EPRI | ELECTRIC POWER RESEARCH INSTITUTE

Optimizing Wireless Spectrum

Operation and Coexistence in Sub-1GHz Unlicensed Spectrum

3002013392

Optimizing Wireless Spectrum

Operation and Coexistence in Sub-1GHz Unlicensed Spectrum

3002013392

Technical Update, December 2018

EPRI Project Manager
T. Godfrey

ELECTRIC POWER RESEARCH INSTITUTE
3420 Hillview Avenue, Palo Alto, California 94304-1338 ▪ PO Box 10412, Palo Alto, California 94303-0813 ▪ USA
00.313.3774 ▪ 650.855.2121 ▪ askepri@epri.com ▪ www.epri.com

DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITIES

This is an EPRI Technical Update report. A Technical Update report is intended as an informal report of continuing research, a meeting, or a topical study. It is not a final EPRI technical report.

NOTE

For further information about EPRI, call the EPRI Customer Assistance Center at 800.313.3774 or e-mail askepri@epri.com.

ACKNOWLEDGMENTS

The Electric Power Research Institute (EPRI) prepared this report.

Principal Investigators
K. Oleksak
T. Godfrey
M. Billings

This report describes research sponsored by EPRI.

This publication is a corporate document that should be cited in the literature in the following manner:

Optimizing Wireless Spectrum: Operation and Coexistence in Sub-1GHz Unlicensed Spectrum. EPRI, Palo Alto, CA: 2018. 3002013392.

ABSTRACT

An evaluation of primary unlicensed frequency bands for utility applications in the sub-1GHz range has been conducted. Wireless device occupants and transmission protocols were investigated to understand future design considerations for coexisting networks and communication standards. Issues related to scalability, interference, and spectrum availability are outlined along with current developments for methods of resolution. The 802.15.4g with a focus toward Wi-SUN and the 802.11ah standard specifications are addressed in terms of their interference resiliency. Development of an unlicensed spectrum surveyor, measuring spectrum occupants and average channel power, has been expanded upon to include enhanced radio-frequency reception and back-end data analytics storage.

Keywords
802.15.4g
802.11ah
Coexistence
FAN
Resiliency
Wi-SUN

CONTENTS

LIST OF FIGURES

LIST OF TABLES

1
INTRODUCTION

Investigating Unlicensed Spectrum

With the continued growth of wireless devices and the limited availability of dedicated spectrum, the use of unlicensed frequencies provides flexibility and openness for the deployment of new wireless networks. To better assess the availability within unlicensed bands, a survey of active users and their methodologies is being conducted in the sub-1GHz bands. With the knowledge of current spectrum occupants and protocols, suggestions for operations in the unlicensed bands could alleviate uncoordinated transmission scheduling, which leads to failed transmissions and a lack of coherent and reliable communication. Dependable packet-based information exchange for monitoring, managing, and controlling electric grid systems demands cooperation of wireless transmissions within local area network (LAN) and wide area network (WAN) utility configurations. Such coordination is already problematic because there are no one-size-fits-all communication devices; however, much progress has been made to adopt generalized data exchange between various system components. This issue is further compounded with wireless systems physical layer (PHY) variations and a propagation medium's dynamic occupancy—especially when multiple networks are in proximity. This report discusses the causes of such conflicts with regard to existing communication standards that operate in the unlicensed bands. Protocols designed for utility use are expanded upon to help resolve imminent transmission interference.

Coexistence in Unlicensed Spectrum

Overlapping network architectures and multiple communication protocols are key issues to allowing coexistence in the unlicensed frequency bands. The *unlicensed* aspect refers to there being no owner of any frequency in that band. Therefore, interference will be encountered, and both parties must make reasonable attempts to reconcile collisions. It is apparent that many methods for transmission interference and collision resolution can be taken by different devices and manufacturers, so even though the unlicensed bands are meant for equal transmission opportunities, there may be some unbalance as protocols are mixed within a network and geographic proximity. Understanding these methods and their differences is of prime importance to assessing coexistence compatibility. In addition, methods for resolving coexistence issues can be established. A better understanding of basic requirements of unlicensed bands forms the foundation for allowing multiple users to operate in an environment in which interference between stations is managed in an unbiased and equal fashion. Each band has slightly different characteristics, but the main concerns in each band are general. A focus on the 902–928 MHz industrial, scientific, and medical (ISM) band in the United States will provide an adequate assessment that can be extended to other comparable bands in many regions.

2
OPTIMIZING THE SUB-1GHZ ISM BAND

The ISM bands are defined and coordinated by the International Telecommunication Union (ITU). Table 2-1 shows the dedicated spectrum (below 1 GHz) and the regions for which they are defined. A map of the approximate region allocations is shown in Figure 2-1.

Table 2-1
Sub-1GHz ISM Band Allocations

Frequency Range	Region
6.765–6.795 kHz	All
13.553–13.567 kHz	All
26.957–27.283 kHz	All
40.66–40.70 MHz	All
433.05–434.79 MHz	Region 1
902–928 MHz	Region 2

The ISM bands were originally allocated for non-telecommunication uses, such as medical equipment, microwave ovens, and similar heating equipment. Communication devices occupying these bands are designated as low power. Any radio communication services operating within these bands must accept harmful interference from other devices. The frequency range 863–870 MHz is not an ISM allocation chart but is a similar unlicensed band allocated for use in Europe. Many sub-1GHz radios are designed for either 902–920 MHz or 863–870 MHz operation (or both). For example, SigFox and LoRa (discussed later in this report) have commercial devices for various industrial sensors and metering purposes in those bands.

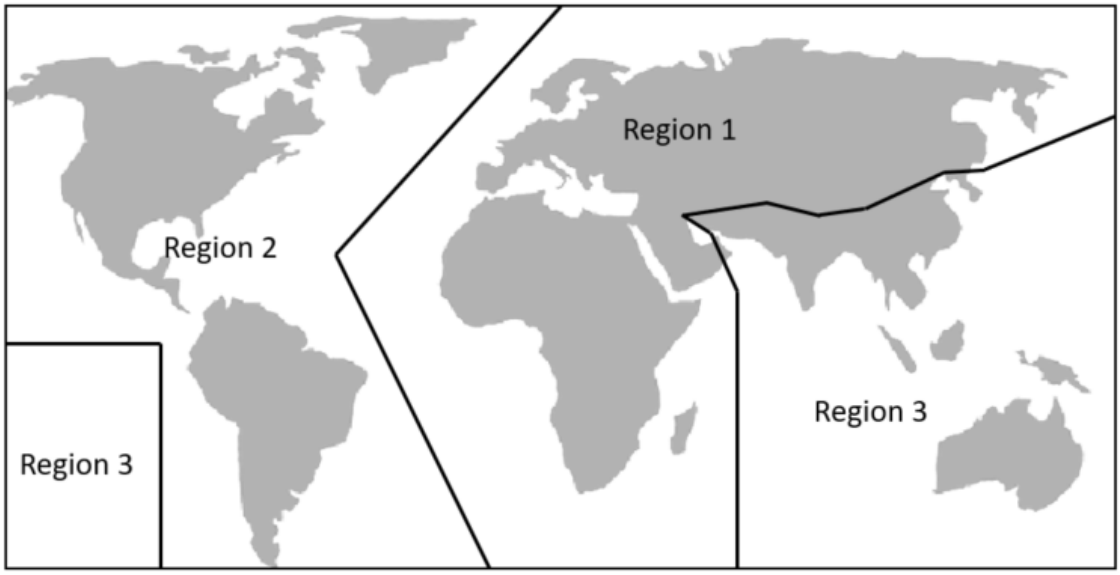

Figure 2-1
ITU Regions

Global Perspective on ISM Bands

Regulations for radiocommunications in the ISM bands are specific to regulatory bodies in each country. Basic operation requirements for the United States and Europe often further restrict the usage of each ISM band based on transmitted power, channel allocations, primary users, and other technical requirements.

U.S. ISM

Radio-frequency (RF) devices for unlicensed operation in the United States according to Title 47 of the Code of Federal Regulations (CFR) Parts 15, 18, and 97 are defined by the Federal Communications Commission (FCC). Part 15 outlines the regulations on RF radiation for both intentional and unintentional usage. This allows the operation of devices that meet transmission, reception, and interference requirements that vary by frequency band and application. Bands of interest are the ISM bands described in 47 CFR Part 18, which defines the non-telecommunications uses. In FCC 18.109, the key phrase is "excluding applications in the field of telecommunication" [1]. The Part 18 regulations for ISM devices in the 915 MHz band are shown in Table 2-2 [1]. More technical specifications can be found in 47 CFR §18.301.

Table 2-2
FCC ISM Part 18 Technical Regulations

RF Power Generated	Below 500 W
Field Strength (below 500 W)	25 µV/m (max) @ 300 m (average)
Field Strength (above 500 W) *Not to exceed 10 µV/m at 1600 m	$25 * \sqrt{Generated\ Power/500}$
Measurement Range (field strength)	Lowest frequency up to the 10th harmonic

ISM equipment is defined as RF energy generating devices for industrial, scientific, and domestic purposes **not** including telecommunications applications. To clarify, telecommunications devices operating in an ISM band do not have primary allocation and have different power, field strength, and distance requirements (which will be discussed).

Radio communications specifications are defined in Part 15. These specifications include telecommunications devices that are not specified to be ISM type equipment. There are different regulations for the use of Part 15 devices: Class A is commercial, while Class B is residential. Class A devices include WiFi and Bluetooth commercial products. Devices can be certified by the FCC according to the Part 15 regulations if the device proves it does not cause harmful interference with other devices; however, they may be subject to additional technical specifications depending on the use. Part 15 devices are secondary to ISM devices defined by Part 18. The locations and allowable field strength often provide adequate distances to prevent such interference, but it should be noted which device types have primary occupancy in any band. For 902–928 MHz, primary users are radio navigation services and ISM devices. Table 2-3 shows the allowed field strengths for intentional radiators according to Part 15 [2].

Table 2-3
902–928 MHz Operation

Field Strength	50 mV/m (max) @ 3 m
Field Strength (spurious emissions)	500 µV/m (max) @ 3 m

The allowable duty cycle also changes with frequency band and use. For the 902–928 MHz band, there are no duty cycle limits.

Regulations for devices outside of Class A and B follow additional regulations that restrict time of transmission and usage according to Subparts C and D of Part 15 regulations on radio devices. Such devices include automobile locks, garage door openers, toys, and alarm controls. Periodic transmissions are regulated differently for control signal transmissions: for control signals, no continuous transmissions, voice, video, or toy control is permitted. Transmitters must deactivate after 5 seconds, and scheduled polling or supervision is permitted only for system integrity and safety applications. There are also restrictions on the total time of transmitted data within a given hour, which is not to exceed 2 seconds per hour for an individual transmitter. Data transmissions (not including controls) can exceed the time limitations for periodic transmissions with a lower field strength and maximum bandwidth of 0.5% for transmissions above 900 MHz [3].

Technical Regulations

Specifications for channel operation are defined in 47 CFR §15.245, 15.247, and 15.249. Two techniques defined are frequency-hopping spread spectrum (FHSS) and direct-sequence spread spectrum (DSSS). FHSS shifts carriers across a frequency band in a pseudorandom sequence in which both the sender and the receiver know the channel allocations for the hops. This method helps to avoid collisions by continually changing the transmission channel and naturally mitigates collisions by hopping to the next channel. Devices in the 915 MHz range using frequency hopping and digital modulation are subject to the following restrictions. For digitally modulated signals without frequency hopping, the minimum 6-dB bandwidth is 500 kHz for channel spacing. For frequency-hopping systems, the channel hopping frequency is defined as a minimum of 25 kHz or the 20-dB bandwidth of the channel, whichever is greater. If the 20-dB

bandwidth is less than 250 kHz, at least 50 hopping frequencies must be used with a maximum transmission time of 0.4 seconds in a 20-second interval. The output power for 50 channels is limited to 1 W (30 dBm). Bandwidths greater than 250 kHz will have at least 25 hopping frequencies and transmit for no more than 0.4 seconds in a 10-second interval. The output power is limited to 0.25 W (24 dBm) [4].

Hop scheduling must be made individually by each device, which means that multiple devices cannot coordinate a group of hop schedules. In addition, all channels must have equal average use. Regulations for antenna gains depending on antenna directivity, point-to-point, point-to-multipoint, and omnidirectional radio uses are also outlined. For example, when directional antenna gains exceed 6 dBi, the allowed output power must be reduced by the amount the limit was exceeded [6]. This is a key guideline for point-to-point systems.

DSSS transmissions reduce signal interference by spreading the transmitted signal over a wide band with added noise. The signal is shortened and spread across a wider frequency band and is then multiplexed when received. Spreading the signal's information helps reduce the overall channel interference. Naturally, this method requires that the receiver know the correct pseudonoise (PN) code sequence to multiplex the pieces of the message. Code division multiple access (CDMA) is often used with this technique to allow for frequency reuse and added channel gain. This encodes transmitted messages, resulting in code words—all of which are recognized in a code space by a receiver. Messages can then be transmitted over the same frequency and decoded by reapplying the code word to the message and correcting any errors with a parity check matrix. Transmitted power using DSSS is limited to 1 W (30 dBm) and decreases similarly to FHSS for directional antenna gains of over 6 dBi.

The ISM bands give ISM devices privileged use, but they may not interfere with radio navigation or safety communications. This protects such devices from other unlicensed systems that may cause harmful interference, including Part 15 devices. Furthermore, amateur radio operators (a secondary user) occupy the band but must follow additional guidelines defined by the American Radio Relay League (ARRL) and 47 CFR Part 97. For instance, amateur radio operators can transmit in multiple ISM allocated bands, but their transmission is not protected from interference caused by ISM devices. Within the ISM bands, devices operating according to Part 18 are protected from harmful interference by similar operating devices as well as non-primary users such as amateur radio stations. Protection from harmful interference is not a sufficient claim to own a particular channel. Amateur operators have 1500-W average output restrictions but do not use interference mitigation methods such as FHSS and DSSS. The modulation methods for amateur operators are also much more constricted and generally occur by AM, FM, or continuous wave (CW) emissions. Consideration for third-party operation is necessary, and devices that provide reasonable spectrum-sharing methods such as collision avoidance and appropriate operating power are expected. The same courtesy is required of Part 15 devices and amateur radio operators.

European Sub-1GHz Use

The European band similar to the U.S. 902–928 MHz band is the 863–870 MHz band. Besides the clear decrease in channel bandwidth, there are numerous regulations for intra-band operations, which include restrictions on channel bandwidth, modulation methods, transmitted power, and duty cycle. Although the 863–870 MHz band is not an ISM band, it is widely used.

Even with only 7-MHz bandwidth, it still provides a significant increase of frequency use from the ISM allocated 433.05–434.79 MHz for Region 1. An outline of the allocations is provided in Table 2-4 [5].

Table 2-4
EU 863–870 MHz Band Specifications [5]

Frequency	Power	Access	Channel Spacing	Modulation
863–870	≤25 mW	≤0.1% duty cycle of Listen Before Talk (LBT) and Adaptive Frequency Agility (AFA)	FHSS: ≤100 kHz (47+ channels) DSSS: no spacing N/W: ≤100 kHz for one or more channels; ≤300 kHz modulation bandwidth	FHSS, DSSS, or narrowband/wideband (N/W)
868–868.6	≤25 mW	≤1% duty cycle of LBT and AFA	No spacing	Narrow or wideband
868.7–869.2	≤25 mW	≤0.1% duty cycle of LBT and AFA	No spacing	Narrow or wideband
869.4–869.650	≤500 mW	≤10% duty cycle of LBT and AFA	25 kHz	Narrow or wideband
869.7–870	≤25 mW (no access requirement if ≤5 mW)	1% duty cycle of LBT and AFA	No spacing	Narrow or wideband

Output powers in the EU 863–870 band are considerably smaller than the U.S. 902–928 band and are limited to less than 10% of the maximum 902–928 MHz output power, except for Section g3, which is 50% (500 mW) of the U.S. maximum (1 W). Most of the subchannels are restricted to duty cycles less than 0.1% except for Section g3, which allows for 10% because it is designated as a high-data-speed transmission channel—which can use the entire 250-MHz channel bandwidth. If a device uses a Listen-Before-Talk (LBT) procedure, the duty cycles are not applicable if the device has Adaptive Frequency Agility (AFA), like frequency hopping [5].

The duty cycle limitations of the EU 863–870 MHz band require system engineers to tediously manage wireless assets transmission scheduling. However, because all devices must adhere to the limit, there is generally more available air time in regions without AFA devices.

Additional Global Use

Wi-SUN, built on the 802.15.4g standard, has global members in Europe, India, Japan, North America, South America, and Southeast Asia. Band plans for ISM devices will vary in each of these countries as Figure 2-1 shows. Region 3 countries (Southeast Asia) may depend on ISM bands above 1-GHz such as 2.4–2.5 GHz, 5.725–5.875 GHz, and above 24 GHz in addition to the low-frequency ISM bands that are globally available. Australia also has a similar sub-1GHz spectrum to Region 2; however, the allocations are from 915 to 928 MHz.

Scalability: What Else Is Operating in the 915 Band?

Advanced metering infrastructure (AMI) provides a way for utilities and other industrial sectors to monitor, manage, and control end devices with bi-directional communication. Existing devices using wireless networks differ depending on end use, power consumption, data rate, and transmission range. Gathering data from end users improves a provider's ability to serve consumers, and additional metrics further allow diversity of service to customers. With this comes the need for more devices for sensors, metering, and collection, which results in denser areas of devices competing for the same airwaves. For low-powered, minimal hardware devices, updating protocols and compatibility with new devices entering the market and therefore existing networks is a challenge. The 915 MHz band is allocated from 902 to 928 MHz and is shared among unlicensed Part 15 devices, amateur radio operators, and radiolocation. Surrounding the 915-MHz band are fixed licensed allocations with additional mobile user rights just above the 928-MHz band. *Fixed allocations* means that the channel assignments for in-band operation are predetermined. Considering these surrounding bands and the high cost/demand for spectrum, one should not be hopeful about seeing the 915-MHz band widened.

Low-Powered Devices

ZigBee

ZigBee devices are an example of small-scale and low-power smart devices, which see many applications for sensors, data collection, smart metering, smart homes, and low-data-rate close-range personal networks. They are based on the 802.15.4 wireless protocol, providing mesh, star, and tree network capabilities with the requirement of a central coordinating node. The close-range nature of ZigBee devices allows for a coherent network in a small area; the central server provides the means for out-of-range connections. For many personal networks, the specification will suffice—but for field area network (FAN) applications in which long-range information exchange between utility substations or central management systems is needed, other protocols such as LoRa, SigFox, and Wi-SUN are practical standards. The ZigBee Alliance is working on a JupiterMesh Neighborhood Area Network (NAN) standard to extend device ranges for wider connectivity and coherency by harmonizing with additional standards such as 802.15.4g [6]. This type of implementation has yet to be standardized.

LoRa and SigFox

Long-range low-power specifications such as LoRa or SigFox extend sensor and metering networks into the WANs. Low-power wide area networks (LPWANs) are crucial to the developing Internet of Things (IoT) and can connect non-line-of-sight devices for extended device awareness. Long-range base stations allow LPWAN based on LoRaWAN to minimize the number of base stations needed while still coordinating long-distance events. The conflict with such a network is that its interference range is also extended, posing a significant problem for unlicensed band operations. However, LoRa and SigFox devices have maximum transmissions per day limits. A more detailed comparison of LoRa and SigFox can be found in the *Low-Power Wide Area Networks* technical update [7].

Wi-SUN

Wi-SUN, the wireless smart utility network, is another long-range, low-power protocol targeted for utilities and municipalities with the need for wireless mesh network operations. Wi-SUN is a more refined subset of the 802.15.4g standard designated for low-rate wireless personal area networks (LR-WPANs). The specification of Wi-SUN differs in the physical layer (PHY) and media access control (MAC) descriptions as well as its use for smart meter utility networks and large-scale interoperability. Coherent transmission methods not only ease the complexity of coordinating spectrum sharing for specific use cases, but also allow devices to extend data transfer to more diverse 802.15.4g devices if necessary. As wide area situational awareness develops between regional utility operators, interoperability from what used to be distinct networks will begin to merge. The Wi-SUN architecture is a FAN topology that uses routing between neighbors and aggregation nodes connected to high-capacity core networks [8]. More Wi-SUN Alliance–certified products are beginning to reach the commercial market.

WiFi HaLow

Another emerging protocol is WiFi HaLow, which is described in the IEEE 802.11ah standard. WiFi HaLow also features low-power and long-range operation while offering high data rates depending on the modulation type and channel spacing. A diverse choice of modulation and coding types allows vendors a greater degree of freedom while still maintaining the standards interoperability requirements. The 802.11ah certifications are found in various routers, phone systems, and computer accessories for home and business applications. The standard also supports machine-to-machine (M2M) communications, which allow device coordination independent of a station access point (AP) [9].

Point-to-Multipoint Systems

Unlicensed occupants also include point-to-multipoint (P2MP) networks, which can offer high data rate and long-range capabilities. Base stations managing such networks allow for centralized control and priority access for time-sensitive and critical communications. General Electric's Unlicensed MDS series devices are an example of such currently deployed systems [10]. Legacy systems such as Motorola Canopy for broadband internet access have offered low latency and long-range access points connected to extended network backhauls. Canopy services have also been managed by a centralized node for improved interference mitigation through time synchronization. Point-to-point (P2P) and P2MP networks offer the advantage of highly synchronized and easily coordinated devices. However, the question of scalability for such networks is limited by the geographic location of access points and centralized management systems. On a local scale, such deployment is readily managed—but as WANs spread into adjacent network territory, the practical uses of centralized management systems for a single network decrease because device-to-device interference will not be coherent among varied protocols. As networks and protocols intertwine, devices' predefined abilities to self-manage interference issues will be key to interoperability.

Terrestrial Beacons

Terrestrial beacon systems (TBS) provide non-satellite-based indoor geolocation details and will also occupy the 915-MHz band. Metropolitan beacon system (MBS) by NextNav will be the first of such systems deployed in the United States. Geolocation and timing information from indoor

sources will aim to have similar reliability as outdoor line-of-sight and near-line-of-sight transmission paths. Ensuring that such transmissions are reliable through various mediums requires higher power transmission—and makes interference more likely. Communication system designers will also have to take developments in TBS into account for unlicensed band operations because proximity to such systems may complicate network design in dense areas. It is important to remember that all unlicensed band devices must provide sufficient means to avoid interfering with in-band devices.

Wi-SUN and 802.11ah Coexistence

Protocols that reside in unlicensed bands, such as 802.11ah for sub-1GHz wireless networking and Wi-SUN for utility communications, are the choice topics for an investigation of what must take place to allow for coexistent protocols and networks. Understanding the protocols' specifications and networking methods allows for determining potential issues with reliable transmission and scalability. The interoperability of these protocols within their own designated operation specifications is not explicitly designed to coexist with one another; however, they must provide methods of avoidance of harmful interference to devices operating according to the ISM regulations. 802.11ah is designed to function on low energy consumption among multiple groups of nodes with the demand of high data rates, depending on the chosen modulation. Wi-SUN is also designed for low power with a slightly lower data rate. Although both 802.11ah (WiFi HaLow) and Wi-SUN are targeted for IoT devices and smart home applications, Wi-SUN has a focus on utility usage and smart city operations. 802.11ah is a subset of the 802.11 standards, and Wi-SUN is a subset of 802.15.4g. Both protocols are PHY and MAC standards whose methods directly reflect their ability to coexist. Considerable work has been done by the IEEE 802.15 and 802.19 Working Groups to assess the interoperability of 802.xx devices. Key findings for interference related to the PHY and MAC protocol specifications have been reported by these groups, and steps toward providing operational procedures for 802.xx devices to follow are underway. Current methods for interference mitigation and future problems related to coexistence will be discussed briefly. Results from 802.19 regarding coexistence will also be introduced.

Resiliency: How Protocols Deal with Interference

DSSS and FHSS transmission methods both deal with interference by spreading the spectrum of the transmitted signal. FHSS increases the probability of successful reception by frequency hopping, while DSSS increases reception with redundancy. DSSS also increases the received signals gain through channel coding methods such as CDMA, which additionally filters out unwanted signals that are not in the coding space of the receiver. Digital modulation methods such as OFDM also spread signals in the frequency domain with subcarriers and can provide redundant information, which increases the likelihood of a successful transmission. Alternative methods to simultaneous reception involve preamble patterns and active equalization. If a receiver can read the preamble pattern of a signal it is meant to receive, it can attenuate the unwanted frequency if the signal-to-noise-ratio (SNR) conditions for the receiver are met. Preambles are referred to as *synchronization symbols* and allow receivers to determine incoming information prior to complete transmission. They are a part of the synchronization header (SHR) along with a start-of-frame delimiter (SFD). This method finds uses in receiver selectivity and minimizing power usage by stopping the demodulation of unwanted messages. Information contained in the preamble such as the data length and a cyclic redundancy check (CRC) also help

filter out unwanted transmissions. If more bytes than the protocol expects are received, the CRC check will fail—but this wastes time and energy with demodulation. A method for resolving this is address filtering: if the destination address is not demodulated, the rest of the process is stopped.

For example, the preamble field for an 802.15.4g signal using MR-FSK with two tones has a 2-octet bit pattern while a four-tone signal uses 4 octets [11, 12]. Preambles for 802.11ah vary depending on the channel bandwidth. For 2 MHz, 4 MHz, 8 MHz, and 16 MHz, three groups of two symbols designate the preamble [13]. Although these methods outline readable differences between received signals, the implementation of deciphering different protocols' SHR patterns is an issue to be addressed.

Regarding modulation, 802.15.4g uses MR-FSK, MR-QPSK, and MR-OFDM as PHY layer specifications [12]. All three modes can be used in the 902–928 MHz band. FHSS is the spread spectrum technique for MR-FSK while DSSS is used for MR-QPSK. 802.11ah uses OFDM with many variant subcarriers allowing for diversity. Dynamic modulation and coding schemes allow 802.11ah devices to coordinate and change transmission methods according to current conditions. A tag within the transmitted frame allows for this. 802.11ah also has DSSS specifications defined for the 2.4-GHz band [14]. IEEE Working Group 802.15 released simulation results between 802.15.4g and multiple 802.11 protocols in IEEE 802.15-10-0668-06-004g [15]. Performance was tested with either the 802.11 or 802.15.4g device as the interferer. All three modulation modes of the 802.15.4g standard were tested. Results show that lower data rate transmission methods such as MR-FSK maintained better bit-error-rate (BER) to frame-error-rate (FER) ratios against multiple 802.11 devices [15]. A general trend also showed that 802.11 standards with higher data rates caused more interference at larger distances. These results show the trade-off between mitigating interference and increasing throughput. The results also show the variation in interference and throughput resulting from the choice of protocol implementation. Resolutions to issues of coexistence are what 802.19 aims to present with standards and agreements for future protocol compatibility.

Interference is also dealt with by using carrier-sense multiple access (CSMA). When the PHY layer receives the transmit go-ahead, it first senses the area for other transmissions on the same channel. If another transmission is sensed, a random back-off time is chosen. Until a clear airwave is sensed, the node will continue to adjust the back-off time. Continually adjusting the random back-off time increases the probability of collision. In 802.15.4g, a multi-PHY management (MPM) scheme allows for coexistence of different operating modes on the same channel [15]. Coordinators must scan for a coex-beacon as part of the MPM operation, which forces the coordinator to switch to a different channel or synchronize with the network. Energy detection (ED) channel scanning is also used by coordinating devices to determine a collision-free access channel. Enhanced common signaling mode (CSM) is an added feature of 802.15.4g; it performs sequence detection, which is more accurate than energy detection [16]. Physical layer methods for interference mitigation by 802.11ah include beamforming and multi-input-multi-output (MIMO) for increased throughput of one device. An example of the differences between sensing and back-off times has been shown by IEEE Working Group 802.19 with a comparison of 802.11ah and 802.15.4g.

Work in IEEE 802.19

The IEEE 802.19 Working Group has shown two root issues between the 802.11ah and 802.15.4g standards that determine transmission capabilities in a shared environment. The interference mechanisms from simulations using fixed channels showed that channel collision avoidance (CCA) times and a higher receiver sensitivity resulted in more air time for 802.11ah nodes. 802.11ah has a CCA time of less than 40 µs and a 5-µs CCA to transmission (CCA2TX) turnaround time. 802.15.4g has a CCA time of 128 µs and a 192-µs CCA2TX turnaround time [16]. This causes 802.15.4g packet transmissions to fail as new 802.11ah packets are being transmitted repeatedly during an 802.15.4g back-off time. The issue of a higher receiver threshold for 802.11ah means that 802.15.4g transmissions are not sensed and therefore no CCA mechanism begins. Proposed solutions for back-off methods can be found in Reference [16]. This is just one example of the work being done to allow for future coexistence of 802.xx protocols. Designers can work with and around these problems by adjusting device functionality and specifications. Future standards outside of 802.11ah and 802.15.4g will set the specifications that allow for maximal interoperability.

Scaling Device Density and Throughput

As networks become denser, these coexistence issues become more drastic. Network designers working with the limited bandwidth of the sub-1GHz ISM bands must take frequency reuse, transmitted power, and network topologies into account.

Frequency Reuse

Cellular networks have employed frequency reuse with much success. This has allowed more users within the same frequency band by allocating numerous “cells” that share the same channels but report to a base station so that their transmissions do not interfere with neighbor cells on the same channel. As users become close to the edges of a cell, the base station with the highest received signal level will acquire the call. Increasing the number of users in a small area means adding more base stations and effectively increasing the number of cells to a denser topology. In addition to the geographical separation, transmitters in a cellular network also use automatic power control to transmit the minimum amount needed by the closest base station. This method cuts down on interference between neighbor cells and saves energy by using less power output when a user is close to a base station. Cellular networks have also shown that sectorization of multiple frequencies at a single base station can allow further frequency reuse within a cell using highly directional antennas. This method essentially creates more subcells without adding a base station. Because cellular networks operate in licensed bands, providers strictly manage power control and cell-to-base-station identification to optimize the network. For unlicensed bands, these same techniques can be adopted conceptually but not exactly translated in practice.

FAN Scalability

FANs can implement frequency use because of their mesh topology. Devices on the same network can use the minimum transmit power to reach the next network hop until the message reaches a border router. Similarly, border routers—the gateway outside of a network subnet—can use similar transmit power control methods, which allows them to route messages to an AP through another border router instead of transmitting directly to an AP. This minimizes

interference and allows frequency reuse between separate border routers' subnets. A key feature of Wi-SUN is the mesh FAN topology, which extends the range of a radio far beyond its own transmission capabilities. 802.11ah, which uses a star topology with M2M (machine-to-machine) communication, complicates frequency reuse because device transmissions must be able to reach any node in the network, not just the nearest. Methods for automatic power control can alleviate this problem in 802.11ah by enabling the power management to be active on a device. In addition, the extreme high data rates available in 802.11ah using up to 256 QAM are realizable only in a highly controlled or short-range network. Very minor amplitude changes to a high QAM modulation transmission lead to unsuccessful reception. Lastly, network designers in unlicensed bands have no control over the power control methods or network topology of geographically coexistent networks in contrast to licensed frequency operators. This further supports the need for a specification standard that allows previous standards to integrate.

Proposed Methods of Resiliency

Solutions for future coexistence are based on specification recommendations, which are a subset of the protocols already defined. Device manufacturers and network engineers working toward coexisting devices will need to adopt technical variations of future technologies. The 802.19 IEEE Working Group has already proposed some solutions to the ED threshold and back-off time conflicts explained previously. Considering the higher ED threshold of 802.11ah, an α-Fairness technique based on ED-CCA is suggested [16]. This method defines how an 802.11ah device reports its channel status. If the energy detected is outside the 802.15.4g receiver sensitivity and 802.11ah threshold, the status is reported according to normal 802.11ah standards. If not, the channel status is suggested to be reported based on the α-Fairness technique—a probabilistic report status to give or take more medium access opportunities [16]. With regard to the interference caused by the faster back-off time of 802.11ah, the proposed solution is a Q-Learning method, which uses reinforcement learning to determine the back-off time or channel report status. If the device does not have a back-off instruction, it reports idle; the Q-Learning algorithm then determines whether a transmit or back-off instruction is to be issued. Both methods have been simulated by the 802.19 IEEE Working Group and show small but positive improvements on packet delivery for α-Fairness when the topology is dense with 802.11ah nodes, while the Q-Learning algorithm improves packet delivery with low-density 802.11ah nodes. For packet delays, the 802.15.4g nodes are minimally affected by the proposed algorithms but can delay the 802.11ah back-offs to allow more shared media access with 802.15.4g [16].

The issue of coexistence must be tackled at the design level, and agreed-upon methods of operation will need to be followed to allow fair access in the unlicensed bands. Looking toward scalable solutions, an arbiter of shared mediums that has wide area and multi-protocol awareness may help with coordination, but the complexity of such a shared point may outweigh the benefits. Unlicensed band networks will have control only over their network space, so a coordinator between networks and protocols is unlikely unless an agreement for such a device is standardized and accepted. More realistically, device and network designers will adopt additional specification guidelines or create an adaptable network capable of efficiently coordinating their own devices based on surrounding spectrum activity. An unlicensed spectrum surveyor being developed at EPRI aims to provide spectral informatics of four unlicensed frequency bands.

Occupancy statistics over minutes, hours, days, and weeks stored in a database could assist in coordination and frequency usage for varying geographical regions. Network designers may use this information to set the PHY and MAC specs of current or future assets while allowing a monitoring system to advise device settings as the network changes both internally and externally. An overview of the project and its progress is presented next.

3
UNLICENSED SPECTRUM SURVEYOR PROJECT

Overview

The Unlicensed Spectrum Surveyor development is described in the EPRI Unlicensed Noise Floor Study Report [17]. Using HackRF One radios, spectral scans in the 902–928 MHz, 2.4–2.5 GHz, 3.5–3.7 GHz, and 5.17–5.82 GHz range are uploaded from a client device to an EPRI sftp server as binary files. The scans take place in 1-minute intervals. Once uploaded, another client can download the binary files and have them converted to comma-separated value (CSV) format using a download and parse program. At the time of Reference [17], waterfall plots were constructed from the received signal strengths over the 1-minute interval. This process continues to repeat, replacing the data on the EPRI server and the localhost data files. To scale the surveyor for long-term operation and data analytics, a database collecting the downloaded spectral scans would allow for minute, hour, day, and week data analytics of multiple sites. Its goal is to display spectrum occupancy in a variety of graphically informative plots to survey a geographic region's spectrum usage. Occupancy statistics will include average values of the frequencies over time, most available channels, and highest and lowest transmitted power. The database will be managed by a server, which further allows control of local database access once the data from the sftp server are collected.

Surveyor Improvements

Building on the work done in Reference [17], an optimized front-end as well as back-end data analysis platform is conceptualized in Figures 3-1 through 3-3. USB driver issues that affected the continual operation of the HackRF devices transferring to a local computer for upload have also been resolved.

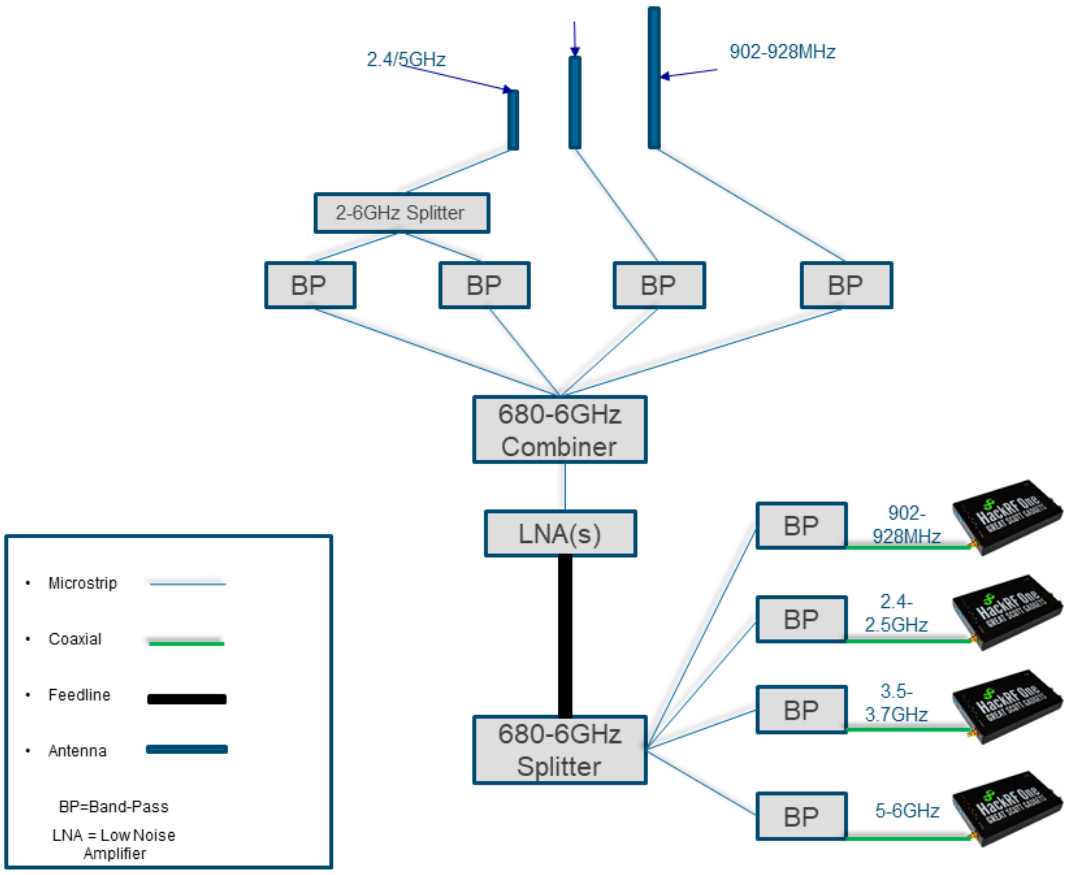

Figure 3-1
RF Front-End Prototype

RF Front-End Prototype

To create a deployable receiver front end for the four frequency bands of interest, amendments to Reference [17] must be made for a unified front end. By using power splitting, all four frequency bands can be surveyed, and the SMA port connections to the front-end receiver can be covered for unused frequencies. The 2.4-GHz and 5-GHz antenna must be split and filtered separately to decrease the noise prior to amplification at the expense of two separate filters. This approach is a simple solution considering the variation in bandwidth of 100 MHz for the 2.4-GHz scan and the >500-MHz bandwidth for the 5-GHz signals. All four bands are then combined and amplified with a wideband and flat low-noise amplifier (LNA) prior to entering the feedline. One LNA will result in a wideband gain of about 20 dB for each band to account for insertion loss over the 100-ft coaxial cable. At the end of the feedline, the wideband splitter is again used and filtered for the respective bands to a unique HackRF One. Originally, one HackRF One switched its scanning between two frequency bands. The issues from this operation are explained in “USB Driver Issue Resolved” (later in this section) along with the solution. Design for the RF front end will contain one enclosed hardware unit between the antennas and the feedline, which is composed of microstrip lines with power splitters/combiners and band-pass filters. An additional enclosed

hardware between the end of the feed line and the HackRF Ones would also be constructed with microstrip lines, a power splitter, and band-pass filters.

Data Analytics

Maintaining a periodically updated and long-term data profile is necessary to monitor the spectrum usage in a dynamic location. Varying transmission times, signal strength, and times of operation will change both regionally and over time. The convenience of loading the downloaded data based on day of acquisition and time allows for a diverse set of data analytics to be performed and customized for any user. An example format of the data stored in the database is shown in Table 3-1; the work flow diagram is shown in Figure 3-2. Table 3-1 shows an example of the first two sample times of two consecutive 60-second spectral scans. Each day might have a table as shown for each frequency band. Multiple days can be stored as separate tables or in addition to existing tables. When memory requirements become constrained, previous data can be transformed into new tables with only informative metrics for graphical display. The demands on memory from such a large data table will depend on the sampling time and intervals of requested data analytics. Extremely high sampling rates are needed to study the noise floor characteristics as well as millisecond transmission times.

Table 3-1
Example Database Entry

Date	Time	Frequency	Signal Strength	Sample Time
2018-12-31	15:41:00.000	902	-68	0.000
2018-12-31	15:41:00.000	…	…	0.000
2018-12-31	15:41:00.000	928	-76	0.000
2018-12-31	15:41:00.001	902	-66	0.001
2018-12-31	15:41:00.001	…	…	0.001
2018-12-31	15:42:00.001	928	-66	0.001
2018-12-31	15:42:00.000	902	-58	0.000
2018-12-31	15:42:00.000	…	…	0.000
2018-12-31	15:42:00.000	928	-74	0.000
2018-12-31	15:42:00.001	902	-67	0.001
2018-12-31	15:42:00.001	…	…	0.001
2018-12-31	15:42:00.001	928	-77	0.001

Analytics can be queried from the database for each frequency over a given time interval. Data keeping in this format also allows for a weekly snapshot of channel characteristics at a given time each day. Querying a channel over its scanned range can determine transmission time lengths—or their absence—and then report with maximum, minimum, and average calculations for each channel. Customized queries in addition to the basic statistics proposed are possible by

using Python, Pandas, and Structured Query Language (SQL) database connectors for entry and processing. Pandas is a high-performance data analytics package for Python, which allows pulling SQL data, processing, and writing new tables. For instance, SQL queries can be executed by Pandas DataFrames in a running Python script. The concept shows MySQL as a database type and Pandas as the analytics package as an example.

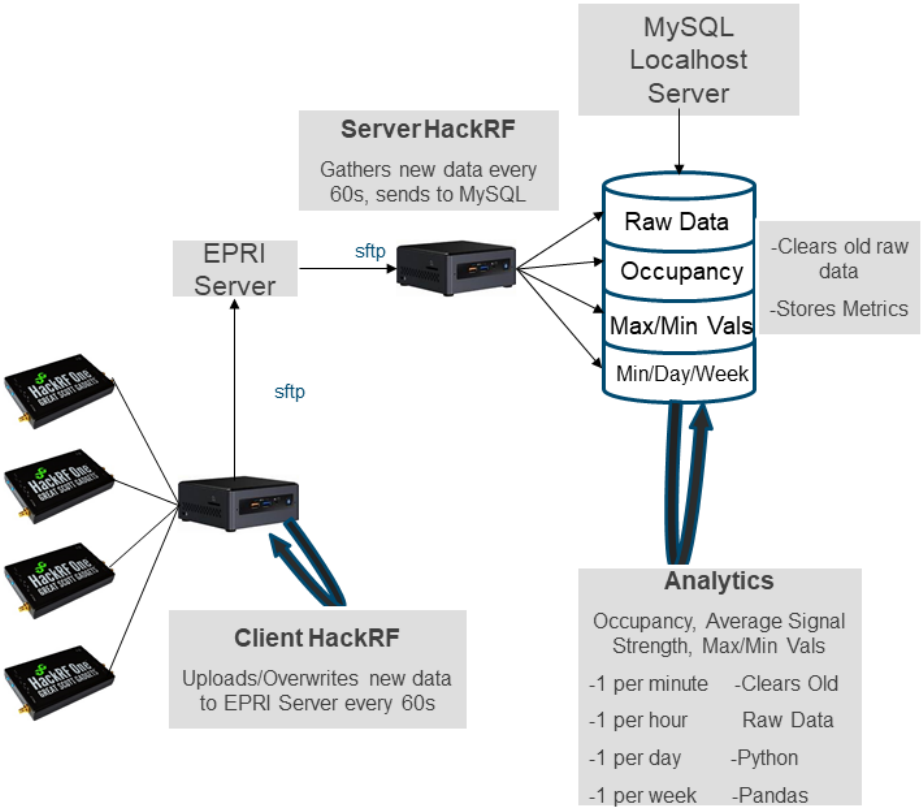

Figure 3-2
Data Analytics Work Flow

Figure 3-3 shows the overview of the entire Unlicensed Spectrum Surveyor with the client and server HackRF computers implementing the data upload and download from the EPRI server.

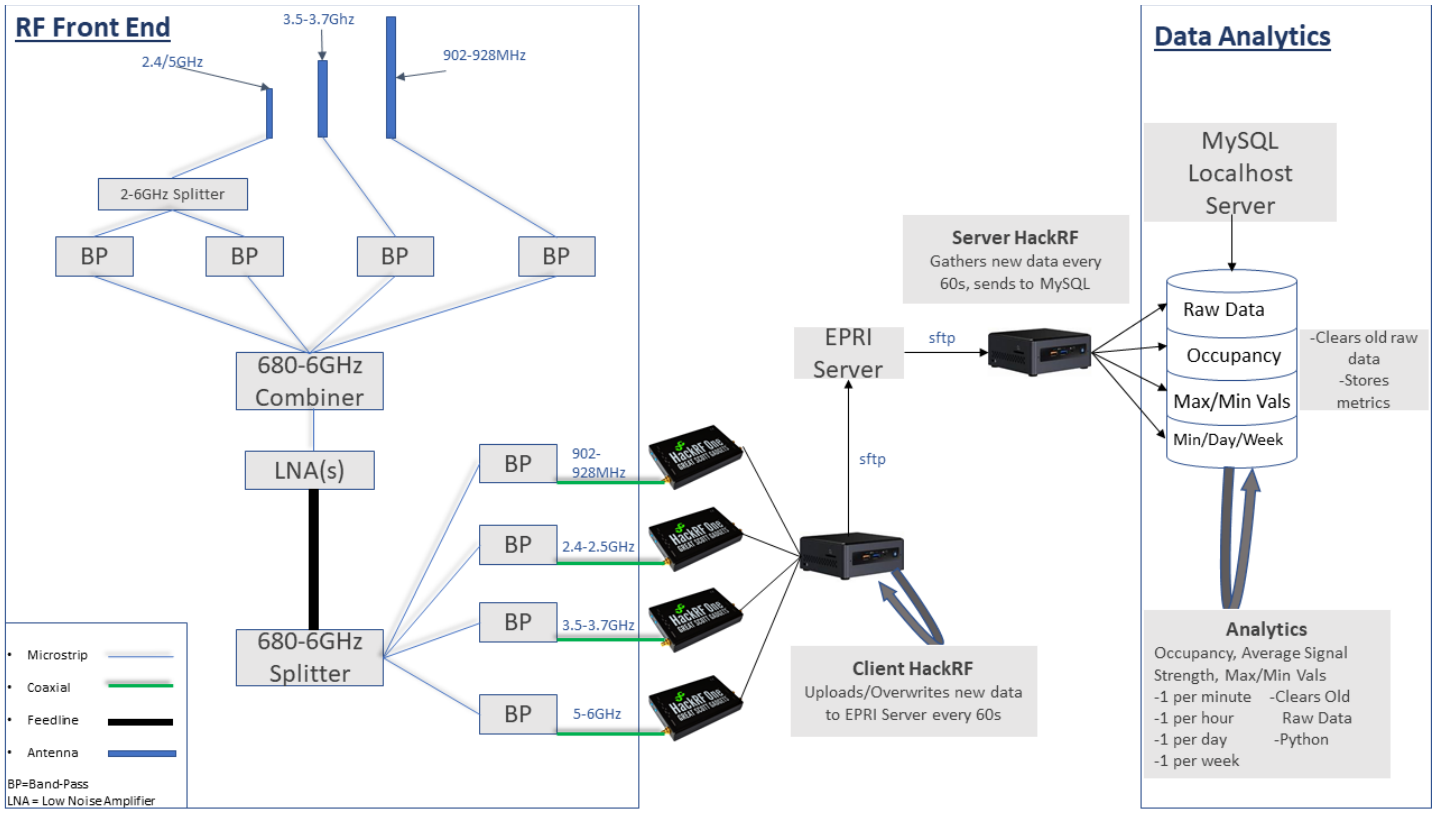

Figure 3-3
Unlicensed Surveyor Operation

USB Driver Issue Resolved

The client device needs to scan four frequency bands simultaneously for 60-second intervals and upload the collected data to the server. This was originally done by using two HackRF devices that each switched between two frequency bands every 60 seconds. A HackRF sweep program scans a frequency band and writes it to a binary file continuously. To parse the data in 60-second intervals, two sweep programs were repeatedly started and killed every 60 seconds so that the binary files could be uploaded to the server. With this approach, the client device failed after 3–4 hours of normal operation because of a bug in the sweep program. Therefore, the HackRF devices failed to properly reset back to idle state. This problem was resolved by changing the sweep program to write to a new binary file every 60 seconds. During this time, the sweep program prints out the start and stop times for the scan interval and starts scanning and writing to a new binary file once more. With this new method, four HackRF devices are used to simultaneously scan the frequency bands. This allows for the HackRF devices to collect data continuously without being interrupted by stopping and restarting the program for each of the frequency bands. The client program starts four different sweep programs and waits to receive start and stop times for this interval. Finally, it uploads the binary file to the server and deletes the file from the client device. This solution allows for continuous data collections for four frequency bands over 60-second intervals.

Results

Expected Outcomes

Analysis of the 902–928 MHz and 2400–2500 MHz spectrum at EPRI's Knoxville laboratory will show the intended use of the surveyor. Activity in the 2.4 GHz and 5 GHz ranges is expected from existing WiFi devices, so it is included to show results from a heavily occupied frequency band. The 902–928 MHz band is expected to have low activity but may find significant transmissions near industrial facilities or utility metering endpoints where sensors are deployed. Initial results will show average received power levels and a normalized occupancy list showcasing the most dominant frequencies over a time interval. The tests were conducted with a 20-minute period because of current memory restrictions of data processing. In the future, when memory limitations are resolved, a day's worth of surveyor scanning will be processed—the amount needed to account for sensor devices that transmit bi-hourly or more slowly. The surveyor's usefulness will scale with IoT sensor, smart meter, and FAN network topology growth.

902–928 MHz Results

Figure 3-4 shows the average magnitude of scanned frequencies in the 902–928 MHz range on 2018-10-29. Occupancy is sparse, and even the strongest signals scanned may still be noise. Measurements taken on 2018-11-02 at a random time show nearly identical results, suggesting that the highest signals are not transmissions but most likely unintentional radiators.

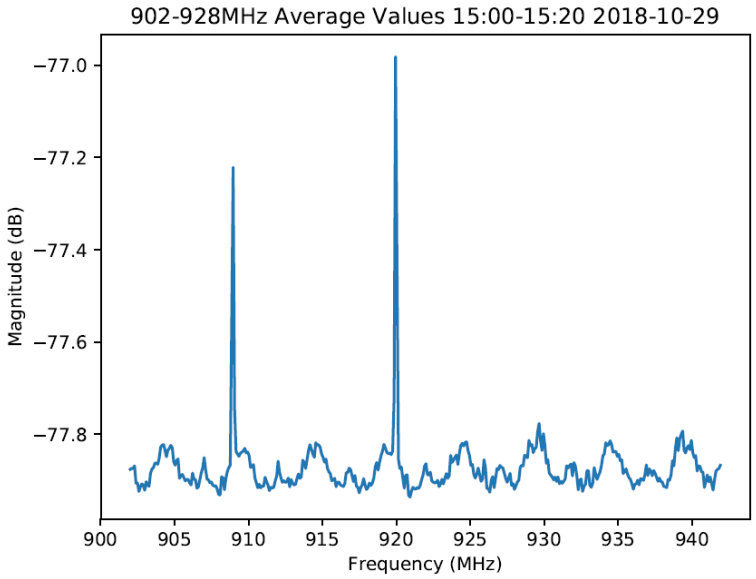

Figure 3-4
902–928 MHz Average Values

Figures 3-5 through 3-7 show the highest measured signal strengths on the order of 10, 25, and 50 signals, respectively. The graphs have been normalized according to feature selection on a 0 to 1 scale.

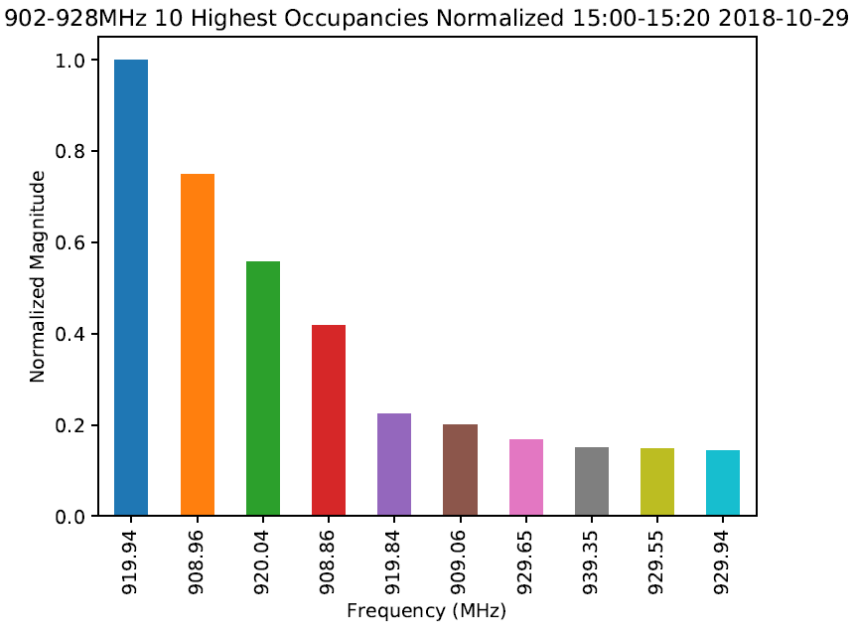

Figure 3-5
902–928 MHz Occupancy (10 Strongest)

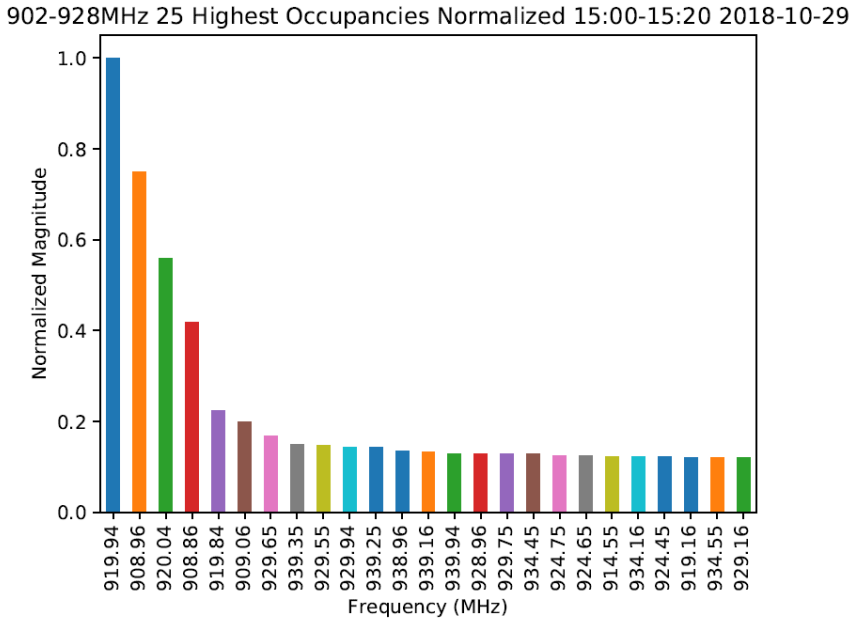

Figure 3-6
902–928 MHz Occupancy (10 Strongest)

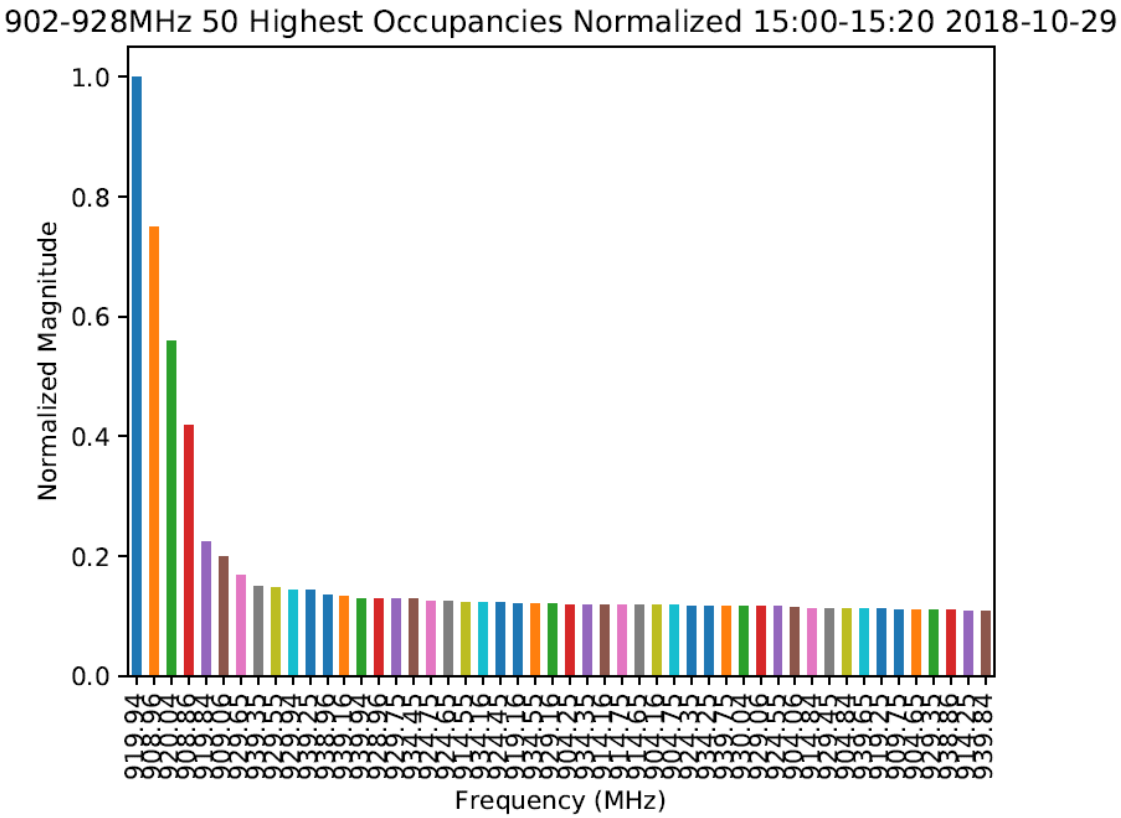

Figure 3-7
902–928 MHz Occupancy (50 Strongest)

Figure 3-7, which displays the 50 strongest scanned signals, clarifies that much of the band is unused. This information can exploit the most probable transmission channels and aid station designers in their frequency coordination.

2400–2500 MHz Results

To see a more valuable result by the surveyor, a scan of the WiFi occupied 2400–2500 MHz range reveals a wide occupancy between approximately 2430 MHz and 2445 MHz. Figure 3-8 shows some activity above the noise floor centered around 2410 MHz as well as 2460 MHz. It is also apparent that the most available channels in this band are from 2470 MHz to 2500 MHz. Figures 3-9 through 3-11 display the normalized occupancies of which the coordinator would want to avoid if possible. Because frequency-hopping channels must have equal transmission times on average, a designer may choose to exploit a narrower bandwidth outside of the more densely populated regions and adjust the modulation and channel hop spacing to accommodate. Further testing would need to be done to show whether the method of avoidance would lead to decreased transmission failures. The least occupied frequencies can be shown in a similar fashion (see Figures 3-12 through 3-14). Improvements would involve adding percent bandwidths around a center channel and calculating the probability of success or interference. These types of tests could be run before coordinating a system and then used as a monitoring tool to maintain appropriate interference mitigation.

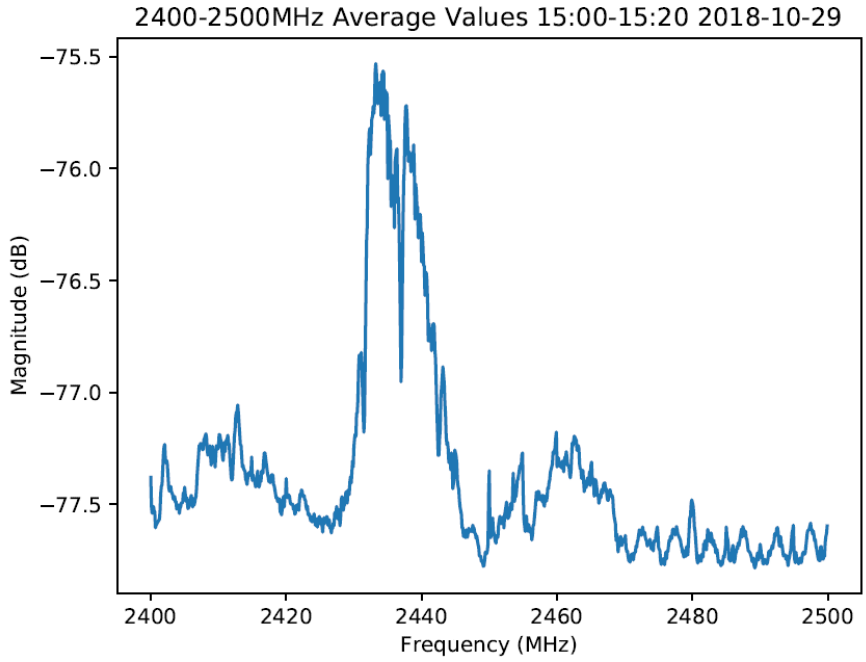

Figure 3-8
2400–2500 MHz Average Values

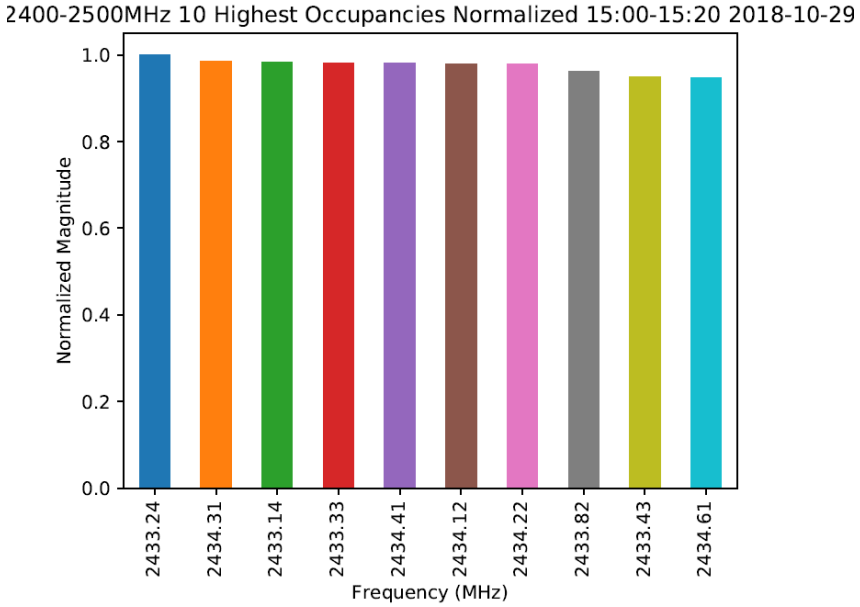

Figure 3-9
2400–2500 MHz Occupancies (10 Strongest)

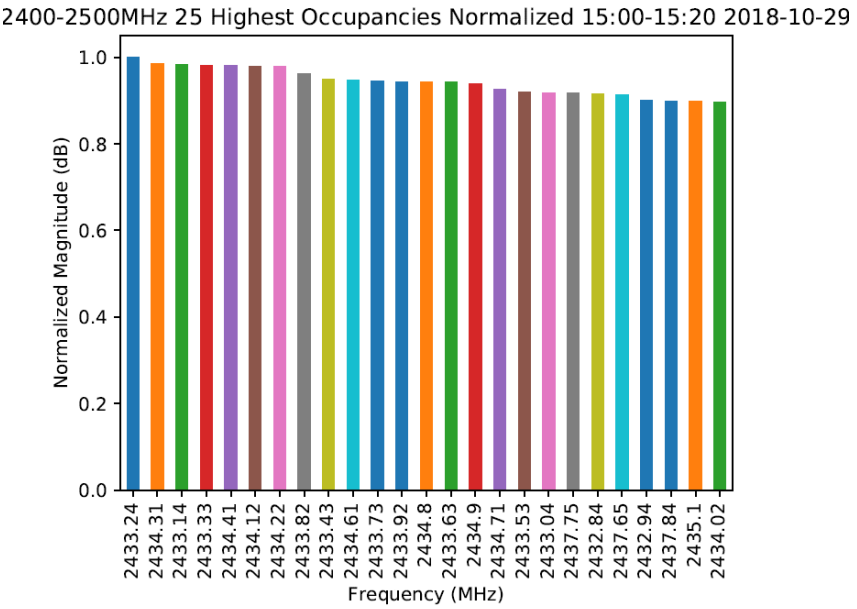

Figure 3-10
2400–2500 MHz Occupancy (25 Strongest)

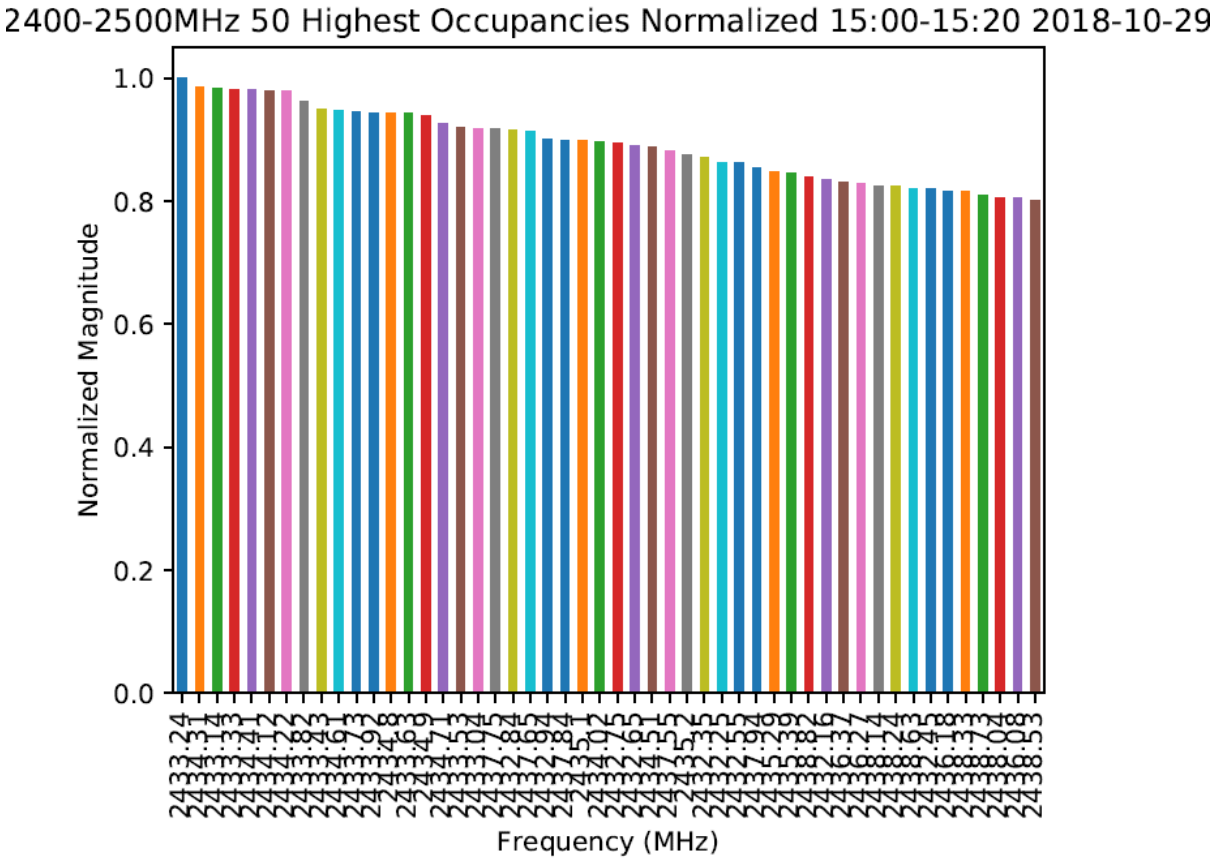

Figure 3-11
2400–2500 MHz Occupancy (50 Strongest)

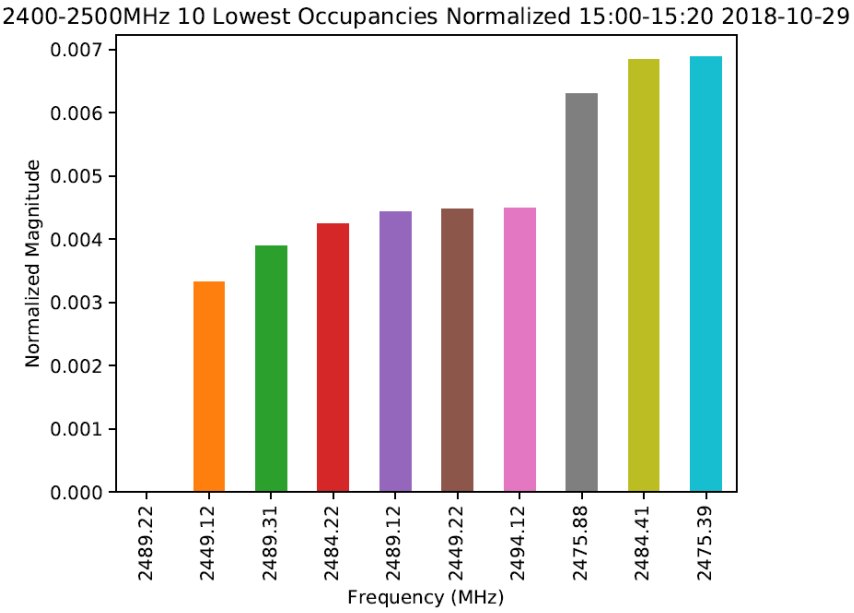

Figure 3-12
2400–2500 MHz Occupancy (10 Weakest)

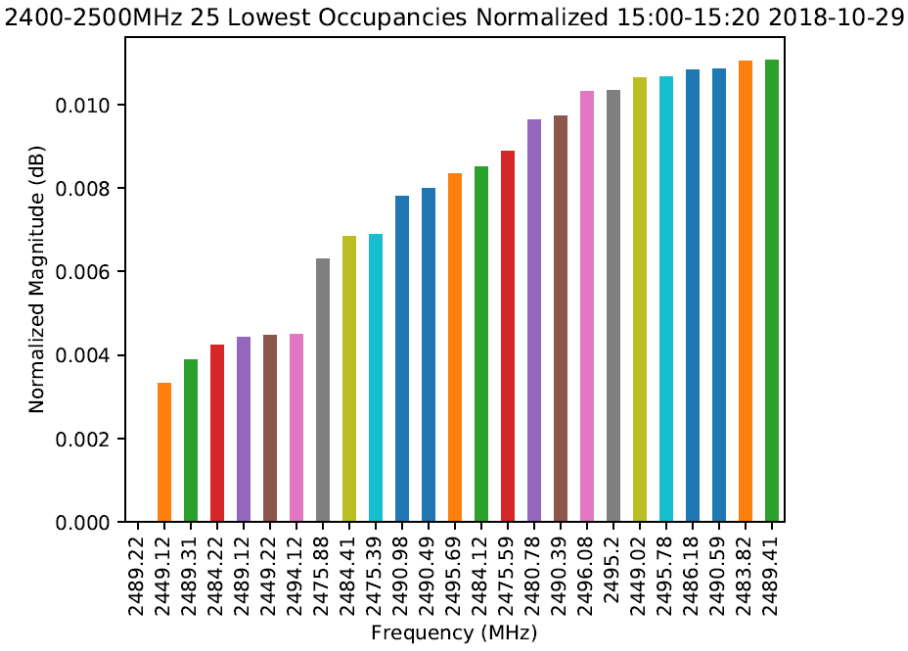

Figure 3-13
2400–2500 MHz Occupancy (25 Weakest)

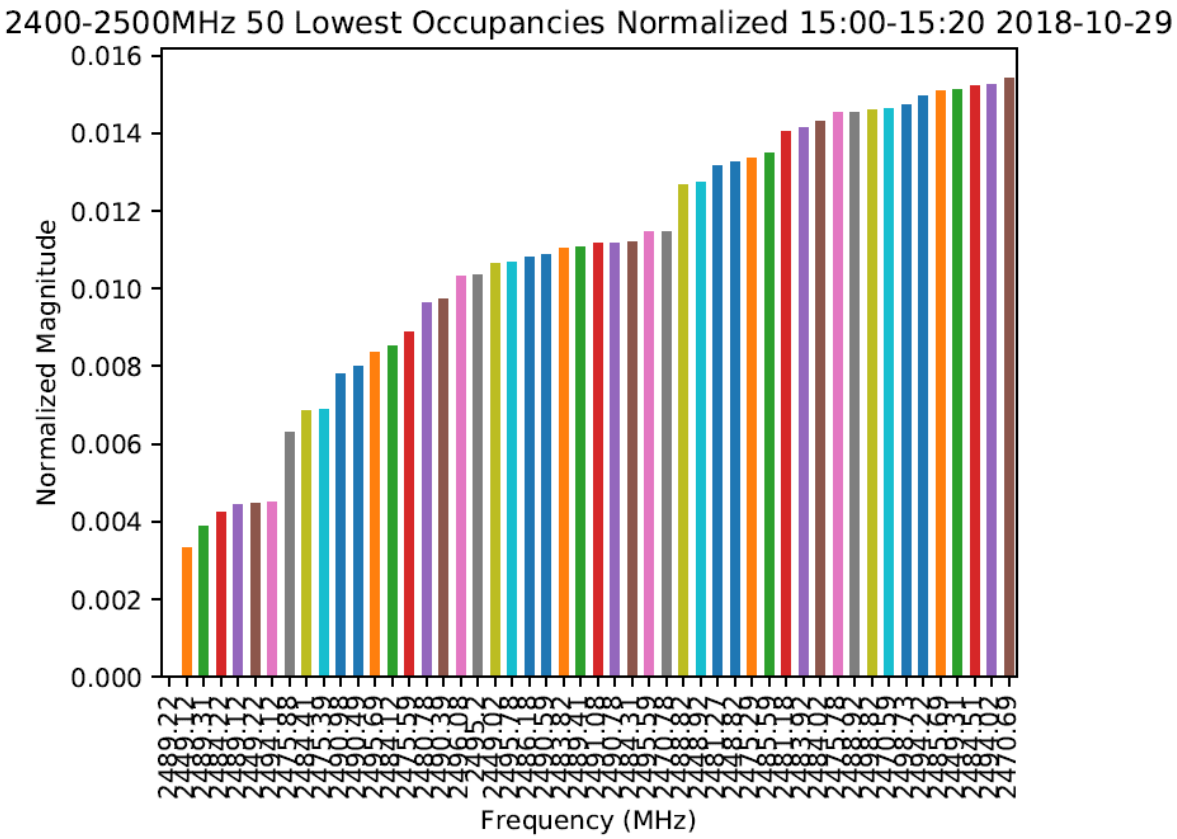

Figure 3-14
2400–2500 MHz Occupancy (50 Weakest)

Outcomes

Results for the 902–928 MHz range show little activity. If the results remain consistent over time, it would suggest that there is no coordinated activity in the region and would allow full use of the unlicensed band. Being able to measure the availability of unlicensed bands is important in choosing radio devices based on regional occupancy, protocol specifications, and vendor design. If the results show a limited range of availability, alternative communication methods would need to be considered—or the risk of trying to dominate a narrow unlicensed band would be imminent. This is not ideal because no ownership can be claimed over any unlicensed frequencies. Using highly robust interference mitigation techniques and a multi-protocol specification would be the most realistic solution in densely populated unlicensed bandwidths. If limited bandwidth is available, but a designer can choose to develop a custom-range device if frequency-hopping spacing allows, a user can still follow the regulations of equal channel transmission times with a narrower bandwidth design. This method may not be scalable in the long term, which leads systems back to the need for more protocol resiliency and compatibility. Results will vary significantly based on location, but the effects of the surveyor will verify occupancy nonetheless.

4
SPECTRUM SHARING IN 406–420 MHZ SPECTRUM

Introduction

The concept of sharing the spectrum at 406–420 MHz between incumbent government users and utility networks has been discussed for several years [18, 19]. Although the size of the allocation makes it suitable for broadband operation with systems such as LTE, some incumbent users have deployed narrowband applications such as land mobile radio (LMR) that do not require or fully use the 14 MHz of allocated spectrum.

To provide a technical basis and validate parameters for sharing, testing and demonstration of suitable scenarios is needed.

Utility sharing of this spectrum could take place in several scenarios:

- Utility FANs for "blue sky" day-to-day operational requirements
- Emergency communication networks to enable restoration in "black sky" events
- A secure emergency network (as defined in DARPA RADICS) to mitigate persistent cyber attacks

Ideally, all these scenarios would be allowed (based on agreements with incumbents), but specific parameters could vary depending on the scenario.

Testing and demonstration of spectrum sharing with a utility FAN for "blue sky" operational requirements would center around standing up a test network implementing LTE in a portion of the 406–420 MHz band while operating the incumbent LMR system in another portion of the band.

The test plan would examine various coexistence scenarios to determine the necessary power levels, frequency separation, geographical separation, and other factors to ensure mutual non-interference.

Incumbent Analysis

Before a detailed test plan can be developed, further analysis of incumbent users and systems is needed. The incumbents are various federal and government agencies that have their spectrum regulated under the National Telecommunications and Information Administration (NTIA) (compared to FCC for commercial spectrum). It is important to have some guidance on the types of communication systems operating in this spectrum to develop appropriate tests for coexistence and sharing.

Because some government users are involved in uses for military or security, the incumbent database is classified. Therefore, this research is expected to be conducted by Idaho National Laboratory (INL), where the appropriate level of access exists. The expectation is that the

incumbent data will be "abstracted" into sharable form, highlighting the generalized geographic areas and technical operational parameters of incumbent systems.

The plan for the incumbent analysis has been in place since summer 2018, but progress has been held up by regulatory and administrative hurdles. INL is working on these issues but does not have a date for when the results will be available. This impact the team's confidence that the test plan will address operation with all types of incumbent systems.

However, many of the incumbents are using analog, narrowband LMR systems; INL itself is an incumbent and has such as system. Therefore, initial testing will focus on interoperability with LMR.

Baseline Performance of LTE in the 406–420 MHz Band

Depending on equipment capabilities, both TDD and FDD modes of LTE can be tested.

The first test bed will consist of a software-defined radio (SDR) implementation of an LTE system (eNodeB, or eNB) and multiple user equipment (UE), running on the Ettus Research Universal Software Radio Peripheral (USRP) platform. This will be a benchtop implementation with cables and attenuators between nodes. In addition to the LTE system, physical 406-MHz LMR base stations and mobile radios will be cabled together with additional attenuators.

Sharing Approaches

The following sharing proposals show possible division of the 406–420 MHz band between a utility LTE system and incumbent users (NTIA).

Keeping the same 10-MHz FDD split as Band 31 and Band 73, the following sharing plans could be proposed and tested with the agreement of the incumbent. These would be appropriate if the NTIA incumbent is lightly using the spectrum; existing (and planned) incumbent operations can be accommodated to 4 MHz.

Option 1: Utility LTE 5 x 5 or 3 x 1.5 x 1.5 FDD (10-MHz utility use; 4-MHz NTIA incumbent)

Frequency Range	User	Width	
406–411	Utility LTE UL	5 MHz	
411–415	NTIA	4 MHz	
415–420	Utility LTE DL	5 MHz	

Uplink = UL
Downlink = DL

Note: FDD split is reduced to 9 MHz with 5-MHz channels.

Option 2: Utility LTE 3 x 3 or 2 x 1.5 x 1.5 FDD (6-MHz utility use; 8-MHz NTIA incumbent)

Frequency Range	User	Width	
406–407	NTIA	1 MHz	
407–410	Utility LTE UL	3 MHz	
410–417	NTIA	7 MHz	
417–420	Utility LTE DL	3 MHz	

Uplink = UL
Downlink = DL

Note: 10-MHz UL/DL split for utility LTE.

Option 3: Utility LTE 1.5 x 1.5 FDD (3-MHz utility use; 11-MHz NTIA incumbent)

Frequency Range	User	Width	
406–408.5	NTIA	2.5 MHz	
408.5–410	Utility LTE UL	1.5 MHz	
410–418.5	NTIA	8.5 MHz	
418.5–420	Utility LTE DL	1.5 MHz	

Uplink = UL
Downlink = DL

Note: 10-MHz UL/DL split for utility LTE.

TDD could be considered for additional flexibility in sharing. TDD modes could occupy the utility LTE DL ranges described previously. Other FDD sharing layouts could be developed if deviation from the 10-MHz FDD split is possible (based on LTE equipment capabilities).

Testing Interference from LTE to Incumbent LMR

LMR operation would be tested with a concurrently operating LTE network (one or more eNB plus two or more UEs) under various conditions of system separation, frequency separation, LTE channel bandwidth, link distances, and power levels. Before defining specific tests, additional information is needed on incumbent operating frequencies, duplex splits, base site locations, and normal operating power levels. For the anticipated testing at INL's wireless test range, this information can be confirmed in advance from the INL operations staff. For this series of tests, the LTE system will be loaded with simulated bi-directional data transfer flows to/from one or more UEs.

Test Type 1: LMR base operation concurrent with operation of LTE eNB on DL. Test LMR sensitivity, range, and data communication (if used), with and without LTE operating. Measure LTE eNB signal strength at LMR base site; test for loss of sensitivity or spurs on all LMR uplink (UL) frequencies.

Test Type 2: LMR remote operation concurrent with LTE eNB. Test LMR field radios (vehicle and handheld) at coverage limit from LMR base with LTE eNB operating in vicinity. Measure LTE eNB signal strength at LMR remote radio. Document any interference or loss of sensitivity when LTE eNB is operating. Test for spurs on all LMR downlink (DL) frequencies. Test effects on LMR data communication if used (P25 or DMR).

Test Type 3: LMR base operation concurrent with operation of LTE UE on UL. Test LMR sensitivity, range, and data communication (if used), with and without LTE UE operating in proximity to base site. Measure LTE UE signal strength at LMR base site; test for loss of sensitivity or spurs on all LMR UL frequencies.

Test Type 4: LMR remote operation concurrent with LTE UE on UL. Test LMR field radios (vehicle and handheld) at coverage limit from LMR base with LTE UE operating in vicinity. Measure LTE UE signal strength at LMR remote radio. Document any interference or loss of sensitivity when LTE UE is operating. Test for spurs on all LMR DL frequencies. Test effects on LMR data communication if used (P25 or DMR).

For each of these tests, specific quantifiable LMR performance metrics will be established to evaluate any interference effects.

Testing Interference from Incumbent LMR to LTE

LTE network operation would be tested during concurrent operation of the LMR system under various conditions of system separation, frequency separation, LTE channel bandwidth, link distances, and power levels.

Test Type 1: Data transfer on the LTE UL (from UE to eNB) with LMR transmission (data and/or voice) from the base station. Test LTE eNB sensitivity, range, and data throughput from remote UE, with and without LMR base station operating. Measure LMR signal strength at input to eNB; test for loss of sensitivity of eNB resulting from transmissions on all LMR DL frequencies.

Test Type 2: Data transfer on the LTE UL (from UE to eNB) with LMR transmission (data and/or voice) from remote radio (vehicle or handheld). Test LTE eNB sensitivity, range, and data throughput from remote UE, with and without LMR remote radio operating. Measure LMR signal strength at LTE eNB. Document any interference, loss of sensitivity, or reduced data throughput when LMR remote is operating.

Test Type 3: Data transfer on the LTE DL (from eNB to UE) with LMR transmission (data and/or voice) from the base station. With LTE UE located near cell edge, test sensitivity, range, and data throughput, with and without LMR base station transmitting. Measure LMR base station signal strength LTE UE input. Test for loss of sensitivity of UE resulting from transmissions on all LMR DL frequencies.

Test Type 4: Data transfer on the LTE DL (from eNB to UE) with LMR transmission (data and/or voice) from the remote radio. With LTE UE located near cell edge, test sensitivity, range, and data throughput, with and without LMR remote radio operating in vicinity. Measure LMR remote radio signal strength LTE UE input. Test for loss of sensitivity of UE resulting from transmissions on all LMR UL frequencies.

For each of these tests, specific quantifiable LTE performance metrics will be established to evaluate any interference effects.

Other Tests

Contingent on INL (which has access to the classified database of NTIA users in the spectrum) completing the incumbent analysis and making the results available, the team will investigate other types of incumbent operations in the 406–420 MHz band that may differ from LMR. This is based on sufficiently detailed technical disclosure of the emission types being used. Additional test scenarios may be defined based on findings if necessary.

These test results will provide the technical basis to define spectrum sharing scenarios between a utility FAN and incumbents, given the existing systems operating in the band, relative geographic locations, and current channel allocations.

Field Testing

Based on the findings from the bench-testing environment, a second phase of field testing is planned for mid-2019. The test plan will be revised to define specific tests to clarify any gaps or areas in which true field data are required.

Field testing will include adaptation of commercial LTE equipment (eNB and UE) originally designed for Bands 31 and 73, modified to operate in the 406–420 MHz range.

The test site and equipment would be modeled in EDX or similar tools to help design the specifics of the baseline test plan.

Because the 406–420 MHz band is not an existing 3GPP band, the behavior of the system will be new. The modified equipment will also be new. Therefore, performing baseline LTE performance tests such as range and cell edge data rates may be valuable for understanding the nominal performance of this new LTE system and band (without interference).

Conclusions

Testing scenarios are presented in the context of developing and documenting the technical feasibility and parameters for successful shared operation in the 406–420 MHz band. *Successful sharing* is defined as simultaneous operation of a utility private LTE system in the band along with incumbent LMR systems, with neither system causing interference or performance degradation to the other. Sharing parameters may include band plans, channel bandwidths, power levels, duplex frequency separation, and guard bands. Similar testing and sharing scenarios are possible in other bands that may be identified. The wireless testing range at INL is ideal for testing of sharing and coexistence because it is an incumbent user of the 406–420 MHz band. This testing approach considers the only known incumbent system: LMR. If other systems with differing characteristics are identified, the testing approach may be altered or expanded.

5
CONCLUSIONS AND NEXT STEPS

An assessment of the issues and need for design standards regarding unlicensed frequency operation has been shown. More discoveries from the 802.19 Working Group and additional standards for interoperability will allow for denser and more diverse networks in the future. Spectrum surveying in the unlicensed bands has been shown in a simplified setting, but widescale development and big data storage requirements will need to be implemented for further advising. Results from the spectrum surveyor have shown how frequency scanning can inform system designers of channel allocations and overall usage regionally. This information assists in channel allocation and network design choices. Multiple sites can be surveyed, and custom coordination on a local basis can be achieved using the occupancy results. The FAN topology may be a viable solution when such local frequency coordination is necessary because its routing capabilities allow for a diverse channel choice among neighboring routers' mesh nodes. Star topologies would not benefit from diverse local channel allocations because the ability to reach all nodes in the network would suffer. The downside of diverse local channel allocations are complexity, organization, and device design limitations.

In addition to the unlicensed bands proposed mitigation methods, licensed frequency operation in the 406–420 MHz band tests for utility LTE systems seeking to harmonize future government and utility coexistence has been conceptualized. More in-depth proposals for coexistence from simulations will help to advise future hardware and network implementations, but further testing of such designs will also need to be conducted. Verification of new standard amendments related to interference mitigation with a radio test bed could also confirm simulation findings. Because of the degree of design choice within existing protocols, adopting subsets of the larger 802.11ah, 802.15.4g, Wi-SUN, and LTE standards from rigorous testing that validates harmonious networks will be a consistent subject in continued efforts toward coexistence.

6
REFERENCES

1. Federal Communications Commission, 47 CFR §18.301 (2010).
2. Federal Communications Commission, 47 CFR §15.249 (2009).
3. Federal Communications Commission, 47 CFR §15.245 (2009).
4. Federal Communications Commission, 47 CFR §15.247 (2009).
5. European Radiocommunications Committee. Recommendation 70-03 Relating to the Use of Short-Range Devices (August 2011).
6. "Utility Industry." *ZigBee Alliance*, 16 Feb. 2018. www.zigbee.org/what-is-zigbee/utility-industry.
7. *Low-Power Wide Area Networks: Overview, Characteristics, and Applications.* EPRI, Palo Alto, CA: 2018. 3002009791.
8. *Utility Telecom Taxonomy and Architecture for Field Area Networks*. EPRI, Palo Alto, CA: 2017. 3002009786.
9. "IEEE Standard for Low-Rate Wireless Networks." *IEEE Std 802.15.4-2015 (Revision of IEEE Std 802.15.4-2011)*, pp. 1–709, 22 April 2016.
10. GE Grid Solutions. *Communications: MDS Orbit MCR-4G*. www.gegridsolutions.com/communications/catalog/MDSOrbit.htm.
11. Gates, Chris and Ganesh Pattabiraman, "Terrestrial Beacons Bring Wide Area Location Indoors." *GPS World*, 12 July 2016. gpsworld.com/terrestrial-beacons-bring-wide area-location-indoors/.
12. "IEEE Standard for Information technology: Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 2: Sub-1GHz License Exempt Operation." *IEEE Std 802.11ah-2016 (Amendment to IEEE Std 802.11-2016, as amended by IEEE Std 802.11ai-2016)*, pp. 1–594, 5 May 2017.
13. "IEEE Standard for Local and metropolitan area networks—Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs) Amendment 3: Physical Layer (PHY) Specifications for Low-Data-Rate, Wireless, Smart Metering Utility Networks." *IEEE Std 802.15.4g-2012 (Amendment to IEEE Std 802.15.4-2011)*, pp.1–252, 27 April 2012.
14. "IEEE Standard for Information technology: Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications." *IEEE Std 802.11-2016 (Revision of IEEE Std 802.11-2012)*, pp. 1–3534, 14 Dec. 2016.
15. Sum, Chin-Sean, "IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs)." *TG4g Coexistence Assurance Document.* April 2011.

16. Gu, J., Orlik, P., Nagai, Y., and Rolfe, B. (Mitsubishi Electric Research Laboratories), *Interference Mitigation for Coexisting 802.15.4g and 802.11ah Networks, 2018-05-08, IEEE 802.19-18/0027r0*. May 2015.

17. *Unlicensed Noise Floor Study: Unlicensed Spectrum Surveyor.* EPRI, Palo Alto, CA: 2018. 3002009787.

18. Utilities Technology Council, *406–420 MHz Band Issue Brief, 2016*. https://utc.org/wp-content/uploads/2018/09/2018_9_IssueBrief406-420.pdf.

19. *Assessment of Licensed Communication Spectrum for Electric Utility Applications*. EPRI, Palo Alto, CA: 2015. 3002005851.

Export Control Restrictions

Access to and use of this EPRI product is granted with the specific understanding and requirement that responsibility for ensuring full compliance with all applicable U.S. and foreign export laws and regulations is being undertaken by you and your company. This includes an obligation to ensure that any individual receiving access hereunder who is not a U.S. citizen or U.S. permanent resident is permitted access under applicable U.S. and foreign export laws and regulations.

In the event you are uncertain whether you or your company may lawfully obtain access to this EPRI product, you acknowledge that it is your obligation to consult with your company's legal counsel to determine whether this access is lawful. Although EPRI may make available on a case by case basis an informal assessment of the applicable U.S. export classification for specific EPRI products, you and your company acknowledge that this assessment is solely for informational purposes and not for reliance purposes.

Your obligations regarding U.S. export control requirements apply during and after you and your company's engagement with EPRI. To be clear, the obligations continue after your retirement or other departure from your company, and include any knowledge retained after gaining access to EPRI products.

You and your company understand and acknowledge your obligations to make a prompt report to EPRI and the appropriate authorities regarding any access to or use of this EPRI product hereunder that may be in violation of applicable U.S. or foreign export laws or regulations.

The Electric Power Research Institute, Inc. (EPRI, www.epri.com) conducts research and development relating to the generation, delivery and use of electricity for the benefit of the public. An independent, nonprofit organization, EPRI brings together its scientists and engineers as well as experts from academia and industry to help address challenges in electricity, including reliability, efficiency, affordability, health, safety and the environment. EPRI members represent 90% of the electric utility revenue in the United States with international participation in 35 countries. EPRI's principal offices and laboratories are located in Palo Alto, Calif.; Charlotte, N.C.; Knoxville, Tenn.; and Lenox, Mass.

Together…Shaping the Future of Electricity

3002013392

Electric Power Research Institute
3420 Hillview Avenue, Palo Alto, California 94304-1338 • PO Box 10412, Palo Alto, California 94303-0813 • USA
800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com