS	Direct Sequence Spread Spectrum	RSS	Receive Signal Strength
DCF	Distributed Coordination Function	RSSI	Receive Signal Strength Indicator
DNN	Deep Neural Networks	SAP	Service Access Point
FEC	Forward Error Correction	SHR	Synchronization Header
FH	Frequency Hopping	SO	Superframe Order
GTS	Guaranteed Time Slot	SIFS	Short Interframe Space
GFSK	Gaussian Frequency shift keying	SU	Secondary Users
IFS	Inter-Frame Spacing	SCO	Synchronous Connection-Oriented
ISM	Industrial, Scientific and Medical	SEQN	Sequence Number
IAACCA	Interference-Aware Adaptive Clear Channel Assessment	SDR	Software-Defined Radio
IoT	Internet of Things	SINR	Signal-to-Interference plus Noise Radio
IAACCA	Interference-Aware Adaptive Clear Channel Assessment	SOA	Service Oriented Architecture
IAFH	Interference-Aware Frequency Hopping	WPAN	Wireless Personal Area Networks
ISDR	Interference Signal Detection Rate	WLAN	Wireless Local Area Networks
ISOAFH	Interference Source Oriented Adaptive Frequency Hopping	WBAN	Wireless Body Area Networks

B. Key Contributions

This paper not only reviews the coexistence scenarios between IEEE 802.15.4 networks and WLANs, but also reviews the coexistence between Bluetooth and WLANs. In addition, the paper also reviews the coexistence scenarios where IEEE 802.15.4, Bluetooth and WLANs co-locate and mutually interfere with each other. The paper also provides thorough discussions on the causes and solutions of co-channel interference. For clarity, we summarize the terminologies and acronyms used in this work in Table I and list the main contributions as follows:

1) This work describes the hierarchy of the IoT system and highlight some potential applications and scenarios where WPANs and WLANs might co-locate and cause co-channel interference due to the proliferation of IoT devices. This work then presents a number of coexistence models either implemented in simulations or analytically derived under saturated WLAN traffic. In particular, the work highlights a few heterogeneous networks comprised of IEEE 802.15.4 networks and WLANs or comprised of Bluetooth and WLANs. These hybrid networks can cause severe co-channel interference in the IoT setting, but they did not attract much attention of researchers.
2) This work discusses different interference mitigation solutions in detail. The advantages and drawbacks of these solutions are classified, compared and summarized using key metrics such as throughput, the packet reception ratio and end-to-end delay, etc., to provide in-depth insights into the future deployment of IoT devices.
3) This work comprehensively reviews the coexistence scenarios for IEEE 802.15.4 networks, Bluetooth and WLANs. We reveal that IEEE 802.15.4 networks can be adversely impacted by WLANs, while WLANs can be negatively affected by Bluetooth. In contrast, when IEEE 802.15.4 networks and Bluetooth co-locate, they tend to not cause much interference to each other.
4) This work explores future research trends, highlight some challenges for WPANs and WLANs coexistence and provide possible generic solutions that might be effective in mitigating co-channel interference. In particular, this work introduces Deep-Learning and Reinforcement-learning-based approaches to dealing with co-channel interference, which show superior performances over the traditional methods.

C. Structure of the Paper

The paper is further organized as follows:

- Section II: We describe the fundamental fabrics of the IoT and present three possible IoT scenarios and applications in which WPANs and WLANs could co-locate and may generate co-channel interference.
- Section III: We present an overview of the IEEE 802.15.4 and IEEE 802.11 Standards to provide a better

understanding for generalists and to pave the way for the discussions later. We discuss the coexistence issues between IEEE 802.15.4 networks and WLANs, and summarize the metrics for simulation and analytical models used to evaluate the coexistence scenarios.

- Section IV: We present an overview of IEEE 802.15.4 networks and WLANs, and discuss the coexistence issues and solutions including the metrics, testbeds, simulation and analytical models, as well as a taxonomy of interference mitigation solutions. The two standards are also analyzed and compared in terms of several key metrics such as transmit power, bandwidth and the packet size, etc. In particular, we also discuss the coexistence issues in the hybrid network comprised of an IEEE 802.15.4 network and a WLAN.
- Section V: We present an overview of the Bluetooth standard including the modulation schemes, packet formats, frequency hopping technology and types of communication links. We also discuss the coexistence issues and solutions between Bluetooth and WLANs, including the metrics, testbeds and simulation models, as well as a taxonomy of interference mitigation solutions. In particular, we also discuss the coexistence issues and the interference mitigation solutions in the hybrid network comprised of a Bluetooth network and a WLAN.
- Section VI: We provide discussions on the reasons why IEEE 802.15.4 networks are subject to WLANs, whereas WLANs are susceptible to Bluetooth. Additionally, we also elaborate on the reasons why IEEE 802.15.4 networks are not adversely impacted by Bluetooth when co-locating.
- Section VII: We highlight some open issues and challenges when WPANs and WLANs co-locate in a close range and provide useful insights for researchers on how to mitigate co-channel interference for WPANs and WLANs in IoT settings, especially the Deep-Learning-based approach to detecting congested channels.
- Section VIII: We conclude this review.

II. WPANs and WLANs Coexistence Scenarios in the IoT

To better help the reader get a comprehensive understanding of how to apply the aforementioned interference mitigation solutions to different applications, the IoT system and several typical coexistence scenarios are introduced.

A. The IoT Definition and Trends

Kevin Ashton coined the term "Internet of Things" and envisioned that pervasive sensors and actuators would connect the physical world using the Internet to improve the quality of human lives [5]. In this process, wired and wireless communications play an important role in using technologies such as pervasive computing and wireless sensor networks. According to [27], the IoT can be divided into three layers. The first layer is responsible for collecting data and includes millions of devices such as sensors, smart meters, Global Positioning System (GPS) terminals, actuators and cameras and so on. The second layer serves as the main Internet connection, relaying and integrating the data. The third layer is cloud computing that processes the collected data from the lower layer, analyzes the data and performs operations. It is expected that billions of IoT devices would be deployed around the globe by 2030 and promote a huge market worth of 2.7 to 6.2 trillion U.S dollars [28] in related industries, especially for health, automation, monitoring, transportation and so on.

B. The Components of the IoT

The three layers in the IoT [29] is shown in Fig. 1. The first is the data collection layer that collects data generated by machines, actuators, sensors, GPS terminals and cameras. The supporting technologies are Sigfox, Long-Range Radio (LoRa), Weightless, Narrow Band-IoT, ZigBee, Bluetooth, 6LoWPAN, Ultra-Wide Band (UWB), and Near-Field Communication (NFC), etc. The second is the data transmission layer focusing on delivering and relaying the data to services and applications that require gateways supporting heterogeneous technologies such as routing and protocol translation. The third is the data processing and analyzing layer processing the collected data and analyzing the data pattern using machine learning techniques to optimize applications and services or to make informed decisions for the system.

1) The Data Collecting Layer: In this layer, many devices such as machines, sensors and actuators continuously or intermittently sense the ambient environment and collect the data. In this process, many important network technologies are involved. Radio Frequency Identification (RFID) with a tag and a reader identify objects with a Ubiquitous Code (uCode) or an Electronic Product Code (EPC) using the tag. RFID reads the tag and sends information to the Internet using the reader [30] with different frequency bands, which is widely used to track inventories in the warehouse. Another similar technique is NFC that enables low-rate personal data transmissions such as video, photos and files between two electronic devices in a close range fewer than 10 cm [31]. Therefore, NFC can be used by application software in smartphones to facilitate payments. A third typical technique is Wireless Sensor Networks (WSNs) that can be applied to many domains such as health care, agriculture, manufacturing and oil industry [32]. The majority of WSN devices are placed in environments often inaccessible for humans such as oceans and mountains for monitoring and operate at the 2.4 GHz license-free band and exchange data in low transmission rates. IEEE 802.15.1 networks, also known as Bluetooth, also share the 2.4 GHz license-free band and could be suitable for deploying the IoT in the data collecting layer. Bluetooth serves as cable replacement for short-range communications between low-power devices such as wireless keyboards, mouses and headsets and can form a star network with one master node and up to seven slave nodes [33]. The master node synchronizes and controls the data transmissions of the slave nodes using the frequency hopping technique to avoid packet collisions in the same 2.4 GHz license-free band. LoRa and SigFox [34] are emerging wireless technologies

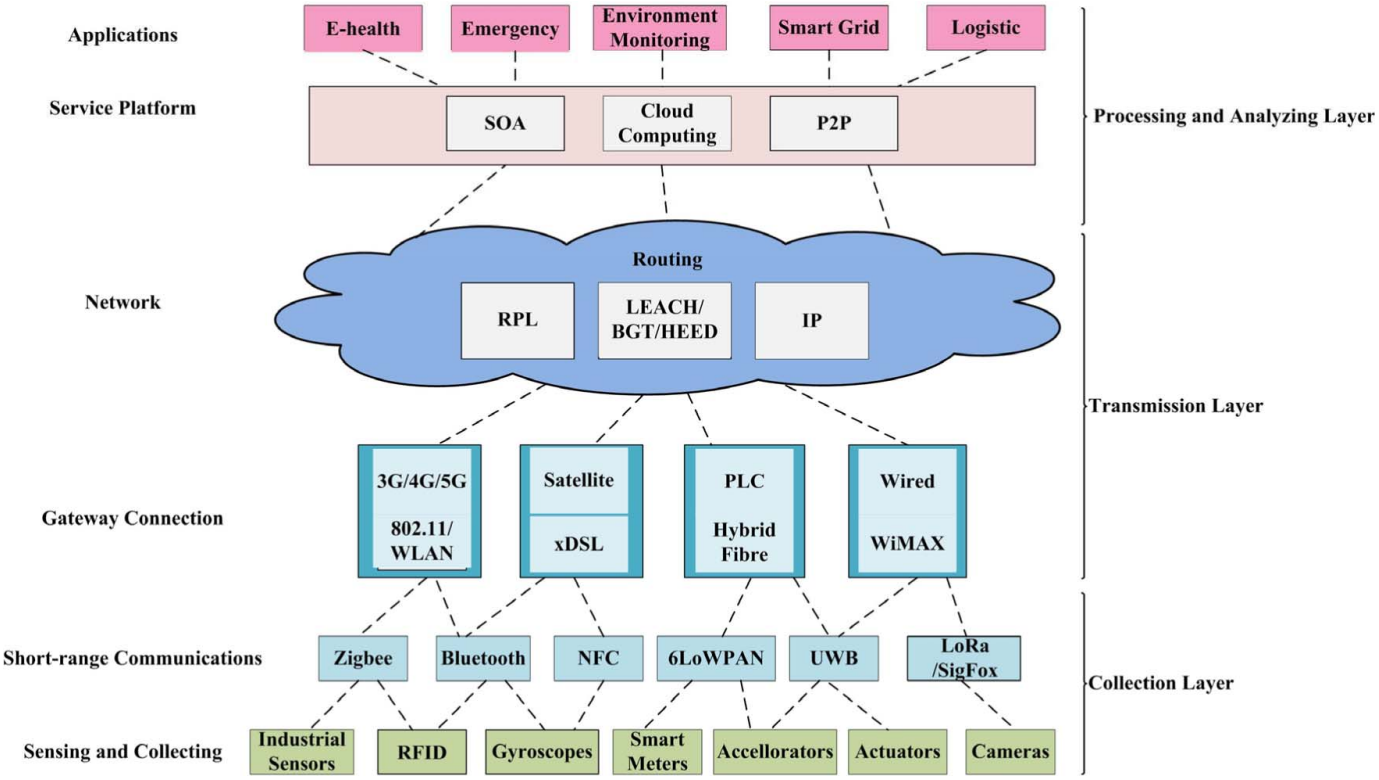


Fig. 1. The three key layers of the IoT.

designed for IoT communications. Sigfox and LoRa are both designed for Low Power Wide Area Networks to support low energy consumption, long-range communications, GPS-free positioning and built-in security.

2) The Data Transmission Layer: In this layer, the gathered data is routed and relayed using different heterogeneous wireless technologies. The most widely deployed network is IEEE 802.3 Ethernet with a high transmission rate up to 100 Gbps [35] and inter-connect all types of applications and services. Another is Power Line Communications (PLC) for Smart Grids. PLC uses a series of the existing power distribution system and includes four types of networks: in-house networking, Broadband over Power line, narrowband outdoor and outdoor communications [36]. However, wired networks might have some intrinsic drawbacks such as adding new devices or reorganizing the network topology, a trending solution is to adopt wireless networks that have better flexibility due to their "plug-and-play" features. One example for indoor environments is WLANs that can form an infrastructure network, in which an access point controls the other nodes, or can form an Ad-hoc network, in which each WLAN station operates independently without a central controller. For even a broader range, cellular networks play an important role due to their design for audio and video transmissions. LTE and 5G networks are designed for broadband communication that provides connectivity for mobile devices and terminals. Many other communications technologies are also suitable for IoT data transmissions such as cognitive networks and opportunistic networks [37], [38]. With these wireless networks emerging, temporarily free spectrum can be fully utilized to increase the efficiency of wireless transmissions.

3) The Data Processing and Analyzing Layer: In this layer, the main objective is to use artificial intelligence to assist humans to learn the useful patterns of the data and make informed decisions for applications and services. All the information is transparent to the lower layers, so the data analysis and processing become easy. Data abstraction is a key factor for applications and services via a Service Oriented Architecture (SOA) [39]. It allows communications protocols to provide services from the application layer to the lower layers via the Internet, which has the potential to be widely used in the IoT scenario. Moreover, the core technology for the data processing and analyzing layer is Cloud Computing that serves as the key platform of the IoT. The cloud has a huge capacity to analyze a massive amount of the data collected from the data transmission layer [40].

C. Coexistence Scenarios of WPANs and WLANs in the IoT

The aforementioned three layers consist of the main functions of the IoT and need the cooperation of the connected devices to operate in a reliable and safe manner. Therefore, the IoT is expected to connect heterogeneous networks including such as ZigBee, 6LoWPAN, Bluetooth, WLANs, cellular, Sigfox and LoRa [41], [42]. This section details three scenarios that may share the unlicensed bands and cause co-channel interference, as shown in Fig. 2.

- Location-Based Services (LBS): One of IoT applications that may experience co-channel interference is indoor

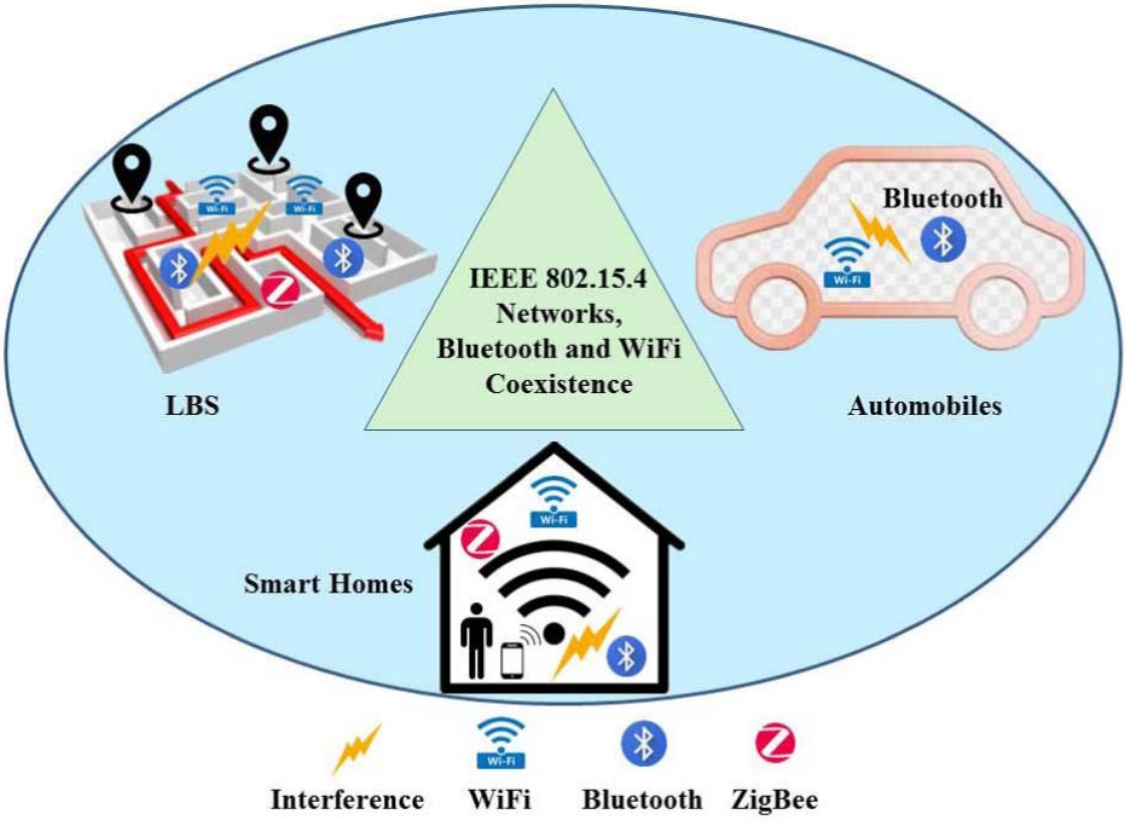


Fig. 2. The three coexistence scenarios with co-channel interference.

positioning [43]. This is because some indoor positioning systems use Bluetooth and WiFi to collect Received Signal Strength (RSS) data and perform positioning at a back-end server. More precisely, when the user walks indoors, the Bluetooth-enabled smartphone or tablet connects to the pre-deployed WLAN/Bluetooth gateways. The gateways then forward the data to a WiFi AP that is connected to a back-end server running the positioning algorithm. Once accurate indoor position of a user is calculated, the location information will be sent to the user and displayed on smartphones or tablets, so the user knows their location. However, the Bluetooth data may interfere with the WLAN data or other conventional wireless networks sharing the same frequency bands. This is especially true in the factory or hospital environments where indoor positioning data traffic may disrupt and interfere with the factory or medical equipment. On one hand, a large of number of short and frequent positioning data transmissions may hamper the normal ongoing data transmission e.g., multimedia traffic. On the other hand, the existing networks or equipment sharing the unlicensed band such as WiFi or microwave ovens may cause co-channel interference or incorrect RSS.

- Smart Homes: In addition to LBS, many devices in a Smart Home such as smartphones and pads are often integrated with many wireless RF radio interfaces such as LTE, WiFi, Bluetooth and 5G. LTE and 5G are mainly used for subscriber services such as voice calls, text messages and multimedia services outdoors, whereas WiFi and Bluetooth are also responsible for the same types of services when people are indoors. These devices in a Smart Home are connected to WLAN/Bluetooth gateways. For example, if many people in a room are using headphones connected to their smartphones using Bluetooth for audio services, which are served by the WiFi AP, the Bluetooth and WiFi traffic would cause co-channel interference. This case could become even worse when people are using Bluetooth-based electronic devices such as wireless mice and keyboards with their laptops equipped with WiFi and Bluetooth interfaces.
- Automobiles: Driven by high customer demands that passengers are more likely to spend time working and entertaining in cars, car manufacturers have put huge efforts to develop infotainment systems to meet the rising needs. The most recent cars are equipped with large LCD screens and a variety of wireless services. This has attracted IT giants such as Google and Apple that have developed special car platforms such as Carplay and Android Auto [44]. These platforms often need short-range wireless network standards such as Bluetooth, WLANs and Kleer [45]. Bluetooth is usually for music streaming, hands-free calling and contact information exchange, while WLANs are used for applications such as screen mirroring using WiFi Direct [46] and Kleer is

designed for streaming high-quality music. Since Bluetooth and WLANs share the 2.4 GHz frequency band, the coexistence problem arises, prompting scholars to find solutions to improve the coexistence in an automobile environment.

III. IEEE 802.15.4 WPAN AND WLAN OVERVIEW

In this section, the IEEE 802.15.4 and 802.11 Standards are briefly described and compared, and the applications based on these networking standards together with their QoS requirements are also presented. The simulation models and their metrics are presented with their network performances.

A. IEEE 802.15.4 Overview

The IEEE 802.15.4 Standard [47] was designed to support low power and low data rate devices that can run for months and years. These devices include sensors and positioning beacons that adopt the license-free 2.4 GHz band shared by microwave ovens, laptops and smartphones. The standard specifies the Physical and Data link layers of the network design with the data rate ranging from 20 kbps to 250 Kbps. The standard has 2003 and 2006 versions, both of which also support 915 MHz and 868 MHz bands in addition to the 2.4 GHz band. The modulation schemes include Binary Phase-Shift Keying (BPSK), Offset Quadrature Phase-Shift Keying (O-QPSK) and the Parallel Sequence Spread Spectrum (PSSS). However, the standard does not include any error correction schemes in the Physical Layer, so restoring corrupted packets is relatively difficult. IEEE 802.15.4 networks normally need to perform Channel Clearance Assessment (CCA) before sending a packet.

Above the Physical Layer, the MAC layer plays an important role in connecting the Physical and higher layers using a Service Access Point (SAP). The SAP has a unit named the MAC Service Data Unit (MSDU) that includes frame control, addressing fields, the auxiliary security header, the sequence number and the data payload. As a packet is forwarded to the Physical Layer from the MAC layer, the MSDU then becomes a Physical Service Unit (PSU) with a Physical Header (PHR) and a Synchronization Header (SHR). The PSU supports a maximum payload size up to 121 bytes.

The MAC layer has two transmission modes: the beacon-disabled un-slotted mode and the beacon-enabled slotted mode. The un-slotted model means that the node directly senses the channel and transmits packets using the CSMA/CA mechanism, which would cost a lot of energy. To save the energy and increase the lifetime of IoT devices, the slotted mode is more widely adopted. In the slotted mode, the period between two control packets emitted by the central node is named as a "superframe", as shown in Fig. 3. The superframe is divided into two parts: the inactive period and the active period. The active period has two periods: the Contention Access Period (CAP) and Contention Free Period (CFP). In the CAP, the device goes to sleep and preserves energy. In the active period, devices contend the channel using the CSMA/CA mechanism. In the CFP, a dedicated channel called

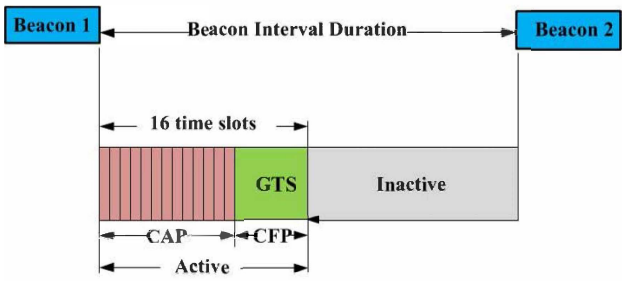


Fig. 3. Superframe Structure [48].

the Guaranteed Time Slot (GTS) is assigned to ensure the guaranteed channel access for real-time traffic. In addition, two key parameters could affect the superframe structure. The first is the Beacon Order (BO) adjusting the duration between two consecutive beacons, and this duration is also named the Beacon Interval (BI); the second is the Superframe Order (SO) adjusting the duration of the CAP. These parameters are defined as follows.

$$BI = T_S F \times 2^{BO}, \tag{1}$$

$$SD = T_S F \times 2^{SO}, \tag{2}$$

where $0 \leq SO \leq BO < 15$ and $T_S F$ is the basic duration, which equals to 60 symbols.

The standard indicates that the inactive period is disabled when $BO = SO$, meaning that the superframe only consists of the active period. If $BO = 15$, the superframe is not available, and the network operates in the un-slotted mode. The minimum superframe duration equals to 60 symbols (0.96 ms). The start and end of a superframe is controlled by the beacon that contains addresses and time slots to be allocated to the GTS. Moreover, an ACK packet is sent back after an Inter-Frame Spacing (IFS) to ensure a reliable connection in the MAC layer after each successful transmission. If the packet transmission fails, the packet is deferred to the next superframe.

The CSMA/CA algorithm has several key parameters that could impact on the system performance. The Back-off Exponent (BE) calculates the number of slots that a device needs to back off due to packet collisions or transmission failure. The value of the BE is chosen between macMinBE and macMaxBE (three and five by default, respectively). The Number of Back-offs (NB) counts the number of times a device backs off and is set to five by default. Before sending a packet, the device needs to perform a Clear Channel Assessment (CCA) twice to ensure that the channel is free. When performing the CCA, the device adopts a Contention Window (CW) set to two by default. Every time when the channel is assessed to be busy, the CW is decreased by one. The packet is then allowed to be sent on the channel until the CW is decreased to zero. If any CCA fails, the packet is held back, and the CW is reset to two. After each packet transmission fails, the number of retransmissions is recorded at each device and is set to three by default.

The CSMA/CA algorithm is described in Fig. 4. As a packet is ready for transmission, the NB, CW and BE values are

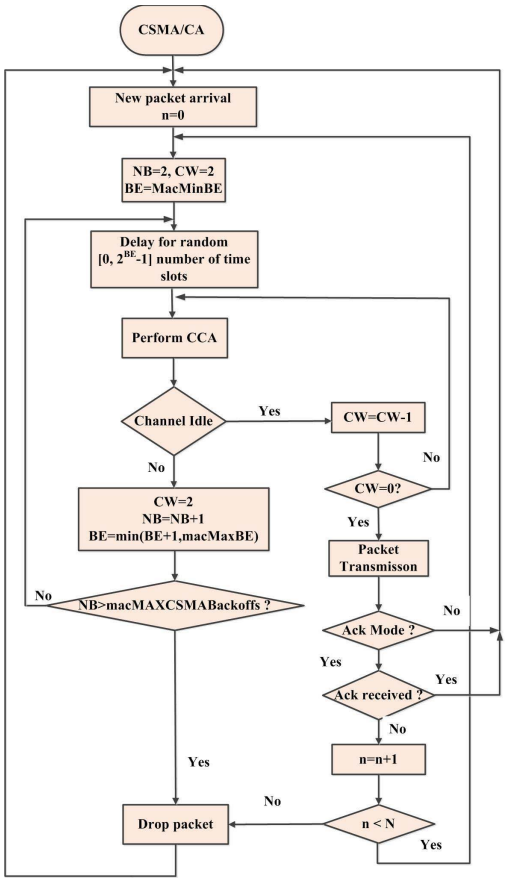


Fig. 4. The CSMA/CA Algorithm in the IEEE 802.15.4 Standard [47].

set to zero, two and three, respectively. When the packet collides, the device firstly chooses time slots uniformly distributed between [0, $2^{BE} - 1$] and then backs off. Afterwards, the device senses the channel and performs the first CCA. If the channel is idle, the device proceeds to the second CCA and senses the channel again. Once the channel is idle, the packet is sent immediately. According to the IEEE 802.15.4 Standard, the Acknowledgement (ACK) for a transmitted packet is optional, so the algorithm can operate either in an ACK-enabled or an ACK-disabled mode. In the ACK mode, the receiver replies with an ACK packet if a packet is successfully transmitted, as shown in Fig. 5; the receiver cannot receive the packet if a collision occurs, thus resulting in no ACK reply. In particular, after the packet is transmitted, the sender enables a timer. When the timer runs out and the ACK packet has not yet been received, the sender assumes the packet is lost during the packet collision and then retransmits the packet three times. If the number of retransmission is greater than a pre-defined threshold aMaxFrameRetries (Three by default), the packet is deemed as a loss. All the parameters CW, NB and BE are restored to two, zero and three.

B. IEEE 802.11g Overview

Since the IEEE 802.11 Standard has many variants 802.11 a/b/g/n/ac/ax, we choose the IEEE 802.11g Standard as a typical example to describe key characteristics of WLANs. The IEEE 802.11g Standard specifies the Physical and MAC layers. Similar to IEEE 802.15.4 networks, WLANs also operate on the 2.4 GHz license-free band. 13 WLAN channels cover the 2.4 GHz band and each sub-band is 22 MHz wide. Fig. 6 presents the WLAN CSMA/CA algorithm that uses two ways to sense the channel: physical carrier sensing and virtual carrier sensing. The physical carrier sensing senses the carrier signal energy on the transmission channel to determine whether the channel is idle. In contrast, the virtual carrier sensing adopts the Network Allocation Vector (NAV) in the MAC layer. The NAV notifies the other WLAN stations of the packet air time. With the NAV, the other WLAN stations will know the packet duration and suspend its packet transmissions to avoid packet collisions. Both approaches are used to sense the channel status. If the channel is busy, the station backs off and senses the channel; if the channel is idle, the station performs a Distributed Coordination Function (DCF) mechanism and prepares to send the packet. Otherwise, it continues to backs off until the channel is idle.

Figure 7 presents the IEEE 802.11 DCF mechanism. The basic principle is to listen before talk. In other words, a station senses the channel before transmitting to avoid packet collisions. When the channel is sensed to be busy, the station backs off and then senses the channel again; the procedure is repeated until the channel is found to be idle. More precisely, a WLAN station with a packet to send needs to wait for a short duration of DCF Interframe Space (DIFS).

After the waiting period, the WLAN station goes into two states. In the first state, the WLAN station has a pending packet to transmit and finds the channel to be idle. After the DIFS waiting period, the WLAN station starts to send the packet and waits for a Short Interframe Space (SIFS). In the second state, when the WLAN station finds the channel to be busy after the DIFS period, it backs off using a random number of time slots chosen from the Contention Window (CW). The time slots for the back-off is uniformly selected from an interval between [0, CW], in which the CW can be set between two values: a minimum CW CWmin and a maximum CW CWmax. After the first channel sensing, if the channel is still busy, the WLAN station continues to back off until the channel is idle, and then the WLAN station completes a successful transmission after the DIFS period. The CW is initially set to CWmin and doubled every time after a transmission failure either due to packet collisions or an absent ACK, so the WLAN station collide with other WLAN stations in a lower chance. The CW will be reset to the CWmin after either the expiration of the retry limit or a successful transmission.

Figure 8 depicts how the CW is increased using the binary exponential back-off algorithm. Firstly, the CW is set 15 for the CWmin. After a transmission failure, a re-try counter is increased by one, and a collided packet is dropped as the re-try counter reaches its upper limit. As shown in Fig. 8, the CW is increased six times due to packet collisions. The CW increases in an exponential manner using (3), in which the $randomslot_{time}$ slot is the time slots in the CW and BE is the Back-off Exponent.

$$randomslot_{time} = 2^{BE} - 1 \tag{3}$$

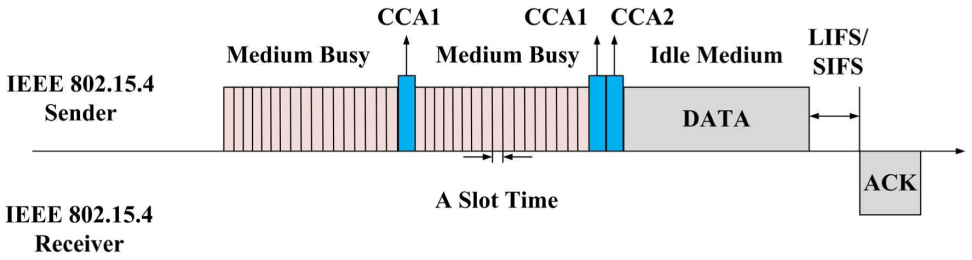


Fig. 5. The IEEE 802.15.4 MAC operation.

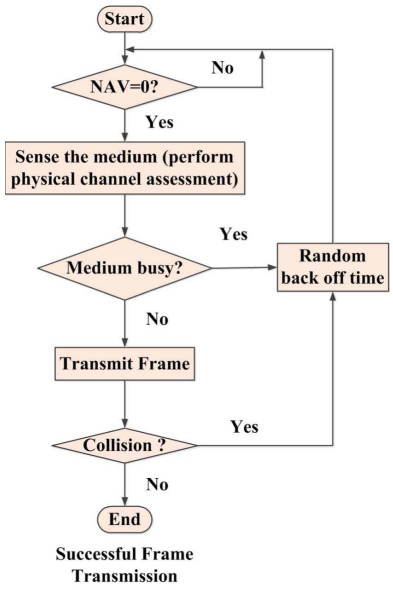


Fig. 6. The IEEE 802.11 CSMA/CA algorithm [49].

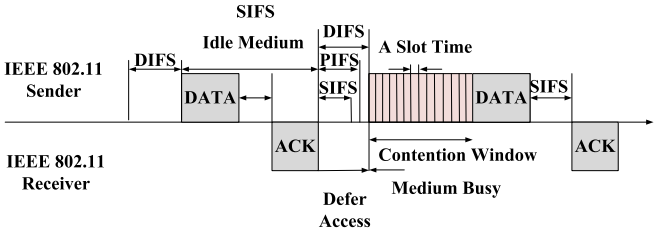


Fig. 7. IEEE 802.11 Distributed Coordination Function.

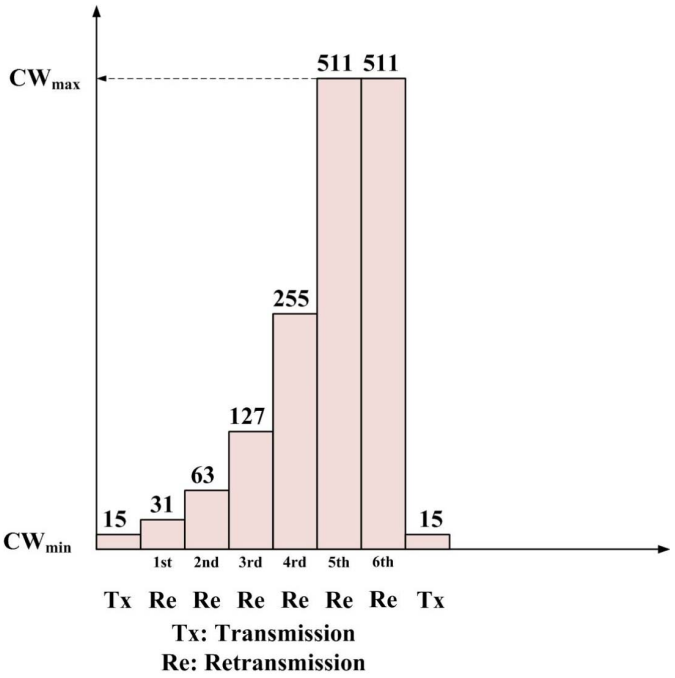


Fig. 8. The binary exponential back-off algorithm [49].

C. Similarities and Differences Between IEEE 802.15.4 Networks and WLANs

1) Frequency Arrangement of IEEE 802.15.4 and IEEE 802.11 Standards: The IEEE 802.15.4 Standard support several frequency bands including the 868 MHz, 928 MHz and 2.4 GHz ISM bands, and the IEEE 802.11 Standard supports two frequency bands 2.4 GHz and 5 GHz. This paper focuses on the 2.4 GHz band, which is the most widely used band. Fig. 9 shows the sub-channel arrangement specified by the IEEE 802.11 and IEEE 802.15.4 Standards within the 2.4 GHz frequency band. The IEEE 802.11g Standard uses a 22 MHz band, whereas the IEEE 802.15.4 Standard employs a narrow 2 MHz band. This figure shows that IEEE 802.11 channel 1, 6 and 11 severely interfere with the IEEE 802.15.4 channels, and each IEEE 802.11 channel interferes with four IEEE 802.15.4 channels. IEEE 802.11 devices transmit data packets at a higher power level than 802.15.4 devices. Therefore, if IEEE 802.11 and IEEE 802.15.4 devices coexist in a relatively confined environment, this would cause co-channel interference and affect the network performance.

2) The Differences Between the IEEE 802.15.4 and IEEE 802.11 MAC Layers: Although IEEE 802.15.4 and IEEE 802.11 Standards both use the CSMA/CA algorithm to access the channel, there is a slight difference between the two algorithms. The major differences lie within: (1) the IEEE 802.11 back-off counter is only related to the random time slots, whereas the IEEE 802.15.4 backs off, channel access and the CCA are required to begin at the boundary of each time slot; (2) an IEEE 802.11 station senses the channel when the random back-off time slots run out, while an IEEE 802.15.4 station senses the channel when the random back-off time slots run out and the CW is decreased to zero; and (3) the IEEE 802.11 CW denotes the number of random back-off slots [50], while the IEEE 802.15.4 CW refers to an integer number that is reduced from one to zero each time when the channel is sensed idle and the random time slots

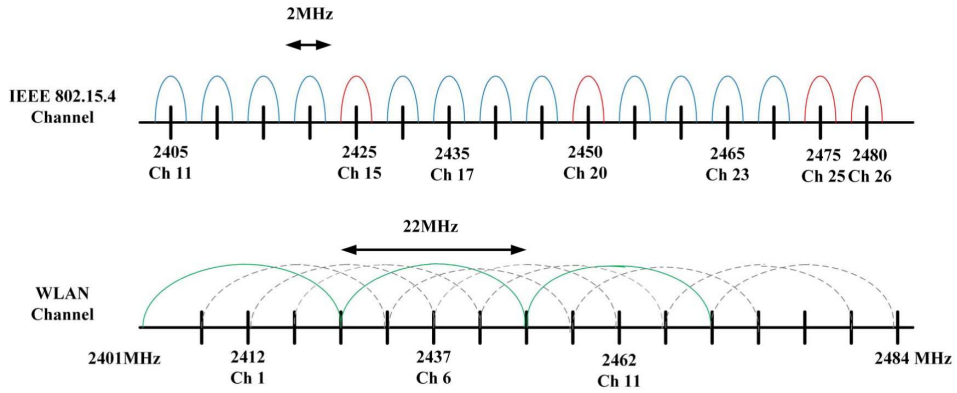


Fig. 9. Sub-channels of the IEEE 802.15.4 and IEEE 802.11 Standards in the 2.4 GHz band [49].

TABLE II
DIFFERENCES BETWEEN IEEE 802.15.4 AND IEEE 802.11 g WLANS [51]

Parameters	IEEE 802.15.4 Networks	IEEE 802.11g WLAN
Transmit Power	-32dBm to 0 dBm	0 to 20 dBm
Receiver Sensitivity	-98 dBm	-95 dBm
CCA threshold	-85 dBm	-84 dBm
Bandwidth	2 MHz	22 MHz
Back-off unit	320 μs	9 μs
SIFS	192 μs	10 μs
DIFS	N/A	28 μs
CCA	128 μs	N/A
CWmin	2	15
CWmax	N/A	1023
Center Frequency of the First Channel	2410 MHz	2412 MHz
Payload Size	80 bytes	1500 bytes
ACK packet	5 bytes	14 bytes
Max Date rate	250 Kbps	54 Mbps
Coverage Range	10-50 meters	100-150 meters
Max No. of Retransmissions	3	7

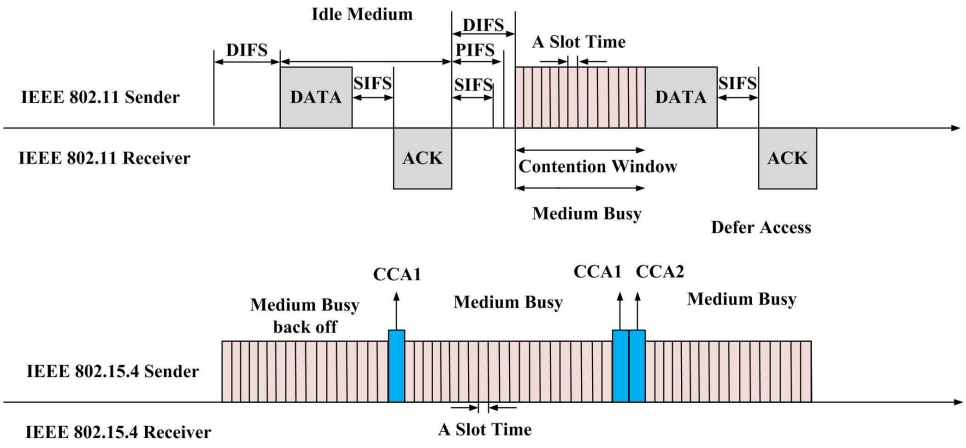


Fig. 10. IEEE 802.11g networks seize the channel faster than IEEE 802.15.4 networks.

elapse. The other differences are summarized in the Table II. Specifically, it can be seen that IEEE 802.11g has much shorter backoff time slots and inter-frame periods compared to IEEE 802.15.4 networks, so IEEE 802.11g networks can seize the channel much faster and more frequently than IEEE 802.15.4 networks. Fig. 10 illustrates a scenario in which the IEEE 802.15.4 networks are interfered with by the IEEE 802.11 networks. Assume that the IEEE 802.15.4 networks just finish backing off and start to sense the channel, while IEEE 802.11 networks also finish sensing the channel that is found to be idle. Since the DIFS is shorter than the back-off slots of the IEEE 802.15.4 networks, the IEEE 802.11 networks can seize the medium and begin transmitting a data packet. As the IEEE 802.15.4 networks complete the second back-off, the medium is still busy due to the IEEE 802.11 ACK packet transmission, so the IEEE 802.15.4 performs the first CCA and resumes to back off. The third time when the IEEE 802.15.4 networks finish backing off, the sender performs

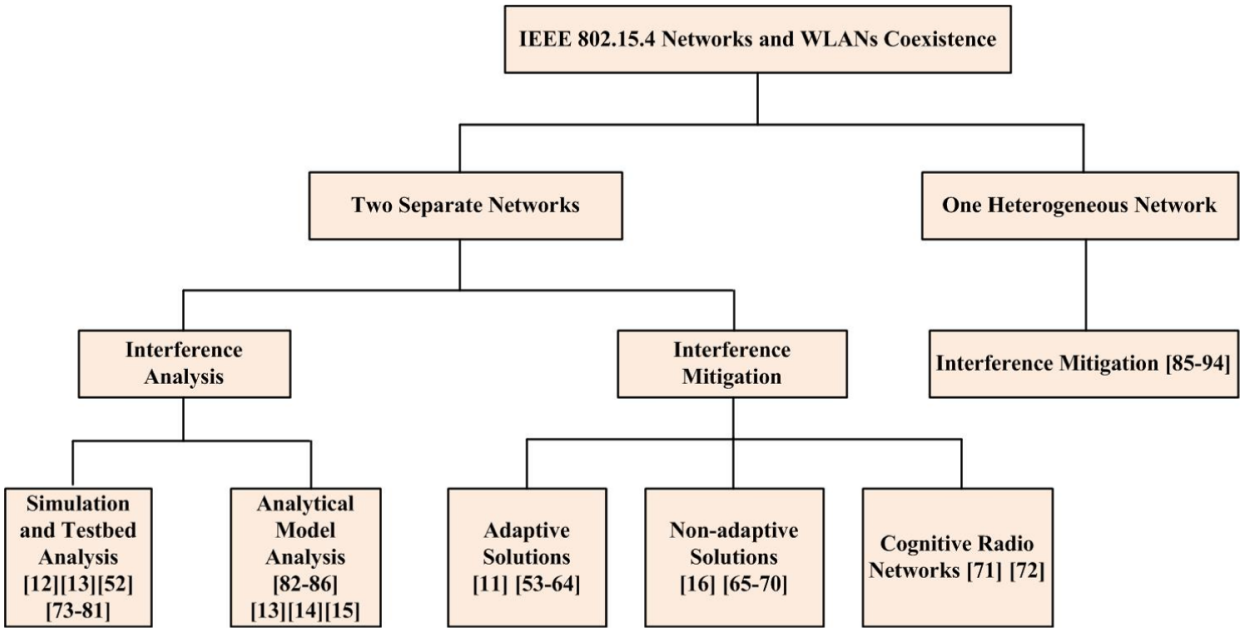


Fig. 11. A Taxonomy of Coexistence and Interference Mitigation Solutions between IEEE 802.15.4 Networks and WLANs.

the second CCA and finds the channel occupied by the IEEE 802.11 networks. The IEEE 802.15.4 networks have to back off for a fourth time. Although IEEE 802.11 packet size is larger than that of IEEE 802.15.4 networks but with a much faster transmission rate and much smaller back-off time slots, so IEEE 802.11 networks can complete the transmission faster and seize the channel for a new transmission. Moreover, the high level of transmit power and coverage range of the IEEE 802.11 networks could interfere with IEEE 802.15.4 networks on a large scale.

IV. Coexistence and Interference Mitigation Solutions Between IEEE 802.15.4 Networks and WLANs

This section summarizes normal solutions to mitigate co-channel interference and explains the impacting factors on the network performance. Most researchers conducted research and analyses with four domains: frequency, time, space and transmit power. Firstly, due to the share of the 2.4 GHz channel, the frame error rate of IEEE 802.15.4 networks could go up to 70% [52], while it sharply decreases as the distance of two networks' central frequencies increases. Particularly, as the frequency offset of the two networks increases to 7 MHz, the frame error rate decreases to zero. Secondly, sending a large-sized packet could increase the frame error rate as the packet could experience longer airtime with a colliding packet. Thirdly, separating the two networks over a long distance can definitely avoid co-channel interference. Fourthly, WLANs normally transmit packets at a power level between 1 to 250 mW, whereas IEEE 802.15.4 devices at 1 mW. These differences make it possible for WLANs to cause more harm to IEEE 802.15.4 networks. The receiver sensitivity for IEEE 802.15.4 is recommended at −98 dBm, whereas for WLANs is −95 dBm depending on modulation schemes. The IEEE 802.15.4 Standard [47] discusses coexistence issues between IEEE 802.15.4 networks and other networks sharing the license-free band and suggests that WLANs operate at low transmit power to alleviate co-channel interference.

Many studies made additional contributions to enable the coexistence between IEEE 802.15.4-based WPANs and WLANs. According to the literature, the research on this topic can be summarized into two categories as shown in Fig. 11: (1) two separate networks; namely, the IEEE 802.15.4 network and the WLAN are two separate networks, and (2) one heterogeneous network; namely, the IEEE 802.15.4 network is connected to the WLAN to form one network. The two-network scenario has been widely investigated and can be further categorized into interference analysis and interference mitigation solutions. Unfortunately, interference mitigation in one heterogeneous network scenario has not been fully investigated because two heterogeneous radios on one physical device can cause very high level of co-channel interference due to the proximity of the heterogeneous transceivers.

A. Two Separate Networks

This category includes interference mitigation and interference analysis. The former can be grouped into adaptive solutions, non-adaptive solutions and cognitive radio networks, while the latter can be classified into simulation and testbed analysis, and analytical model analysis.

1) Adaptive Solutions: The adaptive solutions include two stages: the interference detection stage and the interference mitigation stage. Co-channel interference can be detected using Physical and MAC layer metrics such as the Bit Error Rate (BER) and RSS, the number of ACK packets and so on. Then the adaptive solutions use numerous techniques such as channel switching and power control to mitigate interference. Tang *et al.* [53] proposed an algorithm named Interference-Aware Adaptive Clear Channel Assessment (IAACCA) to reduce the packet loss rate of the ZigBee network. With this

algorithm, a ZigBee node constantly monitors the channel to determine the idle period is long enough to accommodate a ZigBee packet without interference. If the idle period is not sufficient to transmit a ZigBee packet, the size of the ZigBee packet is adaptively reduced to fit the idle period. When an entire ZigBee packet cannot be transmitted due to a busy channel, a channel switching procedure is activated at the detection stage. All the ZigBee nodes change to a free or less-affected channel at the mitigation stage. Jung *et al.* in [54] proposed a Time Division Multiple Access (TDMA) solution. At the detection stage, the PER is used to determine the timing when the ZigBee nodes switch to a free channel. An interference mediator serves as coordinator and gathers the PER. If the PER is larger than a pre-defined threshold, the mitigation stage is activated, so the WLAN packets are transmitted with the inactive period of the ZigBee node, the ZigBee packets are transmitted within the WLAN Point Coordination Function (PCF) period. The same authors proposed another solution in [55]. They use a mediator that has a set of ZigBee transceivers and a set of WLAN transceivers in order to coordinate the WLAN and ZigBee transmissions. In other words, the ZigBee part of the mediator communicates with the ZigBee nodes and the WLAN part only communicates to the WLAN nodes. To evaluate the level of co-channel interference, the ACK packets between ZigBee devices and the PAN coordinator are monitored by the mediator. At the detection stage, as the mediator finds out that the coordinator receives fewer ACK packets, meaning that ACK packets could have been lost due to interference. At the mitigation stage, if the channel is busy, the mediator activates the interference mitigation process. Then the WLAN part of the mediator starts to use the NAV to schedule the transmissions of the WLAN stations, so the ZigBee devices are not interfered.

Wang *et al.* [56] investigated the lost ACK packets at the detection stage. They found that the ACK packets caused by re-transmissions could be affected due to co-channel interference immediately after a packet transmission. To tackle this issue, the coordinator of the ZigBee nodes records N successive RSSI values for 16 μs. If the mean value of the N RSSI readings is below a pre-defined threshold in the mitigation stage, then the ACK packet is transmitted. As the ACK packet is only 11 bytes, the successful delivery rate of the ACK packets is high if a channel is idle. Apart from the measurement of lost ACK packets, Torabi *et al.* [57] discovered that beacons were corrupted due to interference. When the channel is busy, the interference mitigation process is triggered at the detection stage. Since the ZigBee channel 25 is not impacted by interference as shown in Fig. 9, it can be used as a broadcast channel to notify the ZigBee nodes of switching to a free channel in the second stage. More precisely, one slot within the CAP is employed as an alarm slot, and another is used as a switching slot. At the mitigation stage, when a number of corrupted beacons are detected by an end device, the end device transmits a short message within the alarm slot, notifying the PAN coordinator of the interference using channel 25. After that, all the end devices tune to the new channel to avoid interference.

Yuan *et al.* [58] proposed an adaptive CCA solution in a distributed manner. In the detection stage, if the Energy Detection (ED) process of the ZigBee nodes detects the interference, they increase their ED threshold to decrease the packet losses in the mitigation stage. Once the interference disappears, the ZigBee nodes restore the initial ED value to avoid the situation in which some less affected nodes have more chances to transmit packets. An adaptive back-off solution proposed by Ndih and Cherkaoui [59] is that if the ZigBee nodes detect that the channel is busy due to a WLAN transmission instead of a ZigBee transmission, both the Backoff Exponent (BE) and the Number of Back-offs (NB) remain the same with a slight change of the backoff window in the detection stage. The value of the backoff window chosen by the ZigBee node is between zero and two CCAs to mitigate the interference in the mitigation stage. Hong *et al.* [60] adopted the ZigBee end-to-end delay as a metric to evaluate the system performance and employed the gateway as the coordinator that monitors the delay and sends control signals in the detection stage. The ZigBee MAC delay D and WLAN throughput S are mathematically derived. In the mitigation stage, if D is larger than $Dmax$ and S is larger than $Smax$, the coordinator sends a wait signal to suspend the WLAN traffic until the delay and throughput are less the predefined thresholds. The algorithm can maintain the QoS of ZigBee nodes in a Smart Home while retaining a reasonable throughput of the WLANs. Yi *et al.* [11] proposed a channel switching algorithm. The PER and RSSI are used to detect the interference in the detection stage, and once the interference is detected, the algorithm starts to search available channels in the mitigation stage. The authors recommended that switching to another free channel be better and the ZigBee and WLAN networks be placed at least four meters to each other to alleviate co-channel interference.

Tamilselvan and Shanmugam [61] also proposed a channel switching solution for the WPANs grouped and assigned with different frequencies in the mitigation stage. Dynamic time slots are allocated to the WLANs to avoid the interference with the WPAN nodes. Kang *et al.* [62] presented a multi-channel solution. In the detection stage, if one ZigBee node detects the interference, it transmits a Channel Change Broadcast Message (CCBM). Upon receiving this message, the other ZigBee nodes and the PAN coordinator in the same channel group will be notified of the interference. In the mitigation stage, all nodes change to the next channel and re-associate with the PAN coordinator. Tytgat *et al.* [63] proposed a multi-frequency ZigBee network in an office environment in which the interference caused by WLANs is dynamic. The receiver and transmitter in one ZigBee node use two different channels. The network uses the PER as an internal trigger to determine the most suitable channel switching time. Specifically, each ZigBee node selects the channel with the least average PER to avoid co-channel interference. Li *et al.* [64] designed an Adaptive fRequency-Temporal (ART) co-existing framework to deal with co-channel interference between a multi-channel ZigBee network and WiFi. The framework consists of two parts: the first part allocates continuous center frequencies to ZigBee nodes to exploit the unused WiFi channels, which can be formulated into a spatial tessellation problem in a unified

frequency-spatial space, and the other part uses Probabilistic CSMA to opportunistically access the unused WiFi channels to avoid WiFi interference.

2) Non-Adaptive Solutions: Unlike the adaptive solutions, non-adaptive solutions do not have the detection and mitigation stages; rather, they directly deploy their strategies to alleviate interference. This is because in this case WPANs and WLANs are in a close range, so it is urgent to abate the interference immediately; otherwise, the QoS of WPANs could be compromised by WLANs. Zhang and Shin [16] proposed an interference mitigation scheme named the Cooperative Busy Tone (CBT). In this scheme, a central ZigBee controller emits a signal that is strong enough to make the WLAN nodes back off while the ZigBee transmissions are ongoing. The main objective of the busy tone is to enhance the ZigBee visibility by using the strong signal. Specifically, when a ZigBee device transmits on current channel, the ZigBee controller switches to an adjoining channel and emits a strong signal (the CBT), forcing the WLAN nodes to back off until the ZigBee device ends the transmission. The CBT increases the ZigBee throughput in the presence of WLAN co-channel interference. Similarly, Ock *et al.* [65] extended the CBT into a periodical CBT that is effective in mitigating the interference for a multi-hop ZigBee network. Lim *et al.* [66] presented another solution named Narrow Band Protection (NBP), which is also based on the idea of the CBT. More precisely, when a ZigBee node detects a free channel and transmits a packet, a NBP ZigBee protector senses the ZigBee packet by cross correlating it with the pre-defined Pseudo-random Noise (PN) sequence and estimates the duration of the transmission. Then the protector switches to the adjacent channel and reserves it by emitting a strong signal for the estimated duration, so the ZigBee packet transmissions will not be affected. However, the busy tone method has one drawback that the ZigBee protector needs to hop on the adjacent sub-channel to release the busy tone, which would consume more power than using a single channel. Kim *et al.* [67] proposed a full-duplex-based busy tone solution in which the busy tone is emitted on the same channel when transmitting ZigBee packets and is cancelled by a customized canceller implemented in hardware to avoid self-interference but strong enough to defer the WLANs.

Chen and Gao [68] have proposed an interference mitigation solution. This solution involves a module on the WiFi side that can detect weak ZigBee signals using Fast Fourier Transformation (FFT) and reserve the channel for the ZigBee transmissions. Therefore, the ZigBee network can successfully transmit packets without being interfered by WLANs. Liang *et al.* [69] found that ZigBee headers could be corrupted due to co-channel interference. The authors defined two cases regarding the interference: a symmetric case in which the ZigBee and WLAN nodes can detect each other and an asymmetric case in which the ZigBee nodes can sense the WLAN nodes, but not vice versa. As a result, the authors proposed a solution named BuzzBuzz that fully takes advantage of the header and payload redundancy. In the first case, a ZigBee node sends the header multiple times, and the first header causes the WLAN node to back off, ensuring the second one can be sensed by the ZigBee receiver. In the second case, the ZigBee nodes use a Forward Error Correction (FEC) Code to recover the corrupted ZigBee payloads. The results show that this solution can improve the ZigBee packet reception rate by 70% and increase the WLAN throughput by 10%. Yan *et al.* [70] proposed an interference cancellation technique named WizBee (Wise ZigBee). The work replaces the traditional ZigBee sink with a modified ZigBee sink so that the latter can recover the corrupted ZigBee packets using the WLAN interference cancellation technique including the Viterbi decoding scheme across different sub-carriers and a data-aided channel coefficient computation scheme for frequency offset compensation. Compared with other solutions, more advanced solutions tend to focus more on the Physical Layer techniques using such as FFT, the FEC and the Viterbi decoding scheme to actively detect and cancel the interference [68]–[70], or focus on building a framework that fully consider the frequency, time, space and power these factors to alleviate the interference [64]. These solutions have showed the best performances and have the potential to be applied for a large-scale dense network under the IoT era. Overall, advantages and drawbacks of the adaptive and non-adaptive mitigation solutions are summarized in Table III and Table IV, respectively.

3) Cognitive Radio Networks: Cognitive radio networks are a promising solution for mitigating co-channel interference. Many studies have attempted to solve the coexistence issue using cognitive radio networks. Yang *et al.* [71] developed a Markov Chain model to characterize the dynamics of spectrum sharing for one and multiple channel cases in which Secondary Users (SU) are subject to two independent Primary Users (PU). The service time and average waiting time of the SU transmission are derived. The analytical model can be used to predict the ZigBee network performance as SU under the interference of WLANs. Lee *et al.* [72] proposed a cognitive beam-forming algorithm to mitigate co-channel interference between WLANs and smart meters in Smart Grids. An assumption that the home appliance has multiple antennas is considered. The algorithm aims at minimizing the transmit power in the Smart Grid with a constraint of SU's QoS. With this design, home appliances can transmit information via WLANs on the free channel while maintaining the QoS of the Smart Grid.

4) Simulation and Testbed Analysis: Petrova *et al.* [52] conducted real testbed experiments using a pair of WLAN nodes and a pair of ZigBee nodes to determine how co-channel interference impacts on both networks. If the WLAN nodes are the victims, the WLAN packet loss rate remains stable in the presence of ZigBee devices. However, if the ZigBee nodes are the victims, the ZigBee packet loss rate drops sharply due to the detrimental impact of the WLAN nodes. When the WLAN nodes start to transmit, the packet loss rate of the ZigBee nodes increases up to 70%. The study is important because it could be used as a reference model when applying the network resource allocation techniques. Sikora and Groza [73] investigated how Bluetooth devices, WLANs and microwave ovens affect WPANs. Since they all share the 2.4 GHz license-free band, WLAN devices adversely affect the WPANs, causing significant packet losses due to

TABLE III
SUMMARY OF THE ADAPTIVE AND NON-ADAPTIVE SOLUTIONS OF THE INTERFERENCE MITIGATION FOR IEEE 802.15.4 NETWORKS AND WLANS

Solutions	Solution Domain	Power Consumption	Scalability	Ways of Control	Evaluation Setting	Latency	Triggering methods
Yuan in [58]	Power	Low	High	Distributed	OPNET Simulation	Low	CCA Energy Detection
Ndih in [59]	Power	Low	High	Distributed	MATLAB Simulation	Low	CCA Energy Detection
Wang in [56]	Power	Low	High	Distributed	Real testbeds	Medium	RSSI
Chen in [68]	Frequency	Low	High	Distributed	Real testbeds	Low	ZigBee Signal
Torabi in [57]	Frequency	Medium	Low	Centralized	Theory and simulation	Medium	K lost Beacons
Yan in [70]	Frequency and Power	High	High	Distributed	Real testbeds	Medium	Directly decode and recover corrupted ZigBee packets
Jung in [55]	Time	Low	High	Centralized	Real testbeds	High	RSSI and ACK
Tamilselvan in [61]	Time	High	Low	Centralized	Simulations	Low	PER
Tang in [53]	Time	Medium	Low	Centralized	Real testbeds	Medium	The channel idle time
Yi in [11]	Time	Low	Low	Centralized	Real testbeds and simulation	Low	RSSI threshold
Kang in [62]	Time	High	High	Distributed	Real testbeds	Medium	Beacon, ACK/NACK
Jung in [54]	Time	Medium	High	Centralized	Simulations	Low	PER
Lieven in [63]	Time	High	High	Centralized	Real testbeds	Medium	Average PER
Zhang in [16], [65]	Time	High	High	Centralized	Real testbedd and simulation	Medium	WiFi signal
Chen in [68]	Time	Low	High	Distributed	Real testbeds	Low	ZigBee Signal
Hong in [60]	Time	Medium	Low	Centralized	Simulation	Low	Delay threshold
Sangsoon in [66]	Time	Low	High	Distributed	Real testbeds and NS-2	Low	ZigBee Signal
Liang in [69]	Time	high	High	Distributed	Real testbeds	Low	WiFi signal
Li in [64]	Frequency, Space and time	high	High	Distributed	Real testbeds	Low	ZigBee throughput and Packet Reception Ratio

TABLE IV
ADVANTAGES AND DRAWBACKS OF THE ADAPTIVE AND NON-ADAPTIVE SOLUTIONS

Solutions	Advantages	Drawbacks
Yuan in [58]	Easy and fast to implement in a distributed manner	The channel can be seized by the other nodes if the ED threshold does not decrease promptly
Ndih in [59]	Simple and efficient in mitigating the interference	Need to modify the IEEE 802.15.4 and firmware
Wang in [56]	Easy and simple to implement	The MAC delay increases due to RSSI readings
Chen in [68]	Simple to implement with the increased ZigBee throughput	Decrease in WLAN throughput by 10%
Torabi in [57]	Effective in recovering the corrupted beacons and avoid WLAN interference	Need to modify the IEEE 8021.5.4 Standard and the beacon structure. Might not be useful in a dense WLAN scenario
Jung in [55]	Effective in mitigating WLAN interference even in a harsh environment by adjusting the ZigBee packet length	Need to interact with the WLAN that uses NAV to suspend other WLAN's transmissions and might increase the delay
Tamilselvan in [61]	Effective in mitigating WLAN interference	Grouping nodes and assigning with different frequencies based on their transmit power might increase the system cost
Tang in [53]	Easy to implement in hardware	Might not be effective in a dense WLAN scenario
Yi in [11]	Easy to implement and switch to the idle channel	Might not be effective in a dense WLAN scenario
Kang in [62]	Effectively mitigate interference	Exchanging grouping messages could increase the system cost and delay
Jung in [54]	Easy and simple to implement	Might not be suitable for multi-hop IEEE 802.15.4 networks due to the exhausted inactive periods
Lieven in [63]	Effectively mitigate co-channel interference	Need to change the IEEE 802.15.4 Standard and consume more energy due to the channel switching
Zhang in [16], [65]	Effectively protect ZigBee from the WLAN interference	The busy tone might consume high energy and the interactive process could increase the delay
Hong in [60]	Simple and efficient in mitigating interference	Need a controller and increase energy consumption If the controller fails, the system breaks down
Sangsoon in [66]	Easy and simple to implement	ZigBee consumes more energy
Liang in [69]	Effectively increase ZigBee network delivery rate and in reducing ZigBee re-transmissions by a factor of three.	Due to the use of multiple headers, the system might consume more energy
Yan in [70]	Effectively increase both ZigBee and WLAN throughput	Might increase delay and energey consumption
Li in [64]	Effectively increase ZigBee throughput and decrease its latency	Might increase energey consumption

the high transmit power. On the other hand, the microwave ovens and Bluetooth devices do not heavily interfere with the WPANs, and the average packet error rate of the WPANs is approximately 10%. As the IEEE 802.15.4 channel 25 and 26 are not interfered by the WLANs, these two channels are recommended to avoid the interference.

Rihan *et al.* [12] discovered that the blind coexistence of ZigBee, Bluetooth and WLAN nodes could exert a detrimental impact on ZigBee nodes. To investigate the impact of co-channel interference, metrics such as the Received Signal Strength Indicator (RSSI), packet error rate and link Quality Indicator were employed to study co-channel impact on ZigBee nodes. Chong *et al.* [13] compared the ZigBee throughput results using the testbed and analytical model. Specifically, the saturated throughput of the ZigBee nodes has been derived from the analytical model agreed well with the testbed results that the ZigBee throughput decreased in the presence of co-channel interference. Verma [74] systemically investigated the mutual interference between IEEE 802.15.4 networks and WLAN variants (IEEE 802.11 b/g/n). The author conducted a series of testbeds experiments using the packet deliver ratio at the receiver side of an IEEE 802.15.4 device and found that IEEE 802.15.4 networks are often subject to WLAN interference. More specifically, for IEEE 802.11 b/g/n networks, channel 1, 6 and 11 were adopted. For example, for channel 1 of the 802.11 b network, the channels 11-13 of IEEE 802.15.4 should be avoided to mitigate co-channel interference.

Yoon *et al.* [75] analyzed how WLANs impact on WPAN's transmissions in terms of the PER and the collision time duration. The PER is used to derive the safe distance in which the WPANs are placed four meters away from the WLANs. The test results showed that the safe distance can effectively reduce co-channel interference. A similar conclusion can also be found in [76]. Yang and Yu [77] found that the center frequency offset and the distance between WLAN and ZigBee nodes are significant. Specifically, larger frequency offsets lead to a lower ZigBee packet loss rate, and the level of co-channel interference decreases as the distance increases. IEEE 802.11b nodes interfere with ZigBee more severely than IEEE 802.11g nodes due to longer air times caused by lower data rates. Tao *et al.* [78] found out that ZigBee transmissions are severely subject to the fast and frequent WiFi interference, and it is impossible to mitigate interference with MAC layer solutions. Howitt and Gutierrez [79] adopted the packet collision probability as the metric and analyzed co-channel interference. The authors found out ZigBee have no or little impact on the WLAN's performance. Although most studies have proved that WLANs can have detrimental impacts on ZigBee networks, Pollin *et al.* [80] conducted measurements of ZigBee impacts on WLANs and found out that the WLAN's performance could be degraded when the ZigBee network uses a very high packet transmission rate. Zhen *et al.* [81] used the central limit theorem to derive closed-form expressions for energy-based Clear Channel Assessment (CCA). The authors found out that WPANs are oversensitive to 802.11b signals, which are insensitive to WPANs. The authors also recommended that a higher CCA threshold for WPANs can increase spatial reusage, while a lower CCA threshold for WLANs can help sense WPAN signals, which improves the medium sharing fairness.

5) Analytical Models: This section summarizes the mathematical models that can mimic the impact of co-channel interference caused by WLANs. Luong *et al.* [82] presented a bidimensional discrete-time Markov Chain (MC) model that characterizes the behaviour of the pair of WLAN and ZigBee nodes. The ZigBee throughput in the presence of the WLANs is derived via the MC model. The analytical throughput results match with the simulation results quite well, validating the proposed MC model. The ZigBee throughput decreases as the packet arrival rate of the WLAN node increases. Chong *et al.* [13] also used a MC model to describe the operation of each ZigBee device in the presence of WLAN interference. Based on the MC model, the normalized saturation throughput of the ZigBee nodes with co-channel interference is derived. The simulation results agree well with the analytical results. With the WLAN co-channel interference, the throughput decreases much more than that of the case without the WLAN interference. The derived model can also be used to predict the ZigBee performance with the WLANs sharing the same channel. Shin [14] modified the bidimensional Markov Chain model presented in [15] by considering the packet transmission, packet losses and ACK reception in time slots. The saturated ZigBee throughput is derived via the modified Markov Chain model. The simulation results closely match the theoretical expressions, proving the effectiveness of the proposed model.

Tas *et al.* [83] mathematically derived the channel utilization of the ZigBee network under the influence of WLANs via the analysis of the overlapping transmission duration of the ZigBee and WLANs. Through the analysis, the authors found that the WLAN packet size can be tuned to mitigate co-channel interference if 802.11 traffic is moderate. Han *et al.* [84] proposed a one-state MC model that characterizes the successful and failed transmissions. The ZigBee throughput is derived from the Markov Chain model. Without the WLAN interference, the ZigBee throughput increases as the packet size increases, but with the WLAN interference, the ZigBee throughput only reaches a peak and then steadily declines as the packet size increases. This is because the larger the ZigBee packet size is, the higher chance that the ZigBee packets collide with the WLAN packets.

Zhang *et al.* [85] proposed an analytical model for 802.15.4 and 802.11 devices coexistence when predicting the 802.15.4 delay and 802.11 throughput using the M/G/1 queuing and Markov Chain models in the NS-3 simulator. Since it is difficult to transmit 802.15.4 packets in a timely manner in the presence of 802.11 devices, the coexistence model provides a tuning method to guarantee the 802.15.4 delay constraints between 50 to 100 ms and maximize the 802.11 throughput between 27 to 78 Mbps. El-Keyi *et al.* [86] proposed a probabilistic path loss model for Smart Homes where 802.11 and 802.15.4 devices coexist using the NS-3 simulator. The model explicitly accounts for additional path loss from wall penetration, scattering, reflection and diffraction. The probability of encountering additional path loss depends only on the distance between the receiver and the transmitter. Typical Smart Home application traffic is modelled to show that the data rate and density of the interfering nodes have an impact on the 802.11 and 802.15.4 throughputs.

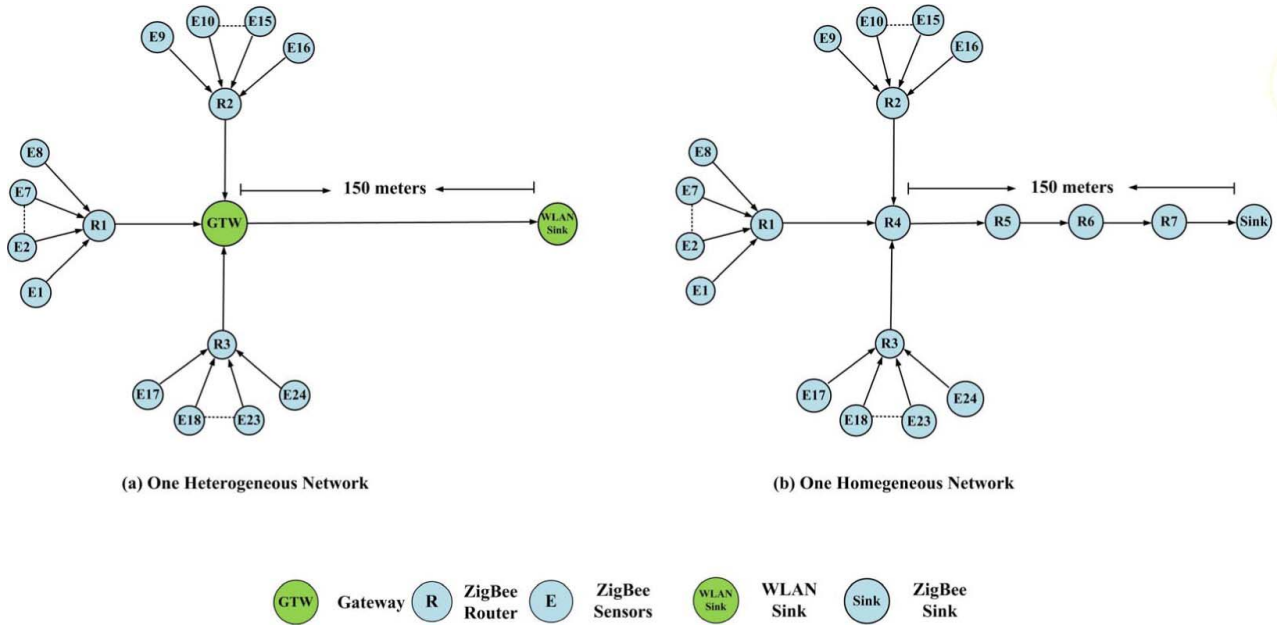


Fig. 12. Comparison of a heterogeneous network and a homogeneous network.

B. One Heterogeneous Network

The majority of the studies mitigate co-channel interference on two independent IEEE 802.15.4 and IEEE 802.11 networks. However, few studies investigated the co-channel interference in one single heterogeneous network where data is collected from IEEE 802.15.4 networks, forwarded to IEEE 802.15.4/WLAN gateways and transmitted by the WLAN interfaces in the gateway. As shown in Fig. 12, the 150-meter link in (b) has been replaced by the IEEE 802.15.4/WLAN gateway and the WLAN sink in (a) to decrease the number of hops and increase the Packet Reception Rate. The interference caused by such heterogeneous network is often more severe than that of the two separate networks. This is because if the IEEE 802.15.4 network's current channel is overlapped with the one the WLAN is using in a single network, the interference is persistent, whereas the interference incurred by the two separate networks are intermittent depending on the types of applications. For example, in a Smart Home, a ZigBee smart meter sends meter reading data to the smart gateway, encountering the interference from the WLAN between the access point and a laptop. If the meter finishes transmitting data, the interference is gone.

A single heterogeneous network comprised of the IEEE 802.15.4 and IEEE 802.11 networks was proposed in [87] to reduce the number of hops in a multi-hop IEEE 802.15.4 network while maintaining the same coverage. This extension could create co-channel interference with the IEEE 802.15.4 network, so the packet aggregation technique is employed to decrease the number of the WLAN packets, thereby avoiding the probability of colliding with the packets of the IEEE 802.15.4 networks. Huang and Park [88] proposed an interference mitigation solution for the wearable health monitoring system. ZigBee sensors are attached to humans to monitor blood pressure and the heart rate, and a ZigBee/WLAN gateway is responsible for transmitting the collected data using the WLAN interface to a WLAN AP, which connects a back-end server. If the sensor captures a time-sensitive signal, it uses a GTS to the ZigBee/WLAN in a collision-free mode and the gateway reserves the channel by using Network Allocation Vector (NAV) to defer the other ZigBee/WLAN gateways and relays the signal to the server.

Other studies also discussed one heterogeneous network consisting of the IEEE 802.15.4/WLAN, but they did not consider co-channel interference. Koubaa and Alves [89] proposed a large-scale dual-radio wireless sensor network, which is connected with WLAN networks to increase data rate and extend the transmission range. The proposed network can improve network performance in a real time manner in terms of reliability and scalability. Due to the longer transmission range and the high data rate of the WLAN, the dual-radio wireless sensor network can transmit the sensor traffic in a real time manner, so WLANs can be adopted as backbone networks supporting transmissions in a wide area with high throughput. However, this study did not provide detailed testbed or simulation results. Similar studies are proposed in [90], [91]. A wireless sensor network supporting the IP protocol was proposed in [92], and this IP-based network is connected with WLANs to enable a fast and cost-effective connection to the Internet. In this study, a gateway has been implemented using TI CC2528 devices, but the study did not present any concrete results or test plans.

The dual-radio WiFi/ZigBee network can also be deployed in the Smart building to assist Advanced Metering Infrastructure (AMI) with heavy network loads [93]. A case study based on the simulation of a one-hop network was conducted to further investigate the hybrid network performance. The round trip time for demand response applications was 0.6 s, and smart metering one-way time transmission was round 9 s.

Wang and Leung [94] also presented a dual-radio WiFi/ZigBee network and compared its performance with that of the ZigBee network using the OPNET modeller. The simulation results showed that the proposed dual-radio network outperformed the single ZigBee network in terms of the packet loss rate, throughput and average end-to-end delay. Another application of the WiFi/ZigBee network is to monitor transportation networks such as truck platoons and trains [95]. More precisely, sensors were grouped into several clusters within different train carriages, and these carriages were wirelessly connected using the WiFi/ZigBee nodes. The OPNET simulation results and the analytical analysis showed a good agreement, but this study did not consider co-channel interference. Above all, most of the above studies did not consider co-channel interference in their measurements, so we proposed an algorithm named Blank Burst to mitigate co-channel interference in a dense area network. The interested reader can refer to [96] for more details.

V. Coexistence and Interference Mitigation Solutions Between Bluetooth and WLANs

A. Bluetooth Overview

Apart from IEEE 802.15.4 networks, Bluetooth is another integral part of WPANs and also shares the 2.4 GHz band with WLANs [97]. This section discusses the coexistence and interference mitigation between Bluetooth and WLANs. The Bluetooth technology is designed to replace non-interoperable proprietary cables connecting cordless phones, laptops, headsets and other portable devices. Similar to IEEE 802.15.4 devices, classic Bluetooth operates in the 2.4 GHz frequency band with 79 radio frequency channels of 1 MHz width and transmit data packets normally at 1mW (Bluetooth Low Energy has 40 radio frequency channels with each taking up 2 MHz, which is not depicted in Fig. 15). The modulation scheme at the Physical Layer is Binary Gaussian Frequency-Shift Keying (GFSK), and the defined data rate is 1 Mbps. In particular, the channel is divided into many micro-channels, each of which occupies 625 μs, so there are 1600 slots in one minute. The transmission of a packet only occurs at the odd number of slots, and the even number of slots are reserved for the receiving packets. In addition, Bluetooth uses the Frequency Hopping technology to mitigate possible interference. The maximum hopping rate is 1600 hops/s, and each small-sized packet takes up one time slot and is transmitted with a different frequency. In contrast, a large-sized packet can take up to five time slots with a minimum frequency hopping rate of 320 hops/s. The transmission of a large-sized packet always adopts the frequency of the first slot until the end of the transmission.

More than two Bluetooth devices can form a piconet, where one device serves as a master and the other devices act as slaves. Each piconet allows a maximum seven slaves to connect to the master simultaneously and uses a master's pseudo-random frequency hopping sequence obtained from the master's 48-bit address. The frequency hopping pattern is generated as follows. Firstly, the frequency band from 2.402 GHz to 2.480 GHz is classified into 79 odd and even frequencies. A window with 32 frequencies is used. The frequency hopping sequence is randomly chosen from the window that contains the first 32 out of 79 frequencies. After the first sequence is executed, a new window is configured with 16 previous frequencies and 16 out of remaining 47 frequencies. Once the connection between slaves and a master is established, the slaves synchronize their timing and frequency hopping with the master. The master controls the access to the channel of the slaves using a polling mechanism, meaning that as long as the master has a packet to transmit, it sends a broadcast packet to all the slaves to ask whose packet it is. If a slave replies, the master transmits the packet to that slave while the other slaves remain silent. A slave always follows a master's packet transmission, as shown in Fig. 13 from the master's perspective. A slave must reply to a packet that is sent by a master and specifically addressed to it. If the slave has no data to transmit, it sends a NULL packet instead.

Bluetooth devices have two types of links: the Asynchronous Connection Link (ACL) and the Synchronous Connection-Oriented (SCO) link. The ACL is for data transmissions between a master and a slave. The ACL includes two packet formats: DMn and DHn packets that take up an odd number of frequency-hopping slots (n=1, 3 and 5). The DM format has Forward Error Correction (FEC), whereas the DHn format does not. To prevent packet losses, the Automatic Repeat Request (ARQ) protocol is adopted to reply the sender with an ACK packet. In contrast, the SCO link is intended for a voice connection between a master and a slave. There are three types of packet formats: HV1, HV2 and HV3. These packets are transmitted at regular time intervals, denoted by T_{SCO}. Specifically, the T_{SCO} is assigned for two, four and six time slots for the HV1, HV2 and HV3 formats with 80 bits, 160 bits and 240 bits of information transmitted, respectively. Unlike the ACL, the SCO link has no retransmissions to prevent packet losses. In addition, the basic packet format for Bluetooth packets is shown in Fig. 14. The format contains a 72-bit access code, a 54-bit header and a variable size of the payload with data or voice packets depending on the connection established between a master and a slave. The access code is for message identification and synchronization. The header includes the active slave address AM_ADDR and the packet type TYPE. The header includes an ARQ Number (ARQN) that indicates whether the previous packet has been successfully received or not, and includes the Sequence Number (SEQN) that facilitates the ordering of the data packets. The differences between Bluetooth and WLANs are presented in Table V.

Similar to IEEE 802.15.4 networks, Bluetooth uses the 2.4 GHz ISM frequency band and could encounter co-channel interference, as shown in Fig. 15. To tackle this problem, the IEEE 802.15.2 Task Group proposes two solutions in [99] for the coexistence between Bluetooth networks and WLANs, as shown in Fig. 16. The first is a collaborative solution in which the Bluetooth and the WLAN residing on the same device collaborate to mitigate the interference, which is similar to one heterogeneous network comprised of an IEEE 802.15.4 network and a WLAN. The second is non-collaborative solutions that alleviate the interference between separate Bluetooth networks and WLANs. This group can be

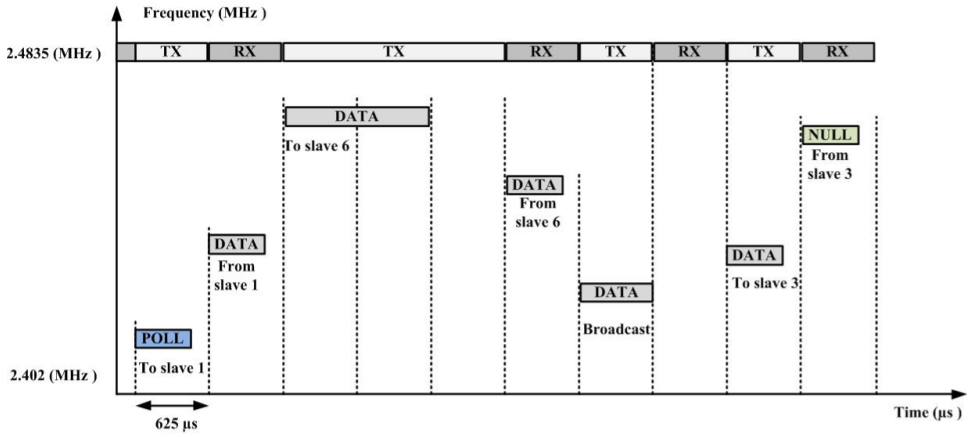


Fig. 13. The hopping sequence from a master's perspective [98].

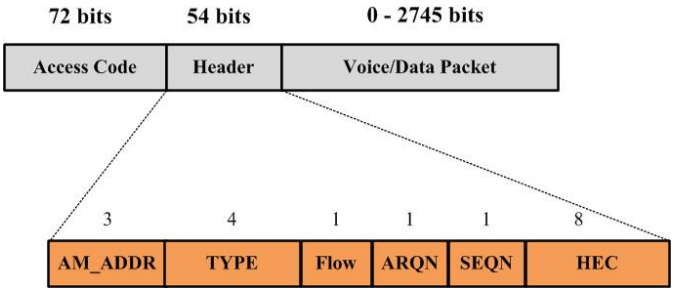


Fig. 14. Bluetooth packet format [33].

TABLE V
DIFFERENCES BETWEEN BLUETOOTH AND IEEE 802.11 g WLANS

Parameters	Bluetooth	IEEE 802.11g WLAN
Transmit Power	1 to 10 dBm	0 to 20 dBm
Receiver Sensitivity	-95 dBm	-95 dBm
CCA threshold	N/A	-84 dBm
Bandwidth	1 MHz	22 MHz
Back-off unit	N/A	9 µs
SIFS	192 µs	10 µs
DIFS	N/A	28 µs
CWmin	N/A	15
CWmax	N/A	1023
Channel Access	Polling	CSMA/CA
Payload Size	80 bytes	1500 bytes
ACK packet	N/A	14 bytes
Max Date rate	1 Mbps	54 Mbps
Coverage Range	1-10 meters	100-150 meters
Max No. of Retransmissions	N/A	7
Basic Cells	Piconet	Basic Service Set

further divided into two categories: interference analysis and interference mitigation. The former includes the analysis for co-channel interference, while the latter uses various solutions to tackle the interference.

B. Non-Collaborative Solutions

Non-collaborative solutions mitigates interference for independent Bluetooth networks and WLANs without cooperation between them. This category includes interference analysis and interference mitigation. The interference analysis can be further divided into analytical model analysis, and simulation and testbed analysis, and the interference mitigation can be divided into adaptive solutions and non-adaptive solutions.

1) Adaptive Solutions: The adaptive solutions mitigate co-channel interference in many ways. The very basic solution is Adaptive Frequency Hopping (AFH) proposed in [23], [24] that groups the interfering channel and free channels into "used" channels and "unused" channels, respectively. As a result, the hopping sequence is generated as per the "unused" channel numbers. Its drawback is that the AFH might need a few seconds to update the channel map to specifically identify the "used" channels. To enhance the AFH scheme, more advanced solutions have been proposed to alleviate co-channel interference. The same author also proposed another method named Backoff Interference Awareness Scheduling (BIAS) [100]. Upon detecting the interference, the Bluetooth network holds the current packet until the next free channel and then transmits the packet. BIAS proves to be more effective than AFH in mitigating co-channel interference in terms of packet losses.

So and Kim [101] proposed an Interference-Aware Frequency Hopping (IAFH) scheme to tackle co-channel interference with dense WLANs. The proposed scheme includes three steps: channel grouping, channel classification and probability-based hopping. More precisely, the proposed IAFH scheme dynamically groups the channel into "good" or "bad" channels, then uses the Bit Error Rate to evaluate the level of interference and transmit Bluetooth packets on "good" frequencies with a non-uniform probability. Lee and Lee [102] enhanced the legacy AFH scheme. The proposed solution groups the Bluetooth channels as per the WiFi channel allocation and classifies the groups according to the level of interference, namely the PER. Then the solution uses a moving average technique to estimate channel quality more accurately. Hsu *et al.* [103] presented an Enhanced Adaptive Frequency Hopping (EAFH) solution. The solution monitors the overall average PER and the individual PER in the hop set, removing the channel associated with the high PER out of the hop set to optimize the performance of the Bluetooth piconet coexisting with other Bluetooth piconet or WLANs. Kwok and Chek [104] compared two interference mitigation solutions: Interference Source Oriented Adaptive

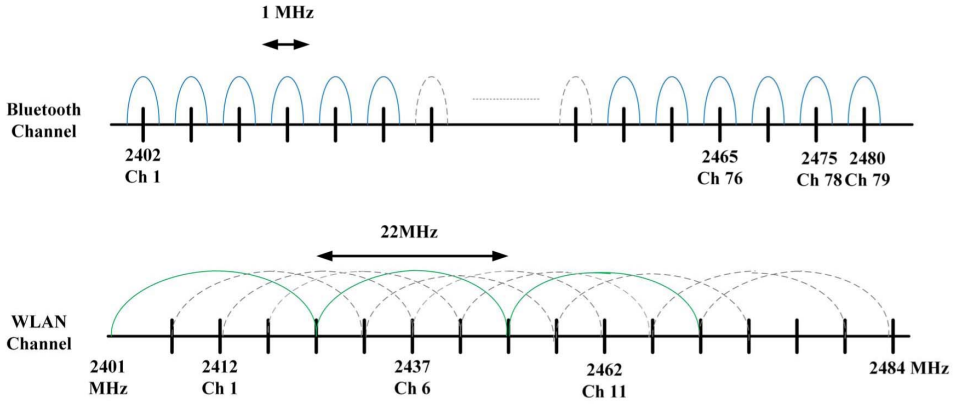


Fig. 15. Sub-channels of Bluetooth and the IEEE 802.11 Standard in the 2.4 GHz band.

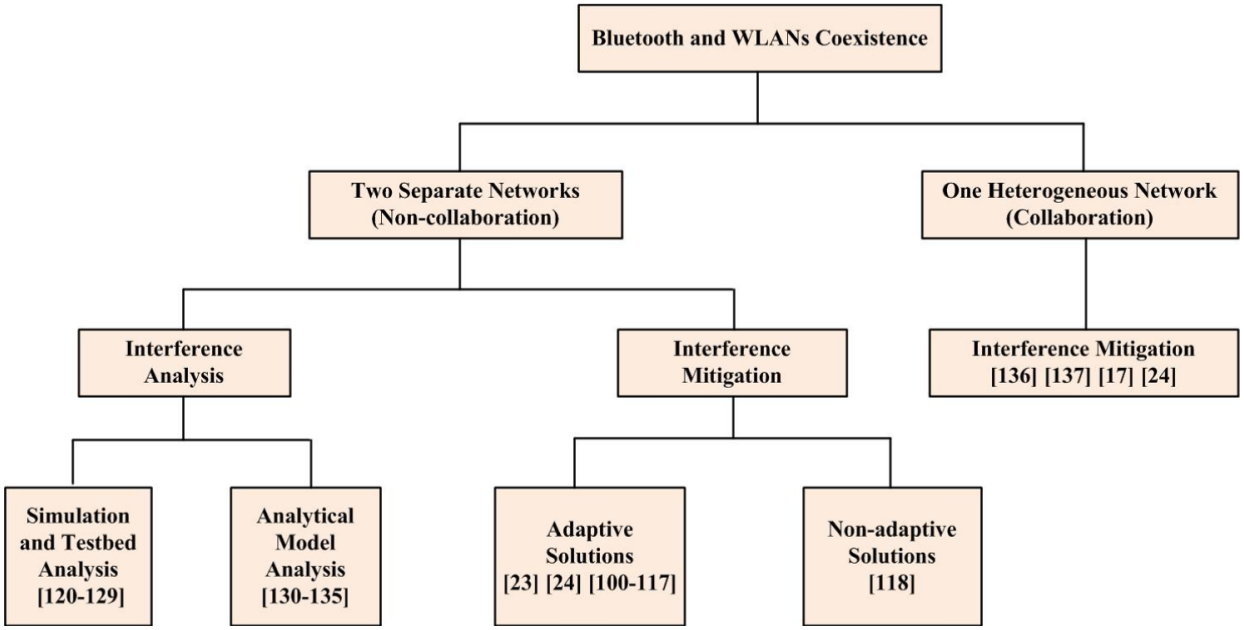


Fig. 16. A Taxonomy of Interference Mitigation Solutions between Bluetooth and WLANs.

Frequency Hopping (ISOAFH) and Interference Source Oriented Master Delay Scheduling (ISOMDMS). The ISOAFH solution improves the conventional AFH, which is sensitive to memory and power limitations, by locating the WLAN channels and avoiding hopping on those channels. In contrast, the ISOMDMS solution reduces the level of co-channel interference by delaying the Bluetooth transmissions.

Taher *et al.* [105] proposed an intelligent Adaptive Frequency Hopping (IAFH) scheme to specifically identify WLAN co-channel interference and alleviate it. More specifically, the IAFH intelligently identifies interfering WLAN channels by determining which WLAN channel has the highest number of interfering Bluetooth channels. For example, if the Bluetooth master detects that WLAN channel 3 has six 'used' channels, channel 4 has five and channel 6 has four, there is a high probability that the WLAN occupies channel 3. Therefore, the IAFH scheme will know that the WLAN is operating on channel 3 and mark all the sub-channels of channel 6 as "used" channels and remove them out of the hopping frequencies. Shao *et al.* [106] proposed a Bluetooth Slot Availability Randomization solution to mitigate co-channel interference in a dense WiFi environment. The rationale behind this is to postpone the Bluetooth packets that are supposed to be transmitted with a probability P, to collision-free time slots. The P is the packet error rate and updated within an packet interval. This solution compared with the legacy AFH significantly improves the WiFi throughput and decreases the WiFi packet losses. Sun *et al.* [107] presented a centralized interference mitigation solution in which a dedicated Bluetooth coordinator controls multiple piconets and parallelizes their frequency hopping sequences. The coordinator also detects WiFi signals to inform all the Bluetooth devices of interfering channels, so these Bluetooth devices can mark the WiFi channels as used channels and update their hopping sequences using the unused channels, thus mitigating co-channel interference. Lee *et al.* [108] proposed a Frequency Hopping (FH) algorithm that mitigates the co-channel interference caused by collocated WLANs and Bluetooth piconets. The algorithm

uses carrier sensing to check if the next FH channel is occupied by other transmissions and removes the channel from the hopping set via the periodical channel classification process. In this process, all available channels are divided into several groups, the PER and Interference Signal Detection Rate (ISDR) are used to test the availability of the channels in a group-wise manner. The algorithm also expands the channel set by incorporating the channels marked as "used" but not actually in use by WLANs.

Howitt and Awad [109] presented an analytical model of the packet transmission time and derive the optimal fragmentation number of the WLAN packets in the presence of collocated Bluetooth interference to boost the network performance. This is because there is a trade-off between an increase in packet overhead caused by packet fragmentation and a decrease in the collision probability due to retransmissions of those fragmented packets. Hsu *et al.* [110], [111] proposed a packet length adaptation solution for mitigating co-channel interference. More specifically, an analytical model has been developed to characterize the interference between Bluetooth and WiFi, and then a dynamical fragmentation scheme is employed to adaptively adjust the size of the WiFi packets as per the PER. If the PER is larger than a calculated threshold, the proposed solution is activated. In doing so, the WiFi and Bluetooth packets have fewer overlapping air times, thus resulting in less co-channel interference. Chiasserini and Rao [112], [113] proposed an adaptive packet size scheme. In this scheme, the Bluetooth master node detects the interference from the WLAN using the RSSI. If the level of interference is intense, the Bluetooth node will use shorter-sized packets or postpone the current packet transmission to mitigate the interference.

N. Golmie combined the power control and packet-postpone techniques to tackle the interference [114], and thus the Bluetooth packet loss rate can be significantly decreased without the increase in the access delay in the MAC layer. The author speculated the use of combined approaches such as traffic scheduling, packet encapsulation and the ARQ would effectively mitigate co-channel interference. Cordeiro *et al.* [115] also proposed a combined technique that involved the AFH and Bluetooth carrier sensing to mitigate the persistent interference [116] and intermittent interference [117]. The persistent interference refers to the interference from the WLAN to the Bluetooth network, whereas the intermittent interference is from Bluetooth to the WLAN. In particular, the carrier sensing mechanism is added within the turnaround time that is the remaining time of one Bluetooth time slot apart from the occupation of a packet transmission.

2) Non-Adaptive Solutions: Apart from the adaptive solutions, there are non-adaptive solutions to cope with co-channel interference. Li and Liu [118] presented a dual-channel solution that transmits the same packet on two separate channels with much less power than that of a single channel. Specifically, the two channels are separated by 22 MHz to ensure the Bluetooth piconet is robust to the WLAN interference. The proposed solution can work without using the PER or BER to detect the interference pattern and work distributively without communicating to other networks. Above all, among all the solutions, only the recent solution [101] adopts the probability-based hopping technique to mitigate co-channel interference and is similar to [64] using a probabilistic CSMA/CA mechanism in Section IV-A.1. The probabilistic CSMA/CA mechanism proves to be effective in mitigating the co-channel interference caused by ZigBee and WLANs, and caused by Bluetooth and WLANs. The summarization of the adaptive and non-adaptive solutions and their advantages and drawbacks are listed in Table VI and Table VII, respectively.

3) Simulation and Testbed Analysis: The co-channel interference between Bluetooth piconets and WLANs have been widely investigated, and some of the studies gave the analysis and discussions on the reasons for co-channel interference between Bluetooth piconets and WLANs in terms of testbeds and simulations. Howitt and Shukla [120] designed a source management tool to understand the relationship between the signal-to-noise ratio and the frequency offset, and to evaluate how the packet transmissions can be interfered with. Matheus and Magnusson [121] conducted a series of fine-grained comparisons and measurements of the Bluetooth behavior with and without WLAN co-channel interference in terms of the packet loss rate. They found that free space propagation, Rayleigh fading and antenna orientation must be considered during simulation, and that the distance to the interferer and time and frequency behaviour also need to be taken into account. Additionally, the levels of interference caused by WLANs and microwave ovens are similar.

Cabral and Lins [122] presented an in-depth discussion on the adverse impact of Bluetooth interference on WLANs. They discovered that Bluetooth transmissions degrade the WLAN performance. They also made another interesting discovery that co-channel interference becomes worse as the distance between Bluetooth and WLAN increases from 2.60 m to 4.60 m. This is because Bluetooth uses DM1 packets with a higher frequency hopping rate. Punnoose *et al.* [123] conducted real testbeds experiments for the interference analysis of Bluetooth and IEEE 802.11b Direct Sequence Spread Spectrum (DSSS) systems. They discovered that IEEE 802.11b throughput rapidly degrades in the presence of co-channel interference. In contrast, the Bluetooth throughput degrades when the IEEE 802.11b interfering signal is strong enough. They mutually adversely affect each other. Shirsat *et al.* [124] made the same discovery with the other studies that Bluetooth packet transmissions lead to co-channel interference with WLANs and ZigBee, and degrade their performances. However, co-channel interference can be mitigated by changing the modulation scheme, adjusting the packet size and selecting collision-free channels.

Mourad *et al.* [125] performed a co-channel interference analysis regarding Bluetooth and WLAN coexisting in an automobile environment. They discovered that music streaming and hands-free calling can be greatly affected in the presence of WLANs. On the other hand, the WLAN throughput is slightly affected by the Bluetooth applications. The reasons are threefold. Firstly, all the devices are placed in a small region and the distance between each device is very short. Secondly, the path loss between different cars is relatively low, causing co-channel interference between cars. Thirdly, due to

TABLE VI
SUMMARY OF THE ADAPTIVE AND NON-ADAPTIVE SOLUTIONS FOR BLUETOOTH AND WLANS

Solutions	Solution domain	Power Consumption	Scalability	Control	Testbeds	Latency	Triggering methods
Golmie in AFH [119]	Frequency	Low	Medium	Centralized	OPNET Simulation	Low	BER, Packet Loss, Frame error rate
Golmie in BIAS [119]	Frequency	Low	Medium	Centralized	OPNET Simulation	Medium	BER, Packet Loss, Frame error rate
Hsu in [103]	Frequency	Low	High	Centralized	Theory and simulation	Low	Average PER
So in [101]	Frequency	Low	High	Centralized	Simulation	Medium	PER
Lee in [108]	Frequency	High	High	Centralized	Theory and Simulation	Low	PER
Lee in [102]	Frequency	Low	Low	Centralized	Simulation	Low	PER
Taher in [105]	Frequency	Low	Low	Centralized	MATLAB Simulations	Low	BER, packet loss, frame error rate
Kwok in [104]	Frequency and Time	Low	High	Centralized	OPNET Simulation	Medium	BER, packet loss, frame error rate
Sun in [107]	Frequency	High	Medium	Centralized	NS-3 Simulation	Medium	BER
Shao in [106]	Time	Low	High	Distributed	Theory and Simulation	Low	PER
Hsu in [110]	Time	Medium	Medium	Centralized	Simulations	Low	PER
Hsu [111]	Time	Medium	Medium	Centralized	Simulation	Low	PER
Howitt in [109]	Time	Medium	Medium	Centralized	Theory	Low	Collision probability
Li in [118]	Time	Low	High	Centralized	Testbeds	Low	SNR

TABLE VII
ADVANTAGES AND DRAWBACKS OF THE ADAPTIVE AND NON-ADAPTIVE SOLUTIONS FOR BLUETOOTH AND WLANS

Solutions	Advantages	Drawbacks
AFH of Golmie in [119]	Suitable for the interference-persistent environment.	Cannot quickly respond to a changing environment. Lead to additional packet losses due to frequent channel estimate
BIAS of Golmie in [119]	Suitable for the frequent changing environment	Might cause a high delay in the interference-persistent environment
Hsu in [103]	Can mitigate co-channel interference by adjusting the hop set and packet size	Might need to modify the Bluetooth standard and Shrinking the hop set cause more interference to IEEE 802.15.4 devices
So in [101]	Effective in mitigating co-channel interference in a dynamical manner	Might increase the Bluetooth delay
Lee in [108]	Effective in mitigating co-channel interference	Need to modify the Bluetooth standard to add carrier sensing that could cost more energy
Lee in [102]	Effective in mitigating co-channel interference	Might not be useful in a dense WLAN environment
Taher [105]	Can quickly detect WiFi channels to adjust the hop set	Might not be useful in a dense WLAN environment
ISOAFH of Kwok in [104]	Suitable for interference-persistent environment.	Cannot quickly respond to a changing environment Might cause additional packet losses due to frequent channel estimation
ISOMDMS of Kwok [104]	Suitable for a frequent changing environment	Could cause a high delay if the interference is persistent
Shao in [106]	Effective in mitigating co-channel interference caused by dense WLANs in a distributed manner	Might increase the Bluetooth delay
Sun in [107]	Can mitigate both inter and intra-network interference caused by Bluetooth piconets and WLANs	Need to modify the Bluetooth standard to support the coordination
Hsu in [110]	Effective in mitigating co-channel interference using packet fragmentation	Fragmentation might increase the system overhead.
Hsu in [111]	Effective in mitigating co-channel interference using packet fragmentation	Fragmentation might increase the system overhead and numbers of re-transmissions.
Howitt in [109]	Effective in mitigating co-channel interference using packet fragmentation	Fragmentation might increase the system overhead and numbers of re-transmissions
Li in [118]	Effective in mitigating co-channel interference using dual-channel transmissions	Need to modify the Bluetooth standard if the dual-channel transmissions are supported

the car mobility, Bluetooth devices in one car could be easily affected by bursty WLAN traffic in another, which makes the Bluetooth AFH scheme less effective. Liu *et al.* [126] employed a Software-Defined Radio (SDR) platform to evaluate the WLAN performance degradation caused by Bluetooth co-channel interference. A series of real-world experiments are conducted to validate the platform. The WLAN throughput, signal strength and jitter are emulated using the platform. Howitt [127] made a three-fold conclusion from the WLAN's perspective. Firstly, the WLAN network is less likely to be adversely affected by the light Bluetooth traffic; secondly, the WLAN network can be severely affected by a moderate or high level of Bluetooth traffic; thirdly, if the WLAN wishes to avoid all the Bluetooth interference, the coverage of the WLAN must be reduced by 50%.

Howitt [128] also conducted experiments from the Bluetooth network's point of view. The Bluetooth network is heavily impacted by the light WLAN traffic although the WLAN transmission range is relatively large. Conversely, the Bluetooth network will be adversely impacted by the heavy

WLAN traffic. The degree of the impact on the Bluetooth network depends on its path loss with the RF environment and the QoS requirement of the application. Golmie *et al.* [129] drew several key conclusions regarding co-channel interference. On one hand, the WLAN power control technique has limited benefits in preventing the WLAN from being impacted by Bluetooth. For example, increasing the WLAN transmission power 50 times as much as the Bluetooth network cannot decrease the WLAN packet loss rate. On the other hand, decreasing the WLAN transmit power could mitigate the co-channel interference caused by the Bluetooth network. It was also found that the Bluetooth voice traffic can be most detrimental to the WLAN and that the WLAN network performance deteriorates very quickly as the Bluetooth network throughput increases.

4) Analytical Models: Apart from the simulation and testbed analysis, a few studies have formulated the co-channel interference between Bluetooth and WLANs. Ashraf *et al.* [130], [131] proposed a *p*-persistent mathematical model based on the CSMA/CA protocol of WLANs. More precisely, the model formulates the transmission success probability of a WLAN packet in the presence of interference caused by both WLANs and Bluetooth piconets. The model can also be derived using WLAN and Bluetooth offered loads, their packet lengths, the number of interfering Bluetooth piconets. Nawaz and Sun [132] derived a Minimum Mean Squared Error (MMSE) algorithm to estimate the channel status in the physical layer of IEEE 802.11g networks. In particular, the Non-linear Least Square (NLS) and polynomial smoothing schemes were employed for non-coincident and coincident interference cancellation. Stranne *et al.* [133] proposed an analytical closed-form framework evaluating the performance of interfering Packet Radio Networks (PRNs) in terms of the WLAN and Bluetooth throughputs. To present a fine-grained analysis of co-channel interference, an example system comprised of one WLAN and multiple Bluetooth piconets is employed to derive the Cumulative Distribution Functions (CDF) of received interfering energy from the interferers. The CDFs are used to further calculate the WLAN and Bluetooth throughout as a function of the number of Bluetooth interferers. The closed-form framework provides a powerful tool in understanding the machination of co-channel interference. Howitt *et al.* [134] conducted an empirical study on the interoperability between IEEE 802.11 networks and Bluetooth. The authors focused on evaluating the co-channel and adjacent channel interference power of Bluetooth and IEEE 802.11b, which is required by packet retransmissions. The authors derived an analytical model of jamming suppression that has a good agreement with the empirical model. Conti *et al.* [135] derived an analytical model that can evaluate the co-channel interference between Bluetooth and IEEE 802.11b networks in terms of the PER in a Rice/Rayleigh fading channel with Additive White Gaussian Noise (AWGN). The coexistence system factors in propagation impairments, thermal noise, interference, modulation schemes, frequency hopping, packet formats and traffic loads. The analytical model is verified by simulations and can be easily implemented in other simulators.

C. Collaborative Solutions

In the collaborative scheme, similar to Section IV-B, the Bluetooth interface and the WLAN interface adopt a time division approach. In other words, the Bluetooth interface and the WLAN interface on the same device transmit packets at different time slots to avoid mutual interference. Under this category, Xhafa *et al.* [136] found out that the collaborative method proposed by the IEEE 802.15.2 special task group has "Avalanche Effects" that significantly decreases the WLAN throughput. This is because the WLAN interface will perform the CSMA/CA algorithm to detect the channel before sending a data packet. Whenever there is a transmission failure, the WLAN interface decreases the transmission rate, so the period for transmitting the same packet will be prolonged, thus resulting in fewer packets transmitted in the same time duration. To solve this issue, the same authors [137] proposed that the WLAN AP should buffer the packets and poll the other WLAN stations. If one WLAN station determines that packet buffered at the AP is addressed for it, it sends an ACK packet to the AP that in turn transmits the packet to the station without any channel contention from the other WLAN stations. As a result, the chance of colliding with the Bluetooth interface is reduced. Han *et al.* [17] discovered that the WLAN back-off time duration is long enough to successfully transmit a Bluetooth packet, so the Bluetooth packets should be transmitted while the WLAN interface is backing off. As for the other periods when the WLAN interface is not backing off, the Bluetooth should use AFH [24] to mitigate the interference. Overall, there are not many studies focusing on the collaborative scheme due to the lack of heterogeneous devices residing on one physical unit, but with the rise of the IoT, the number of such physical units is expected to grow, thus leading to severe co-channel interference that degrades the network performance.

VI. Discussion and Analysis

After presenting the coexistence and interference mitigation between IEEE 802.15.4 networks and WLANs, and between Bluetooth and WLANs, we found that WLANs are susceptible to Bluetooth adverse impacts but can exert detrimental effects on IEEE 802.15.4 networks. This is because Bluetooth is a narrow band jammer that "cuts" the WLAN frequency using the frequency hopping technique, so the WLAN throughput can be heavily affected by Bluetooth. WLANs have much stronger transmit power and a much shorter back-off interval that enables WLANs to seize the channel earlier than IEEE 802.15.4 networks, so once the channel has been occupied by WLANs, IEEE 802.15.4 networks have fewer chances to seize the channel and transmit packets.

IEEE 802.15.4 networks behave quite differently from Bluetooth in the presence of WLAN interference. More precisely, since IEEE 802.15.4 networks and WLANs both adopt the CSMA/CA mechanisms (two different algorithms but with similar names) to perform channel sensing and collision avoidance, it is possible to characterize the channel access using the MC model in the presence of co-channel interference. In contrast, due to the difficulty of modelling the Bluetooth frequency hopping technique, it is nearly impossible to derive an

analytical model for a Bluetooth-WLAN coexistence scenario. This is why much fewer studies have presented analytical models to mimic the co-channel interference caused by Bluetooth and WLANs than that caused by IEEE 802.15.4 networks and WLANs. IEEE 802.15.4 and WLAN coexistence can be modelled by adding an interference state in the MC to model the interference state, as shown in the previous section.

In terms of the adaptive and non-adaptive solutions, the majority of studies focused on the very straightforward way—channel switching to tackle co-channel interference. It is understandable that shifting to an idle or less affected channel could improve the system performance, but it is rather difficult to do so when co-locating with dense WLANs. This is because three WLAN using channel 1, 6, 11 almost cover the whole 2.4 GHz free band, leaving very limited space for IEEE 802.15.4 networks and Bluetooth to shifting channels. Therefore, the centralized methods of switching to a free channel might not be feasible in dense WLANs, and thus the distributed methods are more suitable for dense network scenarios as each node can adaptively adjust their policy as per the level of interference around themselves. In addition, one single interference mitigation solution might not be effective on a large scale, so the combination of different solutions as presented in the previous sections could achieve better performance gains when dealing with dense network scenarios. Among all these solutions, the ones proposed to solve the co-channel interference within one single heterogeneous network are not fully explored by scholars. This is because at the infancy of Bluetooth, IEEE 802.15.4 networks and WLANs, there are not many gateways equipped with two heterogeneous radio interfaces. However, with the rising of the IoT, the number of gateways is expected to increase, and the co-channel interference caused by the gateways would become worse, so it is imperative that the research emphasis be shifted from mitigating co-channel interference caused by separate WPANs and WLANs to that caused by heterogeneous wireless networks comprised by WPANs and WLANs under saturated network conditions.

Apart from the studies discussing the coexistence between IEEE 802.15.4 networks and WLANs, and coexistence between Bluetooth and WLANs, a few studies conducted the performance measurements of the adverse impacts on the three networks. Garroppo *et al.* [138] investigated the reciprocal impacts among IEEE 802.15.4 networks, Bluetooth and WLANs. The results confirm the previous conclusions and found out that IEEE 802.15.4 networks and Bluetooth can harmoniously co-locate in the same region with little interference. This could be explained in a way that unlike WLANs, both ZigBee and Bluetooth have relatively narrow bandwidths. Although Bluetooth uses the FH technique, the chance of having an overlapping channel between the two networks is slim. Penna *et al.* [139] performed energy measurements on IEEE 802.15.4 networks in the presence of WLAN and Bluetooth co-channel interference. The study also confirms that Bluetooth does not adversely impact IEEE 802.15.4 networks heavily in terms of channel capacity. Shin *et al.* [140], [141] analyzed the ZigBee PER in the presence of Bluetooth and WLANs using OPNET simulations. The simulation study found that when ZigBee, Bluetooth and WLANs coexist, the dominant interferer for ZigBee is WLANs. The distance between ZigBee and Bluetooth needs to be larger than 5.7 m, and the distance between ZigBee and WLANs needs to be larger than 8.65 m. This means although ZigBee and Bluetooth in theory do not interfere with each other, they cannot be placed at a very close range due to co-channel interference.

VII. Open Research Trends and Challenges

The root cause of the co-channel interference is the overlapping of spectrum resources, so a straightforward approach is to tackle the overlapping of spectrum resources in four domains: frequency, time, space and transmit power. All the current interference mitigation solutions fall within these four categories. One the future research trend is to combine different solutions from these domains to achieve a better performance in mitigating co-channel interference. This has been achieved in [64] to reduce the chance of co-channel interference. In one or two domains, mathematical optimization methods such as Voronoi Tessellation and the Graph Theory can be used to further enhance the system performance and make the most of the frequency white space to avoid spectrum sharing [64]. Another recent trend, as described in [67], [68], [106], is to use Physical Layer solutions such as channel coding or a specialized hardware system to recover the corrupted packets. The probabilistic CSMA/CA mechanism [64], [101] also plays an important part in avoiding the interference by tuning the CSMA/CA mechanism as per the Packet Error Rate. Despite consuming more energy as opposed to the traditional solutions, they have showed good performances in improving the PER and BER of the system. The third rising trend is to use Deep-Learning and Reinforcement-Learning based approaches to detecting and mitigating co-channel interference. The Deep-Learning-based approach [142], motivated by the study in [143], uses a Deep Neural Network (DNN) to predict the interfered channels by measuring the RSS values. The method includes two stages: an offline training stage and an online testing stage, as shown in Fig. 17. At the offline training stage, WiFi RSS fingerprints are input to the DNN and trained. The trained model predicts the strongest three channels. At the online stage, the trained model is used to predict the congested channel using real-time RSS datasets. After these two stages, WiFi is switched to a less affected channel to operate. The rationale is that the DNN approach can quickly detect RSS variation in a real-time manner, while other methods such as the Hidden Markov Chain (HMM) models and Support Vector Machine (SVM) cannot due to the low learning capacities and inability to adjust to RSS fluctuation [144], [145]. Moy and Besson [146] proposed a Reinforcement-Learning-based algorithm deployed on the IoT devices sharing ISM bands. The authors formulated the interference mitigation process as a Multi-Armed Bandit problem, which is a closed loop process and implemented using ACK packets for maximizing its packet delivery rate, i.e., maximizing its cumulated reward. Still, there remain many challenges to be solved in the future.

1) The existing interference mitigation solutions generally do not consider the distance between the transmitter

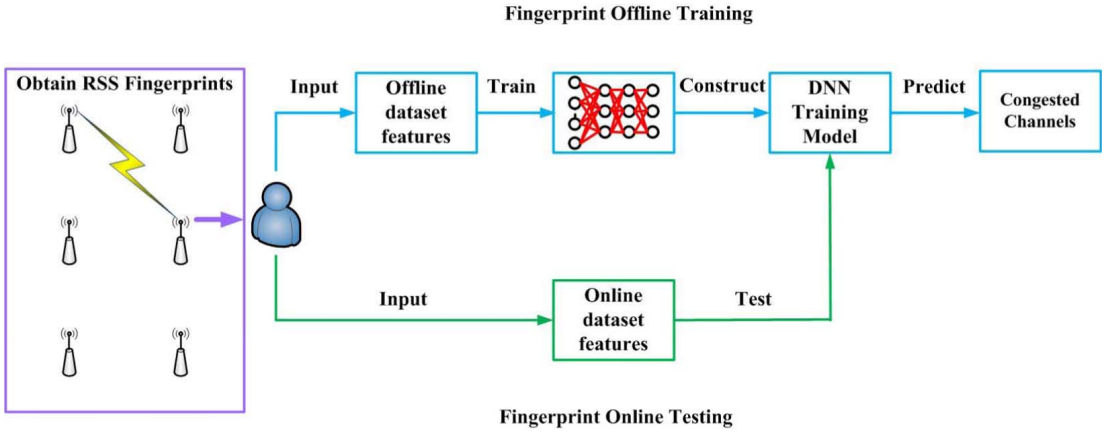


Fig. 17. Structure of the Deep-Learning-based channel selection approach [142].

and the interferer. This is because co-channel interference impacts on the transmitters in different ways. If the transmitter is close to the interferer, the transmitter cannot send packets due to interference. On the other hand, if the transmitter is far from the interferer, the packets from the transmitter will collide with the packets from the interferer. It is imperative that the mitigation solutions be designed as per the interference distance. A typical example is the study in [58], which divides the interference between IEEE 802.11 and IEEE 802.15.4 into three cases based on distinct ranges.

2) The existing solutions do not differentiate the uplink and downlink into account. In WPANs, regardless of IEEE 802.15.4 devices or Bluetooth, there are two types of nodes: control nodes (the PAN coordinator and the master node in Bluetooth) and ordinary nodes (end devices and slave nodes in Bluetooth). The uplink is defined as the packet transmissions from the ordinary nodes to the control nodes, while the downlink is defined as the packet transmissions from the control nodes to the ordinary nodes. The volume of traffic for uplink and downlink is asymmetric: the uplink has more traffic than that of the downlink. The control nodes have more traffic than the ordinary nodes due to traffic accumulation, so the control nodes need more protection due to its high throughput, especially for the case in which they are used as cluster heads.
3) Considering the correlation between coexistence and network parameters, it is difficult to formulate a generalized analytical model based on different settings and topologies, especially for the coexistence between Bluetooth and WLANs due to the frequency hopping technique. In addition, the existing studies only compare the simulation model with the experimental model to show the impact of the interference in terms of the throughput and packet reception rate degradation and rarely consider using the cross layer parameters to mitigate co-channel interference.
4) The current interference mitigation solutions do not distinguish one hop and multi-hop WPAN coexisting with WPANs. The majority of the studies focus on interference mitigation on one-hop network (star topology) due to the easiness of formulating the analytical model using the Markov Chain Model. However, most real-world scenarios of WPANs cover quite a large-scale geographical area using multi-hop networks, and it is rather difficult to formulate an analytical model describing the interference scenario due to the multiple buffers used in the path of a multi-hop WPAN.
5) The separated networks such as IEEE 802.15.4 networks, Bluetooth and WLANs can co-locate with a heterogeneous network made up of an IEEE 802.15.4 network and a WLAN or comprised of a Bluetooth network and a WLAN in the same indoor setting, so the co-channel interference would become more severe and complex. As a result, this requires deploying distributive methods to the key nodes such as ZigBee coordinators and hybrid gateways. Apart from inter-network (between different networks) co-channel interference, intra-network (within the same network) co-channel interference should also be considered when designing solutions.

VIII. Conclusion

In this paper, we presented a comprehensive review and in-depth analysis of coexistence and interference mitigation between WPANs and WLANs. Before introducing the coexistence scenario, we briefly described the key components of the IoT, especially the communications technologies of the three transmission layers. The differences between IEEE 802.15.4 and IEEE 802.11 networks were compared in detail, and the root causes of co-channel interference and solutions were analyzed and summarized. Next, we moved to the coexistence and interference mitigation between Bluetooth and WLANs and gave a thorough analysis on the coexistence and interference mitigation between Bluetooth and WLANs, and the solutions were also analyzed and summarized. We found that IEEE 802.15.4 networks are more likely to be adversely impacted by WLANs due to WLAN's high transmit power and high data rate, whereas WLANs are more susceptible to Bluetooth owing to the frequency hopping technique. Lastly, the remaining issues and challenges were highlighted.

Apart from the current solutions, the techniques combining strategies from the frequency, time, space and transmit power domains are much needed, which are simple, light, distributed and manageable for heterogeneous wireless technologies coexisting in the IoT era. Deep-Learning and Reinforcement-Learning-based methods are expected to become the mainstream solutions in the indoor environment such as Smart Cities and Smart Homes because they can easily deal with random RSS fluctuation as opposed to other methods.

ACKNOWLEDGMENT

The authors would like to thank the Editor-in-Chief and anonymous reviewers who spent a valuable amount of time providing comments and improving the paper. The authors also would like to thank Dr. Deyou Zhang from KTH and Dr. Yulei Wu from the University of Exeter, U.K., for their constructive suggestions.

REFERENCES

[1] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Generat. Comput. Syst.*, vol. 29, no. 7, pp. 1645–1660, 2013.

[2] S. Li, L. Xu, and S. Zhao, "The Internet of Things: A survey," *Inf. Syst. Frontiers*, vol. 17, no. 2, pp. 243–259, 2015.

[3] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Comput. Netw.*, vol. 54, no. 15, pp. 2787–2805, Oct. 2010.

[4] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A survey on enabling technologies, protocols, and applications," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2347–2376, 4th Quart., 2015.

[5] A. Whitmore, A. Agarwal, and L. Da Xu, "The Internet of Things—A survey of topics and trends," *Inf. Syst. Frontiers*, vol. 17, no. 2, pp. 261–274, 2015.

[6] S. Li, L. Da Xu, and S. Zhao, "5G Internet of Things: A survey," *J. Ind. Inf. Integr.*, vol. 10, pp. 1–9, Jun. 2018.

[7] H. Arasteh *et al.*, "Iot-based smart cities: A survey," in *Proc. IEEE 16th Int. Conf. Environ. Electr. Eng. (EEEIC)*, Florence, Italy, Jun. 2016, pp. 1–6.

[8] H. Farhangi, "The path of the smart grid," *IEEE Power Energy Mag.*, vol. 8, no. 1, pp. 18–28, Jan./Feb. 2010.

[9] C. Anton-Haro and M. Dohler, *Machine-to-Machine (M2M) Communications: Architecture, Performance and Applications*. Amsterdam, The Netherlands: Elsevier, 2014.

[10] R. Etkin, A. Parekh, and D. Tse, "Spectrum sharing for unlicensed bands," *IEEE J. Sel. Areas Commun.*, vol. 25, no. 3, pp. 517–528, Apr. 2007.

[11] P. Yi, A. Iwayemi, and C. Zhou, "Developing ZigBee deployment guideline under WiFi interference for smart grid applications," *IEEE Trans. Smart Grid*, vol. 2, no. 1, pp. 110–120, Mar. 2011.

[12] M. Rihan, M. El-Khamy, and M. El-Sharkawy, "On ZigBee coexistence in the ISM band: Measurements and simulations," in *Proc. Int. Conf. Wireless Commun. Underground Confined Areas*, Ferrand, France, Aug. 2012, pp. 1–6.

[13] J. W. Chong, H. Y. Hwang, C. Y. Jung, and D. K. Sung, "Analysis of throughput in a ZigBee network under the presence of WLAN interference," in *Proc. Int. Symp. Commun. Inf. Technol.*, Sydney, NSW, Australia, Oct. 2007, pp. 1166–1170.

[14] S. Y. Shin, "Throughput analysis of IEEE 802.15.4 network under IEEE 802.11 network interference," *AEU-Int. J. Electron. Commun.*, vol. 67, no. 8, pp. 686–689, 2013.

[15] S. Pollin *et al.*, "Performance analysis of slotted carrier sense IEEE 802.15.4 medium access layer," *IEEE Trans. Wireless Commun.*, vol. 7, no. 9, pp. 3359–3371, Sep. 2008.

[16] X. Zhang and K. G. Shin, "Enabling coexistence of heterogeneous wireless systems: Case for ZigBee and WiFi," in *Proc. 12th ACM Int. Symp. Mobile Ad Hoc Netw. Comput.*, New York, NY, USA, 2011, pp. 1–11.

[17] J. Han, C. Joo, and S. Bahk, "Resource sharing in dual-stack devices: Opportunistic Bluetooth transmissions in WLAN busy periods," *IEEE Trans. Mobile Comput.*, vol. 17, no. 10, pp. 2396–2407, Oct. 2018.

[18] D. Yang, Y. Xu, and M. Gidlund, "Coexistence of IEEE802.15.4 based networks: A survey," in *Proc. 36th Annu. Conf. IEEE Ind. Electron. Soc.*, Glendale, AZ, USA, Nov. 2010, pp. 2107–2113.

[19] M. R. Saranya and R. Pugazendi, "A survey on co-existence mechanisms in WLAN and WPAN devices," *Int. J. Adv. Res. Comput. Eng. Technol.*, vol. 3, no. 9, pp. 2967–2972, 2014.

[20] T. Hayajneh, G. Almashaqbeh, S. Ullah, and A. V. Vasilakos, "A survey of wireless technologies coexistence in WBAN: Analysis and open research issues," *Wireless Netw.*, vol. 20, no. 8, pp. 2165–2199, 2014.

[21] S. Movassaghi, M. Abolhasan, J. Lipman, D. Smith, and A. Jamalipour, "Wireless body area networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1658–1686, 3rd Quart., 2014.

[22] E. Ferro and F. Potorti, "Bluetooth and Wi-Fi wireless protocols: A survey and a comparison," *IEEE Wireless Commun.*, vol. 12, no. 1, pp. 12–26, Feb. 2005.

[23] S. Bluetooth, "Bluetooth core specification, Part B: Baseband specification, version 1.0" Bluetooth Special Interest Group, Kirkland, WA, USA, Tech. Rep., 2003, p. 47.

[24] N. Golmie, N. Chevrollier, and O. Rebala, "Bluetooth and WLAN coexistence: Challenges and solutions," *IEEE Wireless Commun.*, vol. 10, no. 6, pp. 22–29, Dec. 2003.

[25] B. Latré, B. Braem, I. Moerman, C. Blondia, and P. Demeester, "A survey on wireless body area networks," *J. Wireless Netw.*, vol. 17, no. 1, pp. 1–18, 2011.

[26] G. Naik, J. Liu, and J.-M. Park, "Coexistence of wireless technologies in the 5 GHz bands: A survey of existing solutions and a roadmap for future research," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 3, pp. 1777–1798, 3rd Quart., 2018.

[27] J. Kim, J. Lee, J. Kim, and J. Yun, "M2M service platforms: Survey, issues, and enabling technologies," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 1, pp. 61–76, 1st Quart., 2014.

[28] M. Z. Shafiq, L. Ji, A. X. Liu, J. Pang, and J. Wang, "A first look at cellular machine-to-machine traffic: Large scale measurement and characterization," *ACM SIGMETRICS Perform. Eval. Rev.*, vol. 40, no. 1, pp. 65–76, 2012.

[29] E. Borgia, "The Internet of Things vision: Key features, applications and open issues," *Comput. Commun.*, vol. 54, pp. 1–31, Dec. 2014.

[30] R. Want, "An introduction to RFID technology," *IEEE Pervasive Comput.*, vol. 5, no. 1, pp. 25–33, Jan./Mar. 2006.

[31] R. Want, "Near field communication," *IEEE Pervas. Comput.*, vol. 10, no. 3, pp. 4–7, Jul./Sep. 2011.

[32] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: A survey," *Comput. Netw.*, vol. 38, no. 4, pp. 393–422, 2002.

[33] N. Golmie, *Coexistence Wireless Networks: Challenges System-Level Solutions Unlicensed Bands*. Cambridge, U.K.: Cambridge Univ. Press, 2006.

[34] M. Centenaro, L. Vangelista, A. Zanella, and M. Zorzi, "Long-range communications in unlicensed bands: The rising stars in the IoT and smart city scenarios," *IEEE Wireless Commun.*, vol. 23, no. 5, pp. 60–67, Oct. 2016.

[35] D. Law, D. Dove, J. D'Ambrosia, M. Hajduczenia, M. Laubach, and S. Carlson, "Evolution of Ethernet standards in the IEEE 802.3 working group," *IEEE Commun. Mag.*, vol. 51, no. 8, pp. 88–96, Aug. 2013.

[36] V. C. Gungor *et al.*, "Smart grid technologies: Communication technologies and standards," *IEEE Trans. Ind. Informat.*, vol. 7, no. 4, pp. 529–539, Nov. 2011.

[37] J. Mitola, "Cognitive radio architecture," in *Cooperation in Wireless Networks: Principles and Applications*. Berlin, Germany: Springer, 2006, pp. 243–311.

[38] L. Pelusi, A. Passarella, and M. Conti, "Opportunistic networking: Data forwarding in disconnected mobile ad hoc networks," *IEEE Commun. Mag.*, vol. 44, no. 11, pp. 134–141, Nov. 2006.

[39] W. Zhiliang, Y. Yi, W. Lu, and W. Wei, "A SOA based IOT communication middleware," in *Proc. Int. Conf. Mechatronic Sci., Electr. Eng. Comput. (MEC)*, Aug. 2011, pp. 2555–2558.

[40] L. Wang and R. Ranjan, "Processing distributed Internet of Things data in clouds," *IEEE Cloud Comput.*, vol. 2, no. 1, pp. 76–80, Feb. 2015.

[41] K. Mekki, E. Bajic, F. Chaxel, and F. Meyer, "Overview of cellular LPWAN technologies for IoT deployment: Sigfox, LoRaWAN, and NB-IoT," in *Proc. IEEE Int. Conf. Pervas. Comput. Commun. Workshops (PerCom Workshops)*, Athens, Greece, Mar. 2018, pp. 197–202.

[42] D. Chen, J. Y. Khan, J. Brown, M. Awais Javed, and Y. Zhuang, "A 6LoWPAN OPNET simulation model for machine-to-machine communications," *Trans. Emerg. Telecommun. Technol.*, vol. 31, no. 11, p. e4120, 2020.

[43] P. Davidson and R. Piché, "A survey of selected indoor positioning methods for smartphones," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 2, pp. 1347–1370, 2nd Quart., 2016.

[44] D. L. Strayer *et al.*, "Visual and cognitive demands of CarPlay, Android auto, and five native infotainment systems," *Hum. Factors: J. Hum. Factors Ergonom. Soc.*, vol. 61, no. 8, pp. 1371–1386, Dec. 2019.

[45] A. Mourad, M. O. Al Kalaa, H. Refai, and P. A. Hoeher, "IEEE 802.11 systems in the automotive domain: Challenges and solutions," in *Proc. 3rd Int. Conf. Vehicle Technol. Intell. Transp. Syst.*, vol. 2, Jun. 2017, pp. 41–51.

[46] M. Conti, F. Delmastro, G. Minutiello, and R. Paris, "Experimenting opportunistic networks with WiFi direct," in *Proc. IFIP Wireless Days (WD)*, Valencia, Spain, Nov. 2013, pp. 1–6.

[47] L. S. Committee *et al.*, *IEEE Standard for Information Technology Telecommunications and Information Exchange Between Systems Local and Metropolitan Area Networks Specific Requirements. Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs)*, IEEE Standard 802, 2006.

[48] D. Chen, J. Brown, and J. Y. Khan, "6LoWPAN based neighborhood area network for a smart grid communication infrastructure," in *Proc. 5th Int. Conf. Ubiquitous Future Netw. (ICUFN)*, Da Nang, Vietnam, Jul. 2013, pp. 576–581.

[49] I. C. S. L. M. S. Committee *et al.*, *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, ANSI/IEEE Standard 802.11-1999, 1999.

[50] *IEEE Standard for Information Technology-Telecommunications and Information Exchange Between Systems-Local and Metropolitan Area Networks Specific Requirements Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs)*, IEEE Standard 802.15. 4-2003, 2003.

[51] W. Yuan, "Coexistence of IEEE 802.11 b/g WLANs and IEEE 802.15. 4 WSNs: Modeling and protocol enhancements," Ph.D. dissertation, Dept. Telecommun., Delft Univ. Technol., Delft, The Netherlands, 2011.

[52] M. Petrova, J. Riihijarvi, P. Mahonen, and S. Labella, "Performance study of IEEE 802.15.4 using measurements and simulations," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Las Vegas, NV, USA, vol. 1, Apr. 2006, pp. 487–492.

[53] Y. Tang, Z. Wang, D. Makrakis, and H. T. Mouftah, "Interference aware adaptive clear channel assessment for improving ZigBee packet transmission under Wi-Fi interference," in *Proc. IEEE Int. Conf. Sens., Commun. Netw. (SECON)*, New Orleans, LA, USA, Jun. 2013, pp. 336–343.

[54] B. H. Jung, J. W. Chong, C. Y. Jung, S. M. Kim, and D. K. Sung, "Interference mediation for coexistence of WLAN and ZigBee networks," in *Proc. IEEE 19th Int. Symp. Pers., Indoor Mobile Radio Commun.*, Cannes, France, Sep. 2008, pp. 1–5.

[55] B. Jung *et al.*, "Ubiquitous wearable computer (UWC)-aided coexistence algorithm in an overlaid network environment of WLAN and ZigBee networks," in *Proc. 2nd Int. Symp. Wireless Pervas. Comput.*, San Juan, PR, USA, 2007.

[56] Z. Wang, T. Du, Y. Tang, D. Makrakis, and H. T. Mouftah, "ACK with interference detection technique for ZigBee network under Wi-Fi interference," in *Proc. 8th Int. Conf. Broadband Wireless Comput., Commun. Appl.*, Compiegne, France, Oct. 2013, pp. 128–135.

[57] N. Torabi, K. Rostamzadeh, and V. C. Leung, "IEEE 802.15.4 beaconing strategy and the coexistence problem in ISM band," *IEEE Trans. Smart Grid*, vol. 6, no. 3, pp. 1463–1472, May 2015.

[58] W. Yuan, J.-P. M. Linnartz, and I. G. Niemegeers, "Adaptive CCA for IEEE 802.15.4 wireless sensor networks to mitigate interference," in *Proc. IEEE Wireless Commun. Netw. Conf.*, Sydney, NSW, Australia, Apr. 2010, pp. 1–5.

[59] E. D. N. Ndih and S. Cherkaoui, "Adaptive 802.15.4 backoff procedure to survive coexistence with 802.11 in extreme conditions," in *Proc. 13th IEEE Annu. Consum. Commun. Netw. Conf. (CCNC)*, Las Vegas, NV, USA, Jan. 2016, pp. 556–561.

[60] K. Hong, S. Lee, and K. Lee, "Performance improvement in ZigBee-based home networks with coexisting WLANs," *Pervas. Mobile Comput.*, vol. 19, pp. 156–166, May 2015.

[61] G. M. Tamilselvan and A. Shanmugam, "Multi hopping effect of zigbee nodes coexisting with WLAN nodes in heterogeneous network environment," in *Proc. 1st UK-India Int. Workshop Cognit. Wireless Syst. (UKIWCWS)*, Delhi, India, Dec. 2009, pp. 1–6.

[62] M. Kang, J. Chong, H. Hyun, S. Kim, B. Jung, and D. Sung, "Adaptive interference-aware multi-channel clustering algorithm in a ZigBee network in the presence of WLAN interference," in *Proc. 2nd Int. Symp. Wireless Pervas. Comput.*, San Juan, PR, USA, 2007.

[63] L. Tytgat, O. Yaron, S. Pollin, I. Moerman, and P. Demeester, "Analysis and experimental verification of frequency-based interference avoidance mechanisms in IEEE 802.15.4," *IEEE/ACM Trans. Netw.*, vol. 23, no. 2, pp. 369–382, Apr. 2015.

[64] F. Li, J. Luo, G. Shi, and Y. He, "ART: Adaptive frequency-temporal co-existing of ZigBee and WiFi," *IEEE Trans. Mobile Comput.*, vol. 16, no. 3, pp. 662–674, Mar. 2017.

[65] J. Ock, Y.-J. Choi, and S. Bahk, "Performance analysis of periodic busy tones protecting a ZigBee network from Wi-Fi interruption," in *Proc. IEEE 79th Veh. Technol. Conf. (VTC Spring)*, Seoul, South Korea, May 2014, pp. 1–5.

[66] S. Lim, S. Lee, J. Yoo, and C.-K. Kim, "NBP: Light-weight narrow band protection for ZigBee and Wi-Fi coexistence," *EURASIP J. Wireless Commun. Netw.*, vol. 2013, no. 1, p. 76, Dec. 2013.

[67] J. Kim, W. Jeon, K.-J. Park, and J. P. Choi, "Coexistence of full-duplex-based IEEE 802.15.4 and IEEE 802.11," *IEEE Trans. Ind. Informat.*, vol. 14, no. 12, pp. 5389–5399, Dec. 2018.

[68] R. Chen and W. Gao, "Enabling cross-technology coexistence for extremely weak wireless devices," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, Paris, France, Apr. 2019, pp. 253–261.

[69] C.-J.-M. Liang, N. B. Priyantha, J. Liu, and A. Terzis, "Surviving Wi-Fi interference in low power ZigBee networks," in *Proc. 8th ACM Conf. Embedded Networked Sensor Syst. (SenSys)*, 2010, pp. 309–322.

[70] Y. Yan *et al.*, "WizBee: Wise ZigBee coexistence via interference cancellation with single antenna," *IEEE Trans. Mobile Comput.*, vol. 14, no. 12, pp. 2590–2603, Dec. 2014.

[71] H.-C. Yang, D. Zhang, X. Kong, and H. Jia, "Performance analysis of cognitive transmission in dual-cell environment and its application to smart meter communications," in *Proc. 7th Int. Conf. Broadband, Wireless Comput., Commun. Appl.*, Victoria, BC, Canada, Nov. 2012, pp. 40–45.

[72] K. Lee, C. B. Chae, T. K. Sung, and J. Kang, "Cognitive beamforming based smart metering for coexistence with wireless local area networks," *J. Commun. Netw.*, vol. 14, no. 6, pp. 619–628, Dec. 2012.

[73] A. Sikora and V. F. Groza, "Coexistence of IEEE802.15.4 with other systems in the 2.4 GHz-ISM-band," in *Proc. IEEE Instrum. Meas. Technol. Conf.*, Ottawa, ON, Canada, vol. 3, May 2005, pp. 1786–1791.

[74] R. Verma, "Assessing coexistence of IEEE 802.15. 4 networks and IEEE 802.11 b/g/n networks-a study of interference effects," Ph.D. dissertation, Elect. Comput. Eng., IOWA State Univ., Ames, IA, USA, 2019.

[75] D. G. Yoon, S. Y. Shin, W. H. Kwon, and H. S. Park, "Packet error rate analysis of IEEE 802.11b under IEEE 802.15.4 interference," in *Proc. IEEE 63rd Veh. Technol. Conf.*, Melbourne, VIC, Australia, vol. 3, May 2006, pp. 1186–1190.

[76] A. Lavric, V. Popa, I. Finis, A.-M. Gaitan, and A.-I. Petrariu, "Packet error rate analysis of IEEE 802.15.4 under 802.11g and Bluetooth interferences," in *Proc. 9th Int. Conf. Commun. (COMM)*, Bucharest, Romania, Jun. 2012, pp. 259–262.

[77] G. Yang and Y. Yu, "ZigBee networks performance under WLAN 802.11b/g interference," in *Proc. 4th Int. Symp. Wireless Pervasive Comput.*, Melbourne, VIC, Australia, Feb. 2009, pp. 1–4.

[78] Y. Tao, X.-Y. Li, and C. Bo, "Performance of coexisted WiFi and ZigBee networks," in *Proc. IEEE 33rd Int. Conf. Distrib. Comput. Syst. Workshops*, Philadelphia, PA, USA, Jul. 2013, pp. 315–320.

[79] I. Howitt and J. A. Gutierrez, "IEEE 802.15.4 low rate–wireless personal area network coexistence issues," in *Proc. IEEE Wireless Commun. Netw. (WCNC)*, New Orleans, LA, USA, vol. 3, Mar. 2003, pp. 1481–1486.

[80] S. Pollin, I. Tan, B. Hodge, C. Chun, and A. Bahai, "Harmful coexistence between 802.15.4 and 802.11: A measurement-based study," in *Proc. 3rd Int. Conf. Cognit. Radio Oriented Wireless Netw. Commun. (CrownCom)*, Singapore, May 2008, pp. 1–6.

[81] B. Zhen, H.-B. Li, S. Hara, and R. Kohno, "Energy based carrier sensing in integrated medical environments," in *Proc. IEEE Int. Conf. Commun.*, Beijing, China, 2008, pp. 3110–3114.

[82] P. Luong, T. M. Nguyen, and L. B. Le, "Throughput analysis and design for coexisting WLAN and ZigBee network," in *Proc. IEEE 80th Veh. Technol. Conf. (VTC-Fall)*, Vancouver, BC, Canada, Sep. 2014, pp. 1–5.

[83] N. C. Tas, C. Sastry, and Z. Song, "IEEE 802.15. 4 throughput analysis under IEEE 802.11 interference," in *Proc. Int. Symp. Innov. Real Time Appl. Distrib. Sensor Netw.*, 2007, pp. 1–8.

[84] J.-S. Han, J.-S. Bang, and Y.-H. Lee, "Transmission performance of wireless sensor networks in the presence of co-channel interference," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Istanbul, Turkey, Apr. 2014, pp. 1956–1961.

[85] W. Zhang, M. A. Suresh, Y. Zhou, R. S. Veera, and R. Stoleru, "On the coexistence of 802.11 and 802.15.4 networks with delay constraints," in *Proc. IEEE 34th Int. Perform. Comput. Commun. Conf. (IPCCC)*, Nanjing, China, Dec. 2015, pp. 1–8.

[86] A. El-Keyi, H. U. Sokun, T. N. Nguyen, Q. Ye, H. J. Zhu, and H. Yanikomeroglu, "A novel probabilistic path loss model for simulating coexistence between 802.11 and 802.15.4 networks in smart home environments," in *Proc. IEEE 28th Annu. Int. Symp. Pers., Indoor, Mobile Radio Commun. (PIMRC)*, Montreal, QC, Canada, Oct. 2017, pp. 1–5.

[87] Y. Jeong, J. Kim, and S.-J. Han, "Interference mitigation in wireless sensor networks using dual heterogeneous radios," *Wireless Netw.*, vol. 17, no. 7, p. 1699, 2011.

[88] M. L. Huang and S.-C. Park, "A WLAN and ZigBee coexistence mechanism for wearable health monitoring system," in *Proc. 9th Int. Symp. Commun. Inf. Technol.*, Seoul, South Korea, Sep. 2009, pp. 555–559.

[89] A. Koubaa and M. Alves, "A two-tiered architecture for real-time communications in large-scale wireless sensor networks: Research challenges," in *17th Euromicro Conf. Real-Time Syst.*, Palma de Mallorca, Spain, 2005.

[90] J. Leal, A. Cunha, M. Alves, and A. Koubaa, "On a IEEE 802.15.4/ZigBee to IEEE 802.11 gateway for the ART-WiSe architecture," in *Proc. IEEE Conf. Emerg. Technol. Factory Automat. (EFTA)*, Patras, Greece, Sep. 2007, pp. 1388–1391.

[91] Q. Li, D. Han, O. Gnawali, P. Sommer, and B. Kusy, "Twonet: Large-scale wireless sensor network testbed with dual-radio nodes," in *Proc. 11th ACM Conf. Embedded Networked Sensor Syst.*, New York, NY, USA, 2013, pp. 1–2.

[92] M. Ha, S. H. Kim, H. Kim, K. Kwon, N. Giang, and D. Kim, "SNAIL gateway: Dual-mode wireless access points for WiFi and IP-based wireless sensor networks in the Internet of Things," in *Proc. IEEE Consum. Commun. Netw. Conf. (CCNC)*, Las Vegas, NV, USA, Jan. 2012, pp. 169–173.

[93] H. Y. Tung, K. F. Tsang, H. C. Tung, V. Rakocevic, K. T. Chui, and Y. W. Leung, "A WiFi-ZigBee building area network design of high traffics AMI for smart grid," *Smart Grid Renew. Energy*, vol. 3, no. 4, p. 10, 2012.

[94] J. Wang and V. C. M. Leung, "Comparisons of home area network connection alternatives for multifamily dwelling units," in *Proc. 4th IFIP Int. Conf. New Technol., Mobility Secur.*, Paris, France, Feb. 2011, pp. 1–5.

[95] P. L. Shrestha, M. Hempel, Y. Qian, H. Sharif, J. Punwani, and M. Stewart, "Performance modeling of a multi-tier multi-hop hybrid sensor network protocol," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Shanghai, China, Apr. 2013, pp. 2345–2350.

[96] D. Chen, J. Khan, M. A. Javed, and J. Brown, "Interference mitigation techniques for a dense heterogeneous area network in machine-to-machine communications," *Trans. Emerg. Telecommun. Technol.*, vol. 30, no. 12, p. e3763, 2019.

[97] J. Lansford, A. Stephens, and R. Nevo, "Wi-Fi (802.11b) and Bluetooth: Enabling coexistence," *IEEE Netw.*, vol. 15, no. 5, pp. 20–27, Sep./Oct. 2001.

[98] N. Golmie and F. Mouveaux, "Interference in the 2.4 GHz ISM band: Impact on the Bluetooth access control performance," in *Proc. IEEE Int. Conf. Commun. Conf. Rec. (ICC)*, Helsinki, Finland, vol. 8, Jun. 2001, pp. 2540–2545.

[99] *IEEE Recommended Pract. for Inf. technology– Local Metrop. area networks– Specific requirements– Part 15.2: Coexistence Wireless Pers. Area Netw. With Other Wireless Devices Operating Unlicensed Freq. Bands*, IEEE Standard, Aug. 2003.

[100] N. Golmie, "Bluetooth dynamic scheduling and interference mitigation," *Mobile Netw. Appl.*, vol. 9, no. 1, pp. 21–31, 2004.

[101] J. So and Y. Kim, "Interference-aware frequency hopping for Bluetooth in crowded wi-fi networks," *Electron. Lett.*, vol. 52, no. 17, pp. 1503–1505, 2016.

[102] S.-H. Lee and Y.-H. Lee, "Adaptive frequency hopping for Bluetooth robust to WLAN interference," *IEEE Commun. Lett.*, vol. 13, no. 9, pp. 628–630, Sep. 2009.

[103] A. C.-C. Hsu, D. S. L. Wei, C.-C.-J. Kuo, N. Shiratori, and C.-J. Chang, "Enhanced adaptive frequency hopping for wireless personal area networks in a coexistence environment," in *Proc. IEEE Global Telecommun. Conf. (GLOBECOM)*, Washington, DC, USA, Nov. 2007, pp. 668–672.

[104] Y.-K. Kwok and M.-H. Chek, "Design and evaluation of coexistence mechanisms for Bluetooth and IEEE 802.11b systems," *Proc. IEEE 15th Int. Symp. Pers., Indoor Mobile Radio Commun.*, Barcelona, Spain, vol. 3, Sep. 2004, pp. 1767–1771.

[105] T. M. Taher, K. Rele, and D. Roberson, "Development and quantitative analysis of an adaptive scheme for Bluetooth and Wi-Fi co-existence," in *Proc. 6th IEEE Consum. Commun. Netw. Conf.*, Las Vegas, NV, USA, Jan. 2009, pp. 1–2.

[106] C. Shao, H. Roh, and W. Lee, "BuSAR: Bluetooth slot availability randomization for better coexistence with dense Wi-Fi networks," *IEEE Trans. Mobile Comput.*, vol. 20, no. 3, pp. 846–860, Mar. 2021.

[107] W. Sun *et al.*, "BlueCoDE: Bluetooth coordination in dense environment for better coexistence," in *Proc. IEEE 25th Int. Conf. Netw. Protocols (ICNP)*, Toronto, ON, Canada, Oct. 2017, pp. 1–10.

[108] S.-H. Lee, H.-S. Kim, and Y.-H. Lee, "Mitigation of co-channel interference in Bluetooth piconets," *IEEE Trans. Wireless Commun.*, vol. 11, no. 4, pp. 1249–1254, Feb. 2012.

[109] I. Howitt and F. Awad, "Optimizing IEEE 802.11b packet fragmentation in collocated Bluetooth interference," *IEEE Trans. Commun.*, vol. 53, no. 6, pp. 936–938, Jun. 2005.

[110] A. C.-C. Hsu, D. S. L. Wei, and C.-C.-J. Kuo, "Coexistence Wi-Fi MAC design for mitigating interference caused by collocated Bluetooth," *IEEE Trans. Comput.*, vol. 64, no. 2, pp. 342–352, Feb. 2015.

[111] A. Hsu, D. Wei, and C.-C. Kuo, "Coexistence mechanism using dynamic fragmentation for interference mitigation between Wi-Fi Bluetooth," in *Proc. MILCOM*, Washington, DC, USA, Oct. 2006, pp. 1–7.

[112] C. F. Chiasserini and R. R. Rao, "Coexistence mechanisms for interference mitigation between IEEE 802.11 WLANs and Bluetooth," in *Proc. 21st Annu. Joint Conf. IEEE Comput. Commun. Societies*, New York, NY, USA, vol. 2, Jun. 2002, pp. 590–598.

[113] C. F. Chiasserini and R. R. Rao, "Coexistence mechanisms for interference mitigation in the 2.4-GHz ISM band," *IEEE Trans. Wireless Commun.*, vol. 2, no. 5, pp. 964–975, Sep. 2003.

[114] N. Golmie and N. Chevrollier, "Techniques to improve Bluetooth performance in interference environments," in *Proc. Commun. Netw.-Centric Oper.: Creating Inf. Force (MILCOM)*, McLean, VA, USA, vol. 1, Oct. 2001, pp. 581–585.

[115] C. D. M. Cordeiro, S. Abhyankar, R. Toshiwal, and D. P. Agrawal, "A novel architecture and coexistence method to provide global access to/from Bluetooth WPANs by IEEE 802.11 WLANs," in *Proc. Conf. IEEE Int.*, Phoenix, AZ, USA, Apr. 2003, pp. 23–30.

[116] C. de Morais Cordeiro, D. Sadok, and D. P. Agrawal, "Piconet interference modeling and performance evaluation of Bluetooth MAC protocol," in *Proc. IEEE Global Telecommun. Conf. (GLOBECOM)*, San Antonio, TX, USA, vol. 5, Nov. 2001, pp. 2870–2874.

[117] C. de M Cordeiro and D. P. Agrawal, "Employing dynamic segmentation for effective co-located coexistence between Bluetooth and IEEE 802.11 WLANs," in *Proc. Global Telecommun. Conf. (GLOBECOM)*, vol. 1, Nov. 2002, pp. 195–200.

[118] J. Li and X. Liu, "A frequency diversity technique for interference mitigation in coexisting Bluetooth and WLAN," in *Proc. IEEE Int. Conf. Commun.*, Glasgow, U.K., Jun. 2007, pp. 5490–5495.

[119] N. Golmie, O. Rebala, and N. Chevrollier, "Bluetooth adaptive frequency hopping and scheduling," in *Proc. Mil. Commun. Conf. (MILCOM)*, Boston, MA, USA, vol. 2, Oct. 2003, pp. 1138–1142.

[120] I. Howitt and A. Shukla, "Coexistence empirical study and analytical model for low-rate WPAN and IEEE 802.11b," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Las Vegas, NV, USA, Mar.Apr. 2008, pp. 900–905.

[121] K. Matheus, "Bluetooth radio network performance: Measurement results and simulation models," in *Proc. Int. Workshop Wireless Ad-Hoc Netw.*, Oulu, Finland, 2004, pp. 228–232.

[122] L. Cabral and R. D. Lins, "An analysis of the QoS in the transmission in 802.11g networks in the presence of Bluetooth interference," in *Proc. 5th Int. Conf. Wireless Mobile Commun.*, Cannes/La Bocca, France, Aug. 2009, pp. 76–81.

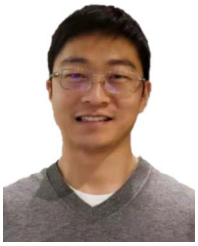
[123] R. J. Punnoose, R. S. Tseng, and D. D. Stancil, "Experimental results for interference between Bluetooth and IEEE 802.11b DSSS systems," in *Proc. IEEE 54th Veh. Technol. Conf. (VTC Fall)*, Atlantic City, NJ, USA, Fall, vol. 1, Oct. 2001, pp. 67–71.

[124] A. S. Shirsat, S. A. Shirsat, and D. M. Yadav, "Performance of Bluetooth in the presence of 802.11b," in *Proc. Int. Conf. Adv. Commun. Comput. Technol. (ICACCT)*, Montreal, QC, Canada, Feb. 2018, pp. 117–121.

[125] A. Mourad, S. Muhammad, M. O. Al Kalaa, P. A. Hoeher, and H. Refai, "Bluetooth and IEEE 802.11n system coexistence in the automotive domain," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, San Francisco, CA, USA, Mar. 2017, pp. 1–6.
[126] W. Liu *et al.*, "Assessing the coexistence of heterogeneous wireless technologies with an SDR-based signal emulator: A case study of Wi-Fi and Bluetooth," *IEEE Trans. Wireless Commun.*, vol. 16, no. 3, pp. 1755–1766, Mar. 2017.
[127] I. Howitt, "WLAN and WPAN coexistence in UL band," *IEEE Trans. Veh. Technol.*, vol. 50, no. 4, pp. 1114–1124, Jul. 2001.
[128] I. Howitt, "Bluetooth performance in the presence of 802.11b WLAN," *IEEE Trans. Veh. Technol.*, vol. 51, no. 6, pp. 1640–1651, Nov. 2002.
[129] N. Golmie, R. E. Van Dyck, A. Soltanian, A. Tonnerre, and O. Rebala, "Interference evaluation of Bluetooth and IEEE 802.11B systems," *Wireless Netw.*, vol. 9, no. 3, pp. 201–211, 2003.
[130] I. Ashraf, K. Voulgaris, A. Gkelias, M. Dohler, and A. H. Aghvami, "Impact of interfering Bluetooth piconets on a collocated *p*-persistent CSMA-based WLAN," *IEEE Trans. Veh. Technol.*, vol. 58, no. 9, pp. 4962–4975, Nov. 2009.
[131] I. Ashraf, A. Gkelias, K. Voulgaris, M. Dohler, and A. H. Aghvami, "Co-existence of CSMA/CA and Bluetooth," in *Proc. IEEE Int. Conf. Commun.*, Istanbul, Turkey, vol. 12, 2006, pp. 5522–5527.
[132] R. Nawaz and S. Sun, "Bluetooth interference mitigation in 802.11g," *Proc. IEEE Int. Conf. Commun.*, Berlin, Germany, May 2008, pp. 930–935.
[133] A. Stranne, O. Edfors, and B. A. Molin, "Energy-based interference analysis of heterogeneous packet radio networks," *IEEE Trans. Commun.*, vol. 54, no. 7, pp. 1299–1309, Jul. 2006.
[134] I. Howitt, V. Mitter, and J. Gutierrez, "Empirical study for IEEE 802.11 and Bluetooth interoperability," in *Proc. IEEE VTS 53rd Veh. Technol. Conf. (Spring)*, Rhodes, Greece, vol. 2, May 2001, pp. 1109–1113.
[135] A. Conti, D. Dardari, G. Pasolini, and O. Andrisano, "Bluetooth and IEEE 802.11b coexistence: Analytical performance evaluation in fading channels," *IEEE J. Sel. Areas Commun.*, vol. 21, no. 2, pp. 259–269, Feb. 2003.
[136] A. E. Xhafa, X. Lu, and D. P. Shaver, "Coexistence of collocated IEEE 802.11 and Bluetooth technologies in 2.4 GHz ISM band," in *Proc. AccessNets*. Berlin, Germany: Springer, 2008, pp. 138–145.
[137] A. E. Xhafa and Y. Sun, "Mechanisms for coexistence of collocated WLAN and Bluetooth in the same device," in *Proc. Int. Conf. Comput., Netw. Commun. (ICNC)*, San Diego, CA, USA, Jan. 2013, pp. 905–910.
[138] R. G. Garroppo, L. Gazzarrini, S. Giordano, and L. Tavanti, "Experimental assessment of the coexistence of Wi-Fi, ZigBee, and Bluetooth devices," in *Proc. IEEE Int. Symp. World Wireless, Mobile Multimedia Netw.*, Lucca, Italy, Jun. 2011, pp. 1–9.
[139] F. Penna, C. Pastrone, M. A. Spirito, and R. Garello, "Measurement-based analysis of spectrum sensing in adaptive WSNs under Wi-Fi and Bluetooth interference," in *Proc. IEEE 69th Veh. Technol. Conf.*, Barcelona, Spain, Apr. 2009, pp. 1–5.
[140] S. Y. Shin, J. S. Kang, and H. S. Park, "Packet error rate analysis of ZigBee under interferences of multiple Bluetooth piconets," in *Proc. IEEE 69th Veh. Technol. Conf. (VTC Spring)*, Barcelona, Spain, Apr. 2009, pp. 1–5.
[141] S. Y. Shin, H. S. Park, S. Choi, and W. H. Kwon, "Packet error rate analysis of ZigBee under WLAN and Bluetooth interferences," *IEEE Trans. Wireless Commun.*, vol. 6, no. 8, pp. 2825–2830, Aug. 2007.
[142] L. Yen, A. B. Adege, H.-P. Lin, C.-H. Ho, and K. Lever, "Deep learning approach on channel selection strategy for minimizing co-channel interference in unlicensed channels," *Microelectron. Rel.*, vol. 105, Feb. 2020, Art. no. 113558.
[143] O. Omotere, J. Fuller, L. Qian, and Z. Han, "Spectrum occupancy prediction in coexisting wireless systems using deep learning," in *Proc. IEEE 88th Veh. Technol. Conf. (VTC-Fall)*, Chicago, IL, USA, Aug. 2018, pp. 1–7.
[144] A. Saad, H. F. Schepker, B. Staehle, and R. Knorr, "Whitespace prediction using hidden Markov model based maximum likelihood classification," in *Proc. IEEE 89th Veh. Technol. Conf. (VTC-Spring)*, Kuala Lumpur, Malaysia, Apr. 2019, pp. 1–7.
[145] J.-Y. Lee, C. Eom, Y. Kwak, H.-G. Kang, and C. Lee, "Dnn-based wireless positioning in an outdoor environment," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, Calgary, AB, Canada, Apr. 2018, pp. 3799–3803.
[146] C. Moy and L. Besson, "Decentralized spectrum learning for IoT wireless networks collision mitigation," in *Proc. 15th Int. Conf. Distrib. Comput. Sensor Syst. (DCOSS)*, Santorini, Greece, May 2019, pp. 644–651.

Dong Chen (Member, IEEE) received the Ph.D. degree in computer engineering from the University of Newcastle, Australia, in 2019. He is currently working as a Postdoctoral Researcher with the State Key Laboratory of Information Engineering in Surveying, Mapping and Remote Sensing, Wuhan University, China. His research interests include indoor positioning, wireless sensor networks, vehicular networks, and machine learning.

Yuan Zhuang (Member, IEEE) received the Ph.D. degree in geomatics engineering from the University of Calgary, Canada, in 2015. He is a Professor with the State Key Laboratory of Information Engineering in Surveying, Mapping and Remote Sensing, Wuhan University, China. To date, he has coauthored over 80 academic papers and 18 patents and has received over ten academic awards. His current research interests include multi-sensors integration, real-time location systems, wireless positioning, the Internet of Things (IoT), and machine learning for navigation applications. He is an Editorial Board Member of *Satellite Navigation* and IEEE ACCESS, a Guest Editor of the IEEE INTERNET OF THINGS JOURNAL, and a Reviewer of over 15 IEEE journals.



Jianzhu Huai (Member, IEEE) received the Ph.D. degree in geodetic engineering from The Ohio State University, USA, in 2017, for the work on collaborative mapping by using camera and/or IMU data collected from smartphones. The Android and iOS apps for data acquisition, MARS logger, has been open sourced. Then, he worked 2.5 years at the Autonomous Personal Robot Group, Segway Robotics, where he developed localization, mapping, and calibration programs for sensor modalities, including wheel encoder, camera, IMU, and lidar. He is a Postdoctoral Researcher with the State Key Laboratory of Surveying, Mapping and Remote Sensing, Wuhan University, China. One of his completed open-source projects has extended the camera-IMU calibration package kalibr to deal with rolling shutter effect and noise identification. As a member of the Institute of Navigation (ION) since 2015, he has been investigating problems in state estimation, area mapping, and sensor calibration, aiming at cost-effective automation systems.

Xiao Sun received the bachelor's and master's degrees from the School of Geodesy and Geomatics (SGG), Wuhan University, in 2017 and 2020, respectively. He is pursuing the Ph.D. degree with the State Key Laboratory of Information Engineering in Surveying, Mapping and Remote Sensing (LIESMARS), Wuhan University. His current research mainly focuses on visible light positioning, high precision GNSS positioning, and seamless positioning.

Xiansheng Yang received the master's degree in computer science and engineering from Hunan University of Science and Technology, Xiangtan, China. He is currently pursuing the Ph.D. degree with the State Key Laboratory of Surveying, Mapping and Remote Sensing, Wuhan University, China. His research interests include deep learning, machine learning, data mining, and indoor positioning.

Muhammad Awais Javed (Senior Member, IEEE) received the B.Sc. degree in electrical engineering from the University of Engineering and Technology Lahore, Pakistan, in August 2008, and the Ph.D. degree in electrical engineering from the University of Newcastle, Australia, in February 2015. From July 2015 to June 2016, he worked as a Postdoctoral Research Scientist at Qatar Mobility Innovations Center (QMIC) on SafeITS Project. He is currently working as an Assistant Professor at COMSATS University Islamabad, Pakistan. His research interests include intelligent transport systems, vehicular networks, protocol design for emerging wireless technologies, and the Internet of Things.

Jason Brown received the B.Eng. and Ph.D. degrees from the University of Manchester Institute of Science and Technology (UMIST) in 1990 and 1994, respectively. He then worked in research and development and operational roles for Vodafone, AT&T, and LG Electronics. In 2011, he joined the University of Newcastle, Australia, researching smart grid and M2M communications technologies. Since 2018, he has been a Lecturer at the University of Southern Queensland. His main research interest areas are the IoT, wireless sensor networks, UAV networks, and machine learning.

Zhengguo Sheng (Senior Member, IEEE) received the B.Sc. degree from the University of Electronic Science and Technology of China, Chengdu, China, in 2006, and the M.S. and Ph.D. degrees from Imperial College London, London, U.K., in 2007 and 2011, respectively. He was with UBC, Vancouver, BC, Canada, as a Research Associate, and with Orange Labs, Santa Monica, CA, USA, as a Senior Researcher. He is currently a Senior Lecturer with the University of Sussex, Brighton, U.K. He has more than 100 publications. His research interests cover the IoT, vehicular communications, and cloud/edge computing.

John Thompson (Fellow, IEEE) currently holds a position of the Personal Chair in Signal Processing and Communications with The University of Edinburgh, U.K. He currently leads the European Marie Curie Training Network ADVANTAGE which trains 13 Ph.D. students in smart grids. His main research interests are in wireless communications, sensor signal processing, and energy efficient communications networks and smart grids. He has published around 300 papers in these topics and was recognised by Thomson Reuters as a Highly Cited Researcher in 2015 and 2016. He is currently an Editor of the Green Series of *IEEE Communications Magazine* and an Associate Editor of IEEE TRANSACTIONS ON GREEN COMMUNICATIONS AND NETWORKS. He was a Distinguished Lecturer on Green Topics for ComSoc from 2014 to 2015.