Wi-Fi Sensing

A New Technology Emerges

Source: Wireless Broadband Alliance
Author(s): WBA Wi-Fi Sensing Group
Issue date: October 2019
Version: 1.0
Document status: Final

ABOUT THE WIRELESS BROADBAND ALLIANCE

Founded in 2003, the vision of the Wireless Broadband Alliance (WBA) is to drive seamless, interoperable service experiences via Wi-Fi within the global wireless ecosystem. WBA's mission is to enable collaboration between service providers, technology companies and organizations to achieve that vision. WBA undertakes programs and activities to address business and technical issues, as well as opportunities, for member companies.

WBA work areas include advocacy, industry guidelines, trials and certification. Its key programs include NextGen Wi-Fi, 5G, IoT, Testing & Interoperability and Roaming, with member-led Work Groups dedicated to resolving standards and technical issues to promote end-to-end services and accelerate business opportunities. WBA's membership is comprised of major operators and leading technology companies, including Broadcom, BSNL, Orange, Facebook, Google, HPE Aruba, Huawei, Microsoft, NTT DOCOMO Ruckus, Shaw, SK Telecom and T-Mobile US.

The WBA Board includes AT&T, Boingo Wireless, BT, Cisco Systems, Comcast, Deutsche Telekom AG, GlobalReach Technology, Intel and KT Corporation. For a complete list of current WBA members, **click here**.

Follow Wireless Broadband Alliance at:
www.twitter.com/wballiance
http://www.facebook.com/WirelessBroadbandAlliance
https://www.linkedin.com/company/wireless-broadband-alliance

UNDERTAKINGS AND LIMITATION OF LIABILITY

This Document and all the information contained in this Document is provided on an 'as is' basis without warranty of any kind, either expressed or implied, including, but not limited to, the implied warranties of merchantability, fitness for particular purpose, or non-infringement.

In addition, the WBA (and all other organizations who may have contributed to this document) makes no representations or warranties about the accuracy, completeness, or suitability for any purpose of the information. The information may contain technical inaccuracies or typographical errors. All liabilities of the WBA (and all other organizations who may have contributed to this document) howsoever arising for any such inaccuracies, errors, incompleteness, suitability, merchantability, fitness and non-infringement are expressly excluded to the fullest extent permitted by law. None of the contributors make any representation or offer to license any of their intellectual property rights to the other, or to any third party. Nothing in this information or communication shall be relied on by any recipient.

The WBA also disclaims any responsibility for identifying the existence of or for evaluating the applicability of any claimed copyrights, patents, patent applications, or other intellectual property rights, and will take no position on the validity or scope of any such rights. The WBA takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any effort to identify any such rights.

Neither the WBA nor any of the other organizations who may have contributed to this document will be liable for loss or damage arising out of or in connection with the use of this information. This is a comprehensive limitation of liability that applies to all damages of any kind, including (without limitation) compensatory, direct, indirect or consequential damages, loss of data, income or profit, loss of or damage to property and claims of third-parties.

CONTENTS

FIGURES

Executive Summary

Wi-Fi Sensing is a new technology which enables motion detection, gesture recognition as well as biometric measurement by using existing Wi-Fi signals. Wi-Fi Sensing operates similarly to a radar system, detecting motion and providing information that can be used to enable new Wi-Fi based services. It builds upon the existing standards, hardware, infrastructure, and deployments of Wi-Fi. Wi-Fi Sensing creates opportunities within the home security, health care, enterprise, and building automation/management markets, among many others, and creates a bridge for Wi-Fi service providers to enter these markets.

Wi-Fi Sensing technology and its applications are relatively new, and there are currently no standards that are specific to this technology. While some applications can be enabled using existing standards, there are technology gaps that limit the range of applications. Some of these gaps may be addressed via proprietary means; however, such an approach could inhibit interoperability, integration, and deployment. Alternatively, there could be opportunities for the introduction of new capabilities into the Wi-Fi standards. Standards support would allow for more efficient handling of existing use-cases and enable new use-cases that were previously not possible.

This paper provides an overview of the Wi-Fi Sensing technology, classifies the Wi-Fi Sensing use cases and requirements, and identifies the gaps in Wi-Fi standards that, if addressed, would lead to the enhancement of the technology and ease of deployment. Furthermore, a case study showcasing home monitoring as an example application is presented, examining topics related to testing.

1 Wi-Fi Sensing Introduction

1.1 Background

In Wi-Fi Sensing, radio information obtained during signal processing is used to detect environmental changes caused by motion of objects, pets and people. In many cases, the primary information extracted from the radio for Wi-Fi Sensing is the channel frequency response and/or the received signal strength. Computing this quantity is a typical function of any Wi-Fi receiver, as it enables a mechanism to compensate for the distortion introduced by the wireless channel. Wi-Fi Sensing builds upon these mechanisms, allowing any Wi-Fi device perform sensing and learn about changes in the environment.

Using one or multiple collaborating Wi-Fi devices to sense the environment and detect motion has many benefits and enables many new business opportunities. Network providers can utilize information made available through sensing to provide a new set of services to customers. Hardware original equipment manufacturers (OEMs) and chipset vendors can add Wi-Fi sensing as a feature to differentiate products. Advances in signal processing and feature extraction algorithms produce even more detailed information. As Wi-Fi sensing technology matures, new and more complex use cases are enabled.

In order to make Wi-Fi Sensing a viable and ubiquitous technology, standardization is needed. Wi-Fi technology has long been recognized for creating an infrastructure in which backward compatibility, interoperability and scalability are fundamental. The current state of Wi-Fi Sensing relies on a single device in a network using proprietary interfaces and application programming interfaces (APIs), which ultimately limit or restrict the technology. As discussed in this paper, there are new Wi-Fi Sensing capabilities that, if introduced into the standard, could improve efficiency and provide a catalyst for a new way in which Wi-Fi can be utilized.

1.2 Scope

The primary goal of this paper is to raise industry awareness of Wi-Fi Sensing technology and outline potential business opportunities. This paper specifies a set of use cases and identifies gaps in Wi-Fi standards that may limit Wi-Fi Sensing applications. Performance metrics required for supporting the use cases also are identified. Finally, next steps for further development of Wi-Fi Sensing technology and future applications are outlined.

1.3 System Overview

1.3.1 Network Topology

There are two primary modes of operation (or types of network) defined for Wi-Fi networks[1]: infrastructure and ad-hoc modes. In infrastructure mode, stations (STAs) are logically organized in a star topology. A central device or Access Point (AP) coordinates and controls communication among all STAs connected to the network. In infrastructure mode, a STA only communicates with its associated AP. The AP and associated STAs form an infrastructure basic service set (BSS). In ad-hoc mode, any STA may communicate with any other STA directly without the need for an AP. The group of STAs that communicates peer-to-peer forms an independent BSS (IBSS). An Extended Service Set (ESS) is formed when two or more APs are connected to the same local area network (LAN); hence, multiple BSSs are connected. Figure 1 illustrates the different Wi-Fi networks.

[1] There is a third mode, Personal Basic Service Set (PBSS). For the purpose of this paper, PBSS can be assumed to be the same as infrastructure BSS.

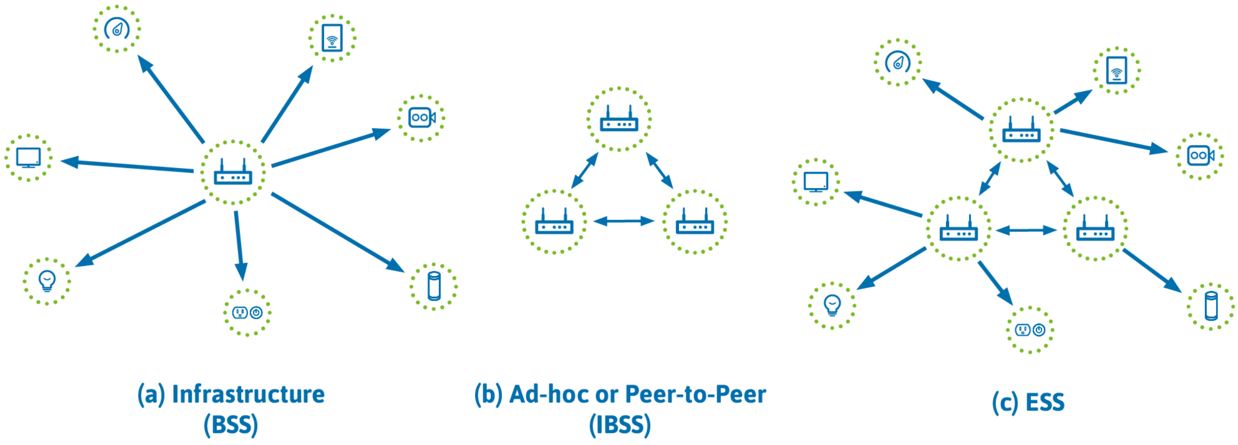


Figure 1. Wi-Fi Networks

Wi-Fi Sensing can be performed with any Wi-Fi device. It is simply an added capability that can be used on an available communication path. Each communication path between two devices provides the opportunity to extract information about the surrounding environment. The network topology and the role of each device places constraints on what devices are capable of communicating.

In addition to utilizing communication paths between multiple devices for sensing, it is also possible for a single device to use the reception of the Wi-Fi signals it has transmitted and collected. In such a case, the topology consists of a single client device and functions similarly to a monostatic RADAR system.

1.3.2 Environment Measurement Procedure

Wi-Fi sensing is based on the ability of the radio to estimate the wireless channel and surrounding environment. Since Wi-Fi networks are constructed of many devices located throughout a given geographical area, they are well suited to exploit transmissions from these devices to form a radar system. Depending on the number of devices, the radar system may be monostatic, bistatic or multistatic.

In monostatic Wi-Fi Sensing, a single device measures its own transmitted Wi-Fi signals. In bistatic Wi-Fi Sensing, the receiver and transmitter are two different devices (for instance, an AP and a STA in infrastructure mode). In multistatic Wi-Fi Sensing, the received signals from multiple Wi-Fi transmitters are used to learn about a shared environment.

At least one Wi-Fi transmitter and one Wi-Fi receiver are required to perform Wi-Fi Sensing measurements, and they may or may not be located in the same device. The measurement is always performed by a Wi-Fi Sensing-enabled receiver on the Wi-Fi signal transmitted by a transmitter, which may or may not originate from a Wi-Fi sensing-capable device. The device that transmits the signal that is used for measurements is called the “illuminator,” as its transmissions enable collection of information about the channel (in other words, it illuminates the channel).

Depending on what triggers the illuminator device to transmit a Wi-Fi signal, there are different modes of Wi-Fi Sensing measurements defined:

1) Passive
2) Triggered
    a. Invoked
    b. Pushed

In passive mode, Wi-Fi sensing utilizes transmissions as part of the regular Wi-Fi communication. The Wi-Fi Sensing receiver(s) rely only on transmissions between itself and the illuminator device. Passive transmissions do not introduce overhead; however, the Wi-Fi sensing device lacks control over the rate of transmissions, transmission characteristics (bandwidth, number of antennas, use of beamforming), or environmental measurements. An example of a passive transmission used for sensing is illustrated in Figure 2.

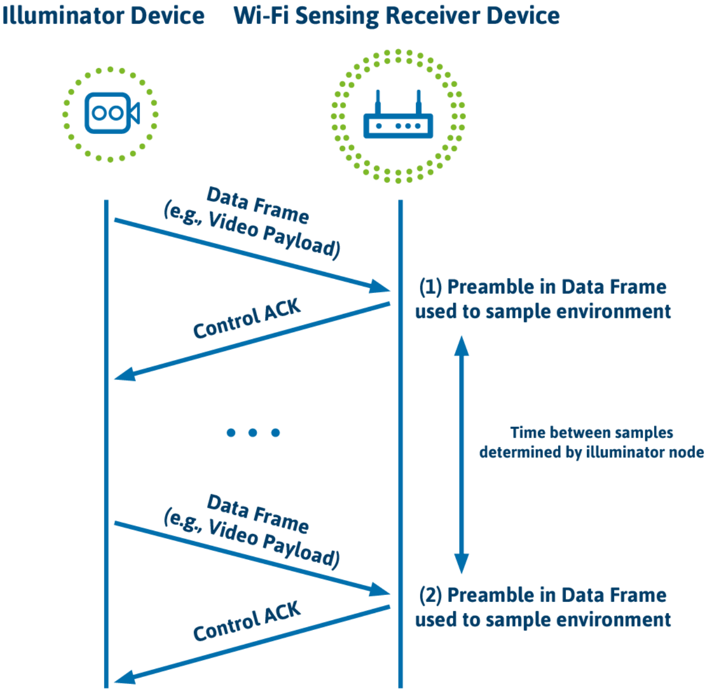

Illuminator Device
Wi-Fi Sensing Receiver Device
Data Frame (e.g., Video Payload)
(1) Preamble in Data Frame used to sample environment
Control ACK
Time between samples determined by illuminator node
Data Frame (e.g., Video Payload)
(2) Preamble in Data Frame used to sample environment
Control ACK

Figure 2. Passive Environment Measurement

A triggered measurement occurs when a Wi-Fi Sensing device is triggered to transmit a Wi-Fi packet for the purpose of Wi-Fi Sensing measurements, either in response to a received Wi-Fi packet or by the higher layers (for instance, in Wi-Fi Sensing software).

A measurement utilizing a packet transmission in response to a packet received from the Wi-Fi Sensing receiver device is an invoked measurement. An example of an exchange leading to an invoked measurement is depicted in Figure 3.

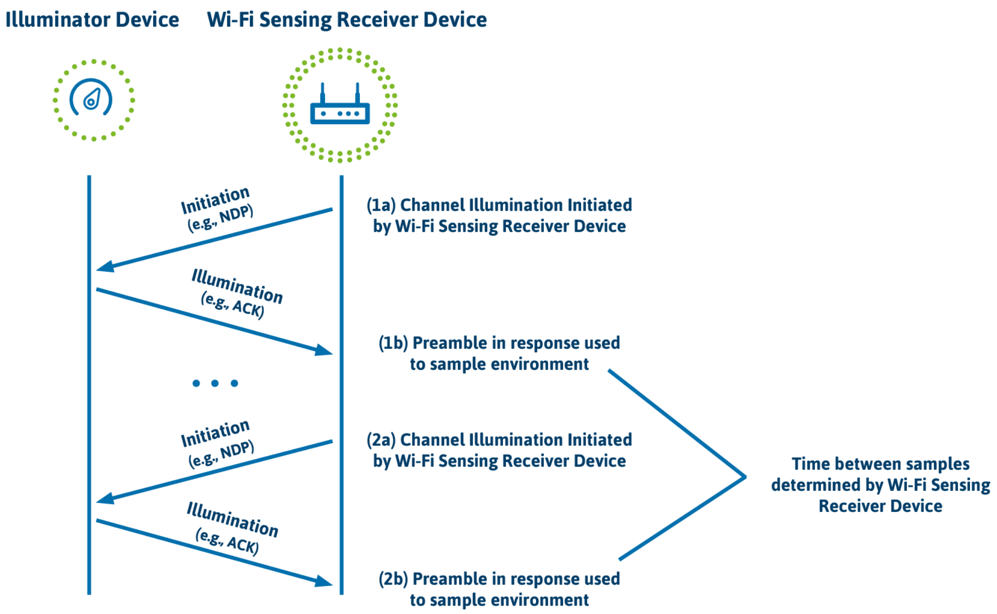

Illuminator Device
Wi-Fi Sensing Receiver Device
Initiation (e.g., NDP)
(1a) Channel Illumination Initiated by Wi-Fi Sensing Receiver Device
Illumination (e.g., ACK)
(1b) Preamble in response used to sample environment
• • •
Initiation (e.g., NDP)
(2a) Channel Illumination Initiated by Wi-Fi Sensing Receiver Device
Time between samples determined by Wi-Fi Sensing Receiver Device
Illumination (e.g., ACK)
(2b) Preamble in response used to sample environment

Figure 3. Invoked Environment Measurement

In pushed mode, a transmission is initiated by the illuminator device for measurement. A pushed transmission can be either a unicast or a multicast/broadcast message. Multicast/broadcast messages can be used for measurements by multiple Wi-Fi Sensing receivers simultaneously if the devices are not in power-save mode. Figure 4 depicts the pushed transmission.

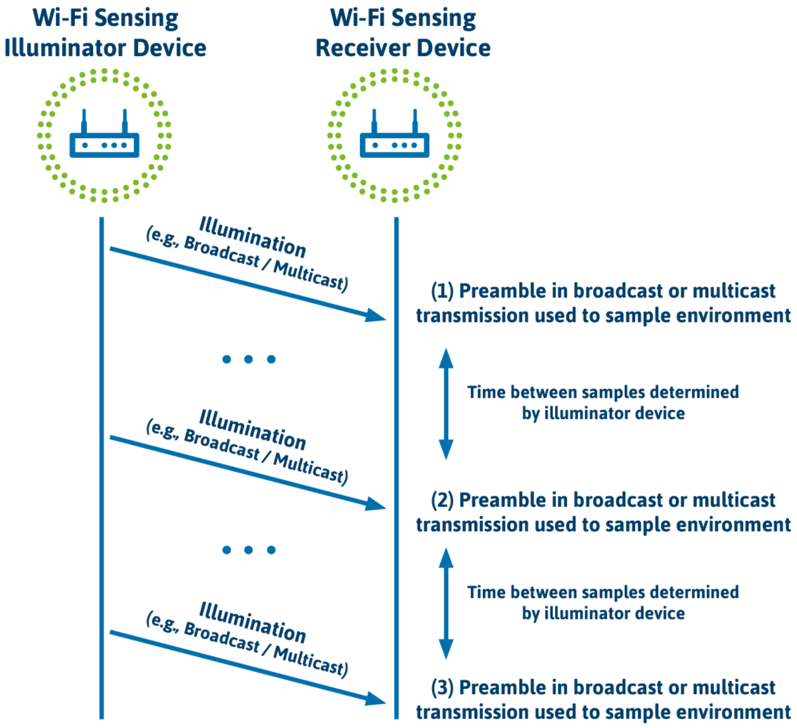

Wi-Fi Sensing Illuminator Device
Wi-Fi Sensing Receiver Device
Illumination (e.g., Broadcast / Multicast)
(1) Preamble in broadcast or multicast transmission used to sample environment
• • •
Time between samples determined by illuminator device
Illumination (e.g., Broadcast / Multicast)
(2) Preamble in broadcast or multicast transmission used to sample environment
• • •
Time between samples determined by illuminator device
Illumination (e.g., Broadcast / Multicast)
(3) Preamble in broadcast or multicast transmission used to sample environment

Figure 4. Pushed Environment Measurement

As opposed to passive transmissions, triggered transmissions introduce some overhead as additional over-the-air transmissions are required. Pushed transmissions introduce less overhead compared to invoked transmissions, because the exchange is unidirectional rather than bidirectional. Triggered transmissions allow for a system to control the rate and occurrence of measurements.

Without standards to support Wi-Fi Sensing, it is not possible to achieve coordination among a group of devices allowing for transmission characteristics to be synchronized between all Wi-Fi sensing receivers in the network.

1.3.3 Wi-Fi Sensing System

A Wi-Fi Sensing network is made up of one or more Wi-Fi Sensing illuminators and one or more Wi-Fi Sensing receivers. There are three main components that make up a Wi-Fi sensing system, present in Wi-Fi Sensing illuminators and receivers. The first component is the Wi-Fi radio, which encompasses the radio technology specified in IEEE 802.11 standards, the interfaces and the APIs connecting the radio to the higher layers. The second component is the Wi-Fi Sensing software agent and consists of a signal processing algorithm and interfaces.

The Wi-Fi Sensing agent interacts with the Wi-Fi environment and is capable of turning radio measurement data into motion or context-aware information. The final component is the application layer that operates on the Wi-Fi sensing output and forms the services or features, which ultimately are presented to the end user. Illustrated in Figure 5 is an overview of a typical Wi-Fi Sensing system. The new Wi-Fi Sensing components will act in conjunction with existing Wi-Fi services, such as MLME and data communication.

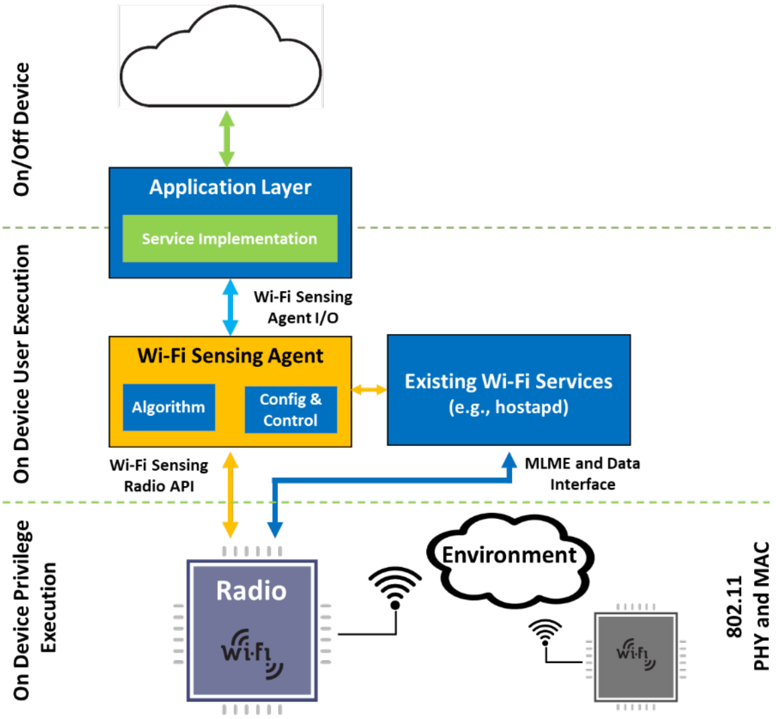


Figure 5. Wi-Fi Sensing System Diagram

1.3.3.1 Wi-Fi Radio

A Wi-Fi sensing system can be built upon existing Wi-Fi standards, hardware, software and infrastructure. Wi-Fi has evolved to include a wide range of operating frequencies, bandwidths, modulation schemes and features. Much work has been made to ensure interoperability and backward compatibility for the technology evolution. As a result, there is a large set of options available to support Wi-Fi sensing in existing hardware and systems.

The fundamental component required to enable Wi-Fi sensing on the radio is the interface to enable control and extraction of periodic channel or environmental measurement data. Implementation of such an interface requires the support of chipset vendors and access to the firmware and drivers. Low-level facilities from the operating system may also be needed to allow application interaction in a standardized way.

Regardless of device type, operating band or Wi-Fi generation, the core APIs to enable Wi-Fi sensing are similar, as the required data and control is common. A standardized Wi-Fi sensing radio API is required to interface with the Wi-Fi Sensing agent. More details of this API and interface are described in section 5.3 - Wi-Fi Sensing Radio API Requirements. Wi-Fi sensing capabilities may be distinguished at a higher level, as different algorithms or services will be tied to frequency band or PHY type.

1.3.3.2 Wi-Fi Sensing Agent

The Wi-Fi Sensing Agent can reside on any Wi-Fi device; for example, in the infrastructure mode, the agent may reside on the AP, in which case channel measurements from all the STAs associated with the AP can be collected. The software agent may also be located on a STA. In ad-hoc mode, since any device may communicate with any other device, the software agent can be placed on any, or all peers.

The Wi-Fi Sensing Agent is expected to be a user privileged application, which makes use of the Wi-Fi sensing radio APIs to interact with the Wi-Fi radio. These APIs enable extraction of desired channel environment measurement information, as well as provide the ability to assert any related controls to configure Wi-Fi sensing features.

There are two main subsystems within a Wi-Fi Sensing Agent, one consisting of Configuration and Control, and a second consisting of a Sensing Algorithm. The Configuration and Control subsystem interact with the radio, using a standard set of APIs. Some tasks performed by the Configuration and Control subsystem include sensing capability identification, Pushed illumination coordination, and radio measurement configuration. The algorithm subsystem includes intelligence needed to extract the desired features out of the radio measurement data and may be different based on the desired sensing application.

The Wi-Fi Sensing agent is required on a sensing receiver; however, it is optional on an illuminator. If it is included on an illuminator, only the configuration and control subsystem is needed. By having the agent on the illuminator, additional enhancements are enabled, including sensing capability identification and coordinated pushed illumination. If the illuminator is not running an agent, it is still technically able to participate in the sensing network; however, only the most basic features that currently exist in Wi-Fi standards will be supported.

The Wi-Fi Sensing agent processes and analyzes the channel measurement information and makes sensing decisions, such as detecting motions or gestures. This information is then shared with the application layer via the Wi-Fi Sensing agent I/O interface.

In addition to interfacing with the radio and the application layer, the Wi-Fi Sensing agent also interfaces with the existing Wi-Fi services on the system. This interface is necessary for the agent to provide feedback for sensing optimizations that can be used in radio resource management decisions, such as band steering or AP selection requests.

1.3.3.3 Application Layer

The application layer of a Wi-Fi sensing system creates the sensing service and presents the information to the end user. This layer provides an opportunity for different participants to define and create sensing-based services derived from the expected use case.

The application layer may reside on any networked device, but it usually resides on the same device as the Wi-Fi Sensing agent. The application layer receives input from one or multiple Wi-Fi sensing software agents. It combines or fuses the information and delivers it to the end user. For example, in the home security use case, the software agent provides motion and location information to the application layer, which may send it to a cloud service. The cloud service can then be used as a data source for a mobile application, allowing end users to receive real-time event notifications or view historical data.

2 Use Cases

In this section, the three most common Wi-Fi deployment environments (i.e., home, enterprise, and personal networks) are briefly described, then example Wi-Fi Sensing use cases for these deployment environments are provided. Finally, a description of the deployment requirements for Wi-Fi Sensing are described.

2.1 Wi-Fi Sensing Deployment Environments

2.1.1 Home Deployment

A typical Wi-Fi home network follows one of two common deployment scenarios. The first consists of a single AP that serves as the internet gateway for all the devices in the house. The second consists of multiple APs forming an ESS and extending coverage throughout the home. More details relating to home networks is described in [11]. Examples of the two deployment scenarios are shown in Figure 6; depending on the use case, the Wi-Fi Sensing receiver may be the AP and/or other devices in the network. Not all the devices in a home deployment need to be Wi-Fi Sensing capable.

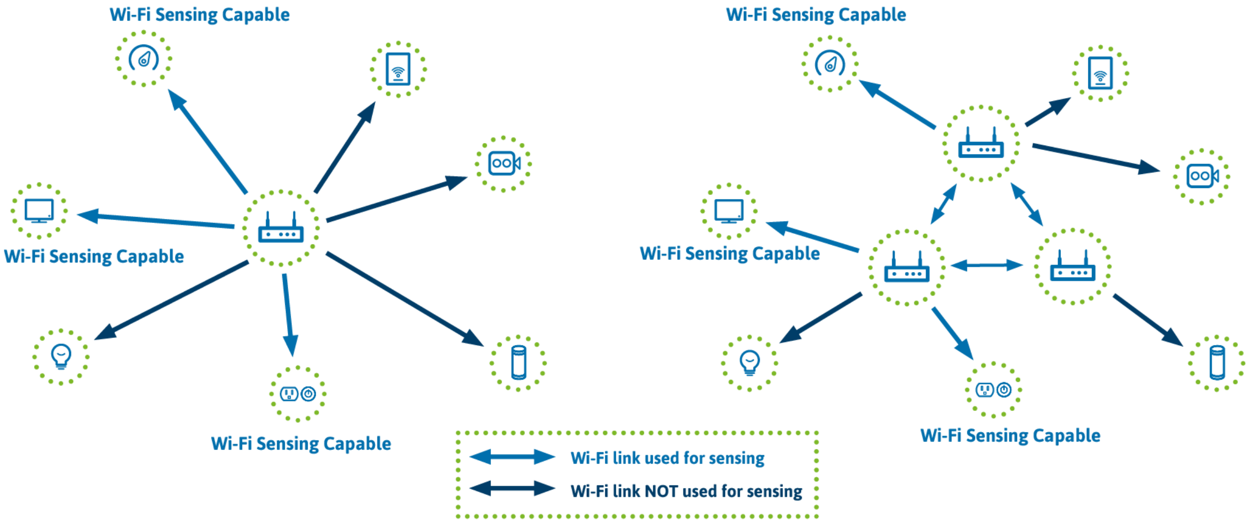


Figure 6. Example Home Wi-Fi Sensing Deployments

2.1.2 Enterprise Deployment

An enterprise Wi-Fi network, as opposed to a home network, consists of many APs and may operate in an extremely dense environment. In most cases, to ensure over-the-air efficiency, the APs are each connected to an Ethernet backhaul connection. If the backhaul connection is wireless, one radio, or frequency band, is used as a dedicated Wi-Fi backhaul connection. A typical enterprise deployment is shown in Figure 7.

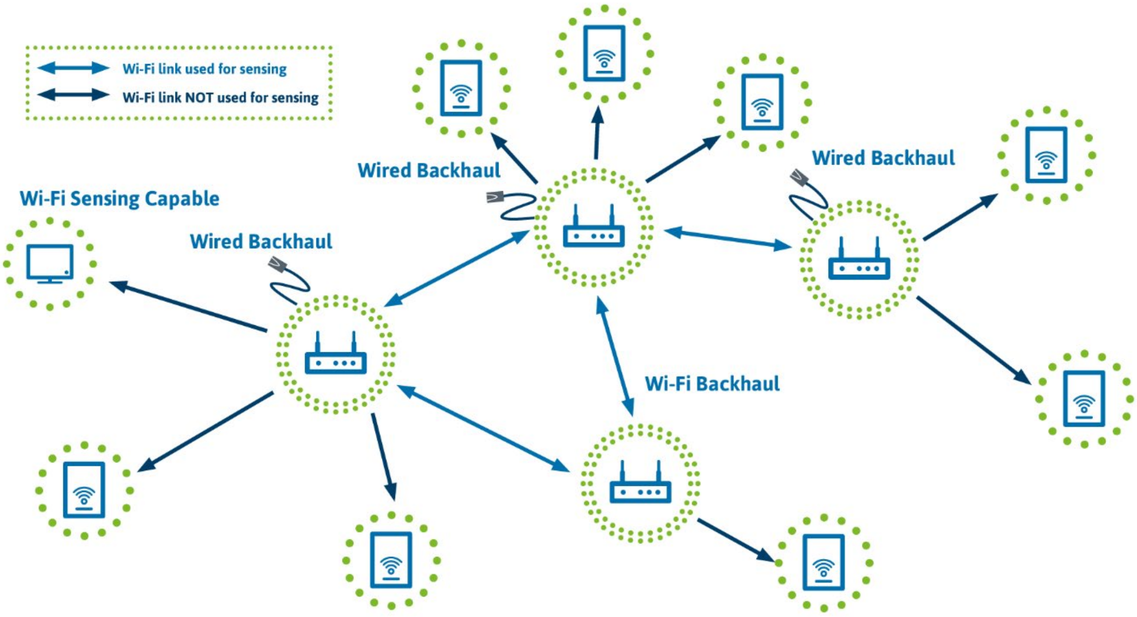


Figure 7. Enterprise Deployment Topology

Because enterprise and public Wi-Fi networks support many consumer devices that consistently join and leave the network, it may be more efficient for the Wi-Fi sensing network to utilize APs within communication range for sensing purposes.

Similar to home deployments, not all devices in the network are necessarily Wi-Fi Sensing capable. Coordination among the APs is required for performing measurements, collecting and processing data.

2.1.3 Personal Device Deployment

Personal area networks consist of a set of personal devices (e.g., PC, smartphone, smartwatch, AR/VR goggles) located in vicinity of one another communicating in a peer-to-peer fashion. One or more of the devices may also be connected to an AP and serve as a soft AP for the other devices. Shown in Figure 8 is a depiction of an example personal network.

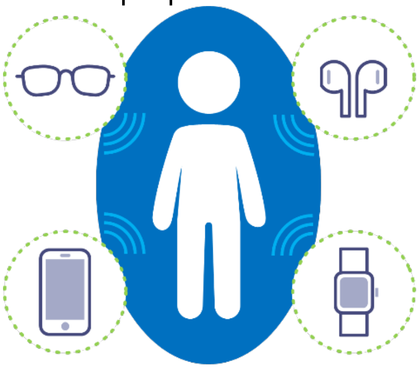


Figure 8. Personal Area Network Deployment

The Wi-Fi Sensing receiver in this case is usually the device with the most processing power, such as a PC or smartphone. It utilizes the transmissions from the AP and the devices in the personal area network for sensing measurements. It is possible that only one device participates in the sensing with simultaneous transmission and reception in a monostatic fashion.

2.2 Wi-Fi Sensing Applications

The following sections describe some example use cases applicable to different deployment environments described in Section 2.1.

2.2.1 Home Monitoring

In home monitoring use cases, the existing Wi-Fi home network is used to gain insight into what is happening in the home when the residents are away. In the simplest case, Wi-Fi Sensing can be used to detect motion in the house. Additionally, the system may need the a level of localization to ascertain when and where motion has occurred. An example is shown in Figure 8, illustrating where mobile alerts are sent to a homeowner.

Likely participants:

1) End consumers installing a DIY home security system
2) Existing security providers augmenting their systems with a new sensor
3) Hardware OEMs providing home monitoring services to customers
4) Network providers offering home monitoring services to customers

The home monitoring use case is an add-on feature for an existing in-home Wi-Fi network, working in conjunction with the Wi-Fi devices a home user may have connected. As described in Section 2.1.1, the devices in the network are not required to operate any differently, and the impact of enabling this use case on network performance should be minimal.

While this use case is primarily targeted for residential and home deployments, similar use cases can apply to enterprise or commercial deployments.

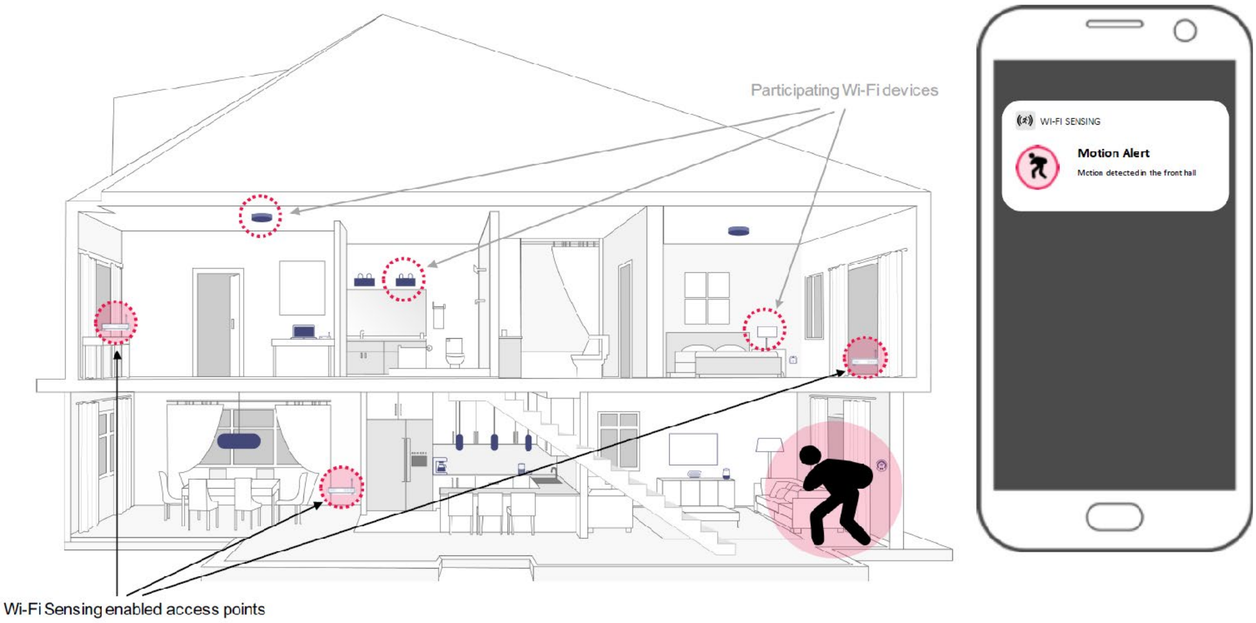

Participating Wi-Fi devices
Wi-Fi Sensing enabled access points
WI-FI SENSING
Motion Alert
Motion detected in the front hall

Figure 9. Home Monitoring Application

Requirements:

1) Detection of large-scale motion (~1m) inside home
2) Differentiation among human vs other motion, including mechanical motions and pets
3) Localization of the motion to a room or an area in the house/building

2.2.2 Energy Management

There are sensors on the market, such as passive-infrared (PIR) sensors, capable of providing environmental control feedback. However, these sensors require line-of-sight connectivity and dedicated installations. By using Wi-Fi sensing, the same feedback can be produced using existing Wi-Fi networks, eliminating the need to build and maintain multiple systems.

Likely participants:

1) Consumers building a DIY home automation system using IoT devices
2) Existing building automation systems utilizing a new sensor
3) Enterprise OEMs providing energy management-related services to customers
4) Network providers offering building/outdoor automation-related services

The energy management use case primarily targets enterprise deployments; however, it can deployed in a home network, as shown in Figure 10.

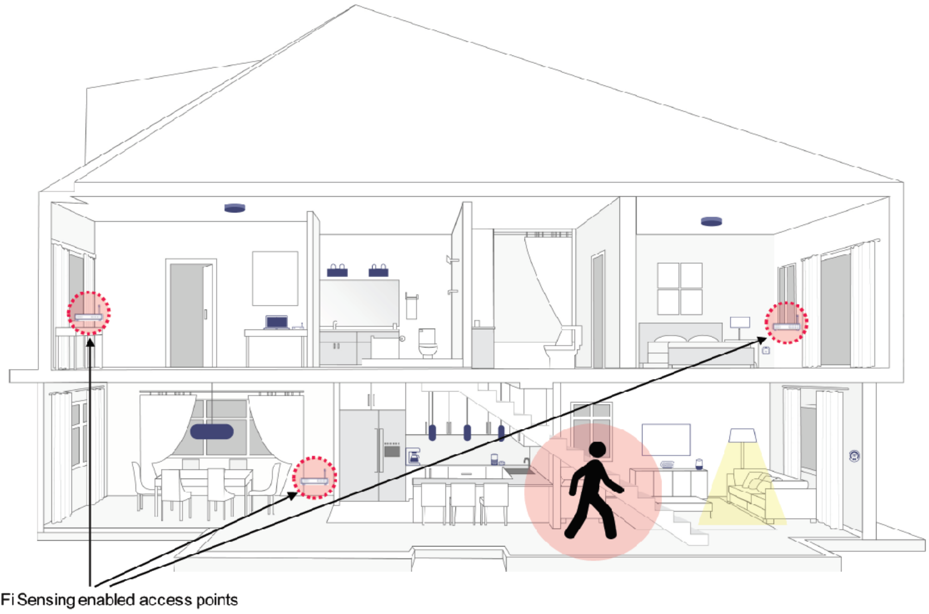


Figure 10. Energy Management Application

Requirements:

1) Detection of large-scale motion (~1m) in an area, such as a room, a large area within a building, the home/building or an outdoor space
2) Detection of number of people within an area
3) Localization of the motion and/or number of people present within an area

2.2.3 Elder Care

Elder Care is a use case in which an existing Wi-Fi home network can be used to address concerns related to caring for the aging population. Many different services in this area are gaining popularity, utilizing technology to allow the aging population to maintain an independent lifestyle, enabling family members and/or caregivers to be notified when there is a need. It is important to ensure these services protect the privacy of the elderly, while also performing autonomously from them. For instance, notifications can be pushed to care providers, as shown in Figure 11.

Likely participants:

1) End consumers installing a DIY elder care monitoring system
2) Existing elder care providers augmenting their systems with a new sensor
3) Hardware OEMs providing elder care-related services to customers
4) Network providers offering elder care monitoring-related services to customers

The elder care use case primarily targets home deployments; however, it also is suitable for deployment in hospitals and elderly care facilities.

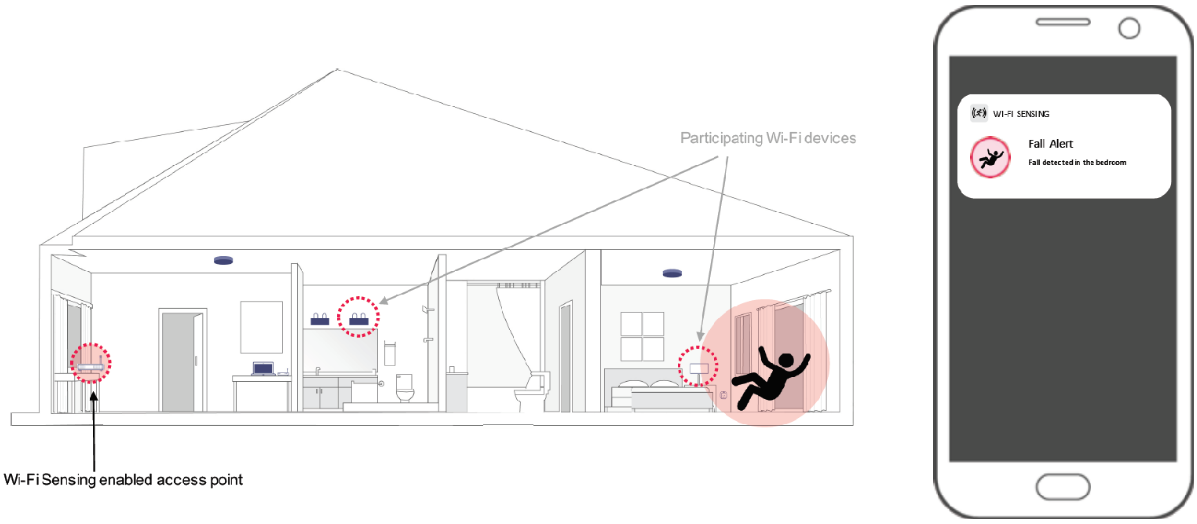

Participating Wi-Fi devices
Wi-Fi Sensing enabled access point
WI-FI SENSING
Fall Alert
Fall detected in the bedroom

Figure 11. Elder Care Application

Requirements:

1) Detection of specific large-scale motion (~1m) patterns, e.g., a fall, in a large area
   - A room, home/building or outdoor space
2) Localization of the motion in a room or an area within the house/building

2.2.4 Remote Operator Troubleshooting

Operator-managed Wi-Fi is gaining market adoption [2][3]. By fusing Wi-Fi Sensing output (such as localized presence detection), operators can help direct troubleshooting efforts, especially when correlated with other captured key performance indicators (KPIs). With multiple APs becoming more common, inter-AP roaming issues could be identified by combining association data with Sensing information. Such data may be obtained as shown in Figure 12.

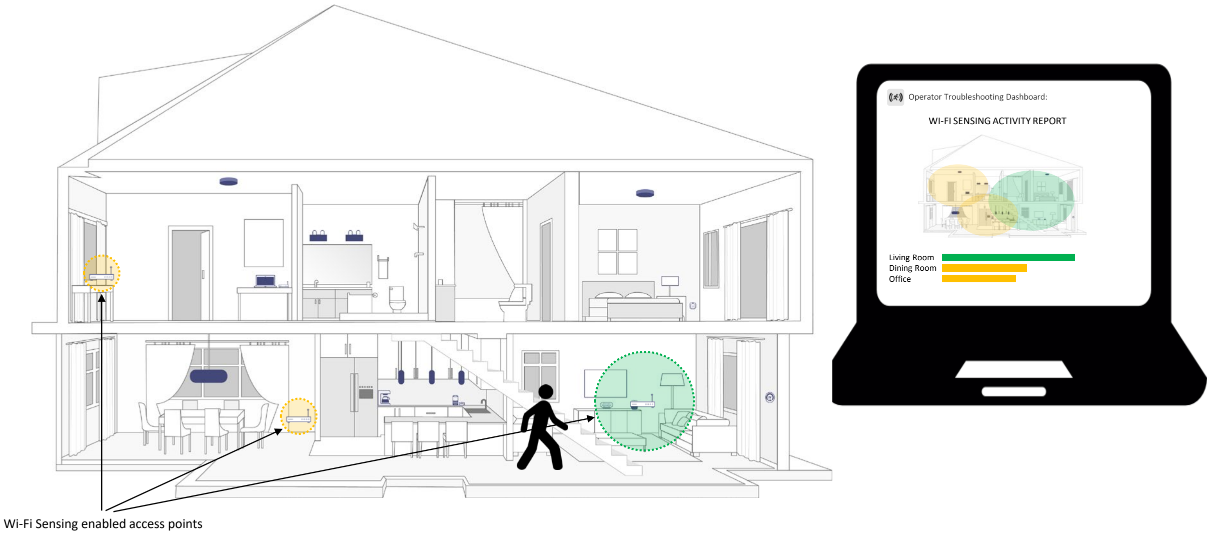

Operator Troubleshooting Dashboard:
WI-FI SENSING ACTIVITY REPORT
Living Room
Dining Room
Office
Wi-Fi Sensing enabled access points

Figure 12. Remote Operator Trouble Shooting Application

Likely participants:

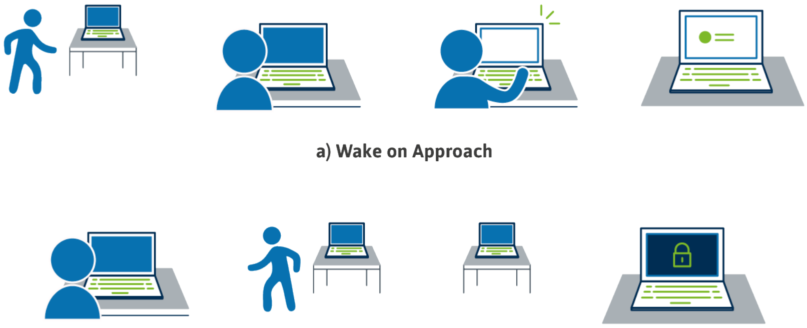
1) Network providers managing operator-supplied APs
2) Customers paying for managed Wi-Fi

Requirements:

1) Localization of the motion to a room or an area in the house/building

2.2.5 Wake-On-Approach / Lock-On-Walk-Away

In the wake-on-user approach use case, consumer electronics devices – including computers, smart monitors and TVs – switch from standby and/or power-save mode upon detecting an approaching user. Similarly, in the lock-on-walk-away use case, detection of a user leaving a device triggers the switch to power-save mode and/or locking of the device. Wi-Fi Sensing can be used to monitor and detect proximity of a user to the device. Alternative approaches rely on use of additional sensors; however, with Wi-Fi Sensing, an existing radio on the device would be used. An example of such is illustrated in Figure 13.



a) Wake on Approach

b) Lock on Walk-Away

Figure 13. Wake-on-approach / Lock-on-walk-away Application

Likely participants:

1) Consumer electronics OEMs providing new value-add features
2) Network providers enabling new security services

The walk-on-approach and lock-on-walk-away use cases primarily target enterprise deployments; however, it can also be deployed in home environments.

Requirements:

1) Detection of proximity of a human to a specific device

2.2.6 Gesture Recognition

In the gesture recognition use case, specific gestures made by the users are used to interact with the device. The gestures can be small-scale gestures made by fingers and hands, larger-scale facial gestures or whole-body poses. Wi-Fi Sensing can be used to detect specific gestures without use of cameras or alternative sensors, reducing cost and increasing privacy. An example is shown in Figure 14.

Figure 14. Gesture Recognition Application

Likely participants:

1) Users utilizing gesture to interact with personal devices
2) Consumer electronics OEMs providing value-add features of gesture recognition for enhanced quality of experience (QoE) and ease of use

The gesture recognition use case primarily targets personal device deployments.

Requirements:

1) Detection of gesture
   - Small-scale finger/hand gestures, larger-scale body poses

2.2.7 Biometric

High-resolution sensing can be utilized to measure physiological and behavioral data for security and medical applications. Biometric data measurements include heartbeat and respiration rates. This information can be used for monitoring patients in a noninvasive and passive manner, as shown in Figure 15. Additionally, high-resolution sensing has security applications, such as in the case of polygraphs.

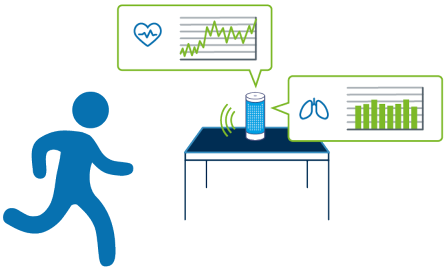


Figure 15. Biometric Application

Likely participants:

1) Patients requiring passive monitoring
2) Healthcare providers
3) Security and law enforcement agencies
4) Healthcare or security device manufacturers

The biometric use case primarily targets personal device deployments, however it may be suitable for home and enterprise deployments, as well.

Requirements:

1) Extremely high-resolution detection of body movement, such as chest movements while breathing

2.3 Wi-Fi Sensing Deployment Requirements

2.3.1 Underlying Wi-Fi Network And Network Management

Wi-Fi Sensing can be deployed in all types of Wi-Fi networks and topologies, operating in different frequency bands (2.4, 5, 6, and 60 GHz) and different bandwidths. The sensing resolution and performance depends on the use case requirements. In general, it is enhanced with the increase in the number of participating devices and higher bandwidths. Applications that require lower resolutions and longer range, such as home monitoring, can be deployed using Wi-Fi networks operating in 2.4GHz and 5GHz. Applications that require higher resolutions and lower range, such as gesture recognition, require 60GHz Wi-Fi networks.

In multi-AP and/or multi-band deployments, there may be an advantage to having a Wi-Fi sensing device connected to a specific AP or operating in a specific frequency band. Radio resource management (RRM) events, such as AP and/or band steering, should be conducted in coordination with the Wi-Fi Sensing agent/operation.

2.3.2 Participating Devices

The devices involved with Wi-Fi Sensing will depend upon the deployment environment and the specific use case. The sensing measurements also need to be processed by the device with enough computation power. The coordination of sensing, including participating devices, is a role befitting the AP when present.

At any time, the user should be able to add additional Wi-Fi sensing capable devices to the network to enhance accuracy, coverage and/or localization. These additional devices do not necessarily need to be Wi-Fi Sensing capable or dedicated Wi-Fi sensing devices to participate; however, they should identify their Wi-Fi sensing capabilities and supported features to the AP. It is expected that any Wi-Fi device, including various IoT devices, can participate in Wi-Fi sensing in addition to their expected function. Some examples for home deployments include a Wi-Fi controllable plug, light bulb or thermostat. However, even when a device connects to the AP and reports that it is Wi-Fi sensing capable, the Wi-Fi Sensing agent may elect not to make use of that device.

2.3.3 Wi-Fi Sensing Operation

Given that Wi-Fi Sensing is an add-on feature operating within an existing Wi-Fi network, performance degradation due to airtime usage and sensing overhead must be minimized. To ensure this happens, Wi-Fi transactions required for conducting sensing measurements and sensing management and processing must be optimized for efficiency.

For each Wi-Fi Sensing application, there is at least one network device executing the sensing software, or Wi-Fi Sensing Agent. The Wi-Fi Sensing agent is typically placed on the AP; however, it can be placed on any STA.

Following authentication and association of a device with the Wi-Fi network, the Wi-Fi Sensing agent should discover the device and its sensing capabilities. Depending the capabilities of the device, its role in the Wi-Fi sensing network would be determined. If the new device is another Wi-Fi Sensing-capable AP, then coordination among the agents is required.

The Wi-Fi Sensing agent shall have a mechanism to determine which devices are capable and should participate in the sensing for each application on a device-specific basis.

A Wi-Fi Sensing agent should also be capable of configuring the radio for measurements and triggering transmissions on a periodic basis for sensing measurements. It should also be able to enable/disable measurements or adjust configuration parameters for Wi-Fi sensing-capable devices. The Wi-Fi Sensing agent may also be able to request specific radio resource management operations, such as AP or band steering.

The Wi-Fi Sensing agent should be able to detect and process specific sensing events and communicate the information to the application layer for specific handling and user presentation.

Finally, the Wi-Fi Sensing agent should be considerate of the limited resources available on the device on which it operates. If the agent is running on an AP, it may have limited processing resources that need to be shared with the primary application. It should also assume limited broadband network resources, as sensing operations should require a minimal broadband footprint.

3 Business Opportunities

Wi-Fi Sensing and its motion detection capabilities create many business opportunities, with two major factors to consider.

The first is that smart homes trend are increasing in popularity. Recent market research shows that the average household now features 10.4 connected IoT devices, including entertainment devices and voice assistants, with the overarching goal of making everyday life easier through technology [4].

The second factor is the availability of technology. Wi-Fi chipset vendors are beginning to make different radio measurement information available, which is the cornerstone for enabling Wi-Fi Sensing [5][6]. This information is then processed by intelligent algorithms, capable of turning a Wi-Fi network into an advanced sensor [7]. Several opportunities created from these capabilities are highlighted below.

Security

Motion detection and home security are obvious uses for Wi-Fi Sensing, and there are many potential business models that can be explored. Adding Wi-Fi Sensing features to any existing network can be accomplished with only a software or firmware upgrade on the AP, requiring virtually no overhead to deploy.

New companies looking to enter the home security market can build security services around Wi-Fi Sensing or use it to enhance existing systems. An Internet service provider (ISP) now has the ability to add or bundle security services as part of its offerings. Service providers can add new features and services, increasing network value for new and existing customers, while reducing and rthe likelihood of churn for existing customers [5].

Energy and Resource Management

The usage of existing Wi-Fi infrastructure deployments presents another opportunity to optimize building management systems. A building manager or network provider can leverage existing Wi-Fi infrastructure already deployed and use it in conjunction with other IoT devices to become more interactive and optimize energy and resources using only a single system.

Healthcare

For healthcare service providers, Wi-Fi sensing provides wellness monitoring with numerous benefitscompared to use of cameras, including privacy, affordability, ease of installation and expanded coverage.

There exists a large untapped opportunity in the elder care market, as aging generations become increasingly comfortable with technology [9]. To leverage this trend, many companies are introducing new technology to help people maintain an independent lifestyle as they age [10], [11], [12], [13], [14]. Healthcare service providers are beginning to offer noninvasive home monitoring systems to track subscriber behavior, detect nonconformities, anticipate expected patterns and even detect serious issues, such as slips and falls.

Network Service Providers

Network owners, service providers and operators benefit from Wi-Fi Sensing by having accurate location information about a user's proximity to APs or other Wi-Fi devices. This can be helpful for troubleshooting, such as improving network performance or optimizing AP placement.

Consumer Device & IoT

Utilizing new mm-wave Wi-Fi technologies to sense small movements, such as hand gestures or finger movements, will enable many new innovative ways for people to interact with consumer devices. An example of industry trends moving in this direction is the new motion-sensing features announced by Google, expected to be released in its latest Pixel 4 smartphone [15]. Utilizing existing Wi-Fi hardware and components for such capabilities provides a cost-effective solution, as no additional hardware is required.

4 Wi-Fi Sensing Performance

4.1 Parameters Impacting Wi-Fi Sensing Performance

Wi-Fi Sensing performance depends on a variety of parameters, most of which impact the performance of the Wi-Fi network, as well. These parameters are described in this section.

4.1.1 Interference

One of the parameters that impacts the quality of the received signal in a wireless network is the amount of interference present. Interference can be caused by other Wi-Fi devices operating in the same band, which causes cochannel interference, or in an adjacent channel, which causes adjacent channel interference. It can also be caused by non-W-Fi devices, which can be other communication systems or unintentional transmissions that create electromagnetic noise in the band.

Interference can impact Wi-Fi Sensing performance in two ways. First, it may interfere with the sensing transmissions and thereby reduce the number of measurements made in a given time interval. As such, it introduces jitter in time instants during which the measurements are made.

Second, channel-state measurements may capture the impact of transient interference, such as for a non-Wi-Fi device, as opposed to motion in the environment.

Wireless systems deploy various techniques and guidelines to avoid and/or minimize the impact of interference [16]. The same techniques will help improve the performance of Wi-Fi Sensing. These techniques aim at maximizing the reuse of spectrum, while minimizing the overlap of spectrum used by nearby networks. Some of these techniques include Dynamic Channel Allocation (DCA); Auto Channel Selection (ACS); optimized RF planning; (e.g., non-overlapping channels and use of reduced channel width when applicable), and power control.

4.1.2 Coverage And Signal Strength

One of the parameters that impacts the quality of a Wi-Fi network is network coverage and the received signal strength throughout the network. Similarly, the performance of a Wi-Fi Sensing network is impacted by its coverage and the received signal strength. For many use cases, it is important that the Wi-Fi network sufficiently covers the full target environment. Additionally, the strength of the signals received impacts the Wi-Fi sensing performance, as the quality of the channel state measurements depend upon the signal strength.

4.1.3 Channel Bandwidth

The channel bandwidth of the sensing transmissions impacts the spatial resolution of Wi-Fi Sensing. The larger the bandwidth, the higher the resolution. In 2.4GHz and 5GHz bands, the bandwidths larger than 20MHz (up to 160MHz in 5GHz) are available via channel bonding. In 60GHz, the channel bandwidth is in excess of 2 GHz, which results in much higher achievable resolution.

4.1.4 Resource Availability

Resource availability refers to the resources required by the Wi-Fi Sensing system to make reliable and scheduled channel measurements. As Wi-Fi resources become depleted, such as under heavy load scenarios, the measurement rate may degrade and produce unwanted behaviors, such as misses or false alarms.

4.1.5 Number Of Sensing Illuminators

An increased number of illuminators may result in a higher sensing performance in three different ways. First, with more transmitters that are located sufficiently apart from one another, motion in a larger area can be detected. Second, when motion is detected using transmissions on one or more transmitters, information is provided that can be used to determine localization of the motion. Third, sensing accuracy is improved with a higher number of measurements taken across a larger number of transmitters in most scenarios.

4.2 Wi-Fi Sensing Performance Metrics

Wi-Fi Sensing performance can be measured using different parameters that are described in this section. Not all of the parameters are applicable to all the use cases; different parameters become more important in measuring the performance of Wi-Fi Sensing in different applications.

4.2.1 Sensing Reliability

Wi-Fi Sensing reliability is measured in the form of probabilities of hits, misses, false alarms and correct rejections:

- **Probability of hits** is the probability of correct detection of a motion/gesture/event of interest when it occurs
- **Probability of misses** is the probability of no detection of a motion/gesture/event of interest when it occurs

- **Probability of false alarms** is the probability of detection of a motion/gesture/event when there is either no motion/gesture/event, or the event was not one of interest; for example, human presence detection when there is a pet moving in the house
- **Probability of correct rejections** is the probability of correct detection of no motion/gesture/event of interest when there is either no motion/gesture/event or not the event of interest; for example, a pet moving in the house is not identified as human presence

The higher the probability of hits and correct rejections and the lower the probability of misses and false alarms indicates a higher Wi-Fi Sensing accuracy.

Sensing reliability is not only dependent on Wi-Fi Sensing capabilities at the radio level, but also the techniques utilized at the higher layers for interpretation of changes in wireless channel, as detected by the radio. The reliability of Wi-Fi sensing at the radio level is impacted by the parameters listed in Section 4.1.

4.2.2 Sensing Resolution

Sensing resolution specifies the scale of the detectable motion. For example, sensing resolution defines whether the Wi-Fi Sensing system is capable of detecting small size movements, such as movement of a hand, or larger scale movements, such as a person walking. Another metric used in measuring Wi-Fi Sensing resolution is the number of targets that can be detected; for example, whether there is one person or multiple people moving in an area.

The parameter that most impacts the sensing resolution is channel bandwidth, as described in Section 4.1.3.
While the higher sensing resolution enhances the performance of all applications, very high resolution is a critical requirement for gesture recognition (section 2.2.6) and biometric (section 2.2.7) use cases; thus, it is required for mm-wave systems.

4.2.3 Sensing Range & Coverage

Sensing range and coverage is a measure of the area within which an event of interest is detected. The coverage of a sensing system depends on similar factors to those that impact the Wi-Fi coverage, including transmission power and frequency band. Larger sensing range and coverage is required for applications that cover a large sensing area, such as in-home monitoring (section 2.2.1).

4.2.4 Sensing Latency

The time duration between when an event of interest occurs and when the event is detected is sensing latency. Sensing latency depends upon multiple factors, including frequency of measurements. Low sensing latency is a requirement for time-sensitive applications, such as elder care (section 2.2.3) and biometric (section 2.2.7) use cases.

4.2.5 Airtime Efficiency

Wi-Fi Sensing is expected to be an additional service provided over and above the regular operation of a Wi-Fi network, i.e., communication of Wi-Fi devices. Hence, it is important that the overhead resulting from sensing applications is minimal and does not negatively impact the performance of the Wi-Fi network, typically measured by throughput and latency experienced by Wi-Fi devices.

Airtime efficiency is a measure of the overhead associated with Wi-Fi Sensing's use of over-the-air resources. In the extreme case that there are no additional transmissions introduced for conducting

Wi-Fi sensing measurements, there is no overhead, and the airtime efficiency is maximum. However, in many scenarios, there is a need for additional messages to enable the use case. Careful design of Wi-Fi sensing protocol and message exchanges is required to ensure minimal impact to Wi-Fi network performance.

4.2.6 Noise Rejection

Noise rejection is the ability for the sensing system to operate in a “noisy” environment but still maintain a high sensing performance. Noise may occur in the form of spectrum measurement error as the result of thermal noise, frequency phase noise, limited dynamic range or other non-linear system effects. Noise may also occur in the form of environmental noise, such as movement of background objects within the sensor range, but not contributing to the motion/gesture/event of interest.

5 Wi-Fi Technology Requirements

This section provides detailed information on the technology requirements to enable a Wi-Fi Sensing system, as described in section 1.3.

5.1 PHY Layer Requirements

The PHY layer is responsible for performing the physical measurements for sensing the environment. The measurements required to enable Wi-Fi Sensing to occur on the Wi-Fi receiver side. Given a transmission from another STA, the receiver is required to compute a channel estimation and make the results available to the higher layers. The specific measurements and mechanisms for channel estimation depend upon the specific PHY deployed by the Wi-Fi system.

5.1.1 OFDM-Based PHY

The OFDM-based PHY was first defined in IEEE 802.11a standard in 1999 [18] for operation in 5GHz band. Many standards following 802.11a used OFDM-based PHYs, including 802.11g/n/ac (OFDM), 802.11ax (OFDMA) operating in 2.4, 5 and/or 6GHz and 802.11ah/af operating in sub 1 GHz and 802.11ay operating in 60GHz.

This section provides a more detailed description of OFDM-based PHYs operating in 5GHz and how the channel estimation can be utilized for Wi-Fi Sensing. While a similar principle applies to other OFDM-based PHYs, channel bandwidth and the number of OFDM subcarriers impact the accuracy of the channel estimation. For example, the IEEE 802.11ah standard [22], operating in sub-1GHz, supports 1, 2, 4, 8 and 16MHz bandwidths, which results in much lower achievable resolution as compared to 20MHz and larger channel bandwidths available in 2.4 and 5GHz bands. On the other hand, IEEE 802.11ay operating in 60GHz band can achieve very high resolutions due to the channel bandwidth in excess of 2GHz.

The newer OFDM-based PHYs defined following 802.11a, for operation in 5GHz band, are High Throughput (HT) PHY (IEEE 802.11n [1]), Very High Throughput (VHT) PHY (IEEE 802.11ac [19]) and High-Efficiency (HE) PHY (IEEE 802.11ax [20], [21]).

In IEEE 802.11a-1999, each transmission was limited to a 20MHz channel bandwidth. Within the 20MHz channel, there are 64 evenly spaced subcarriers (312.5 kHz); however, only 52 are used. The OFDM frame format consists of a preamble, header, data and tail.

The IEEE 802.11a preamble is important for Wi-Fi Sensing. The preamble contains a short training field (STF), a guard interval and a long training field (LTF). The STF is used for signal detection, automatic gain control (AGC), coarse frequency adjustment and timing synchronization. The LTF is used for fine frequency adjustment and channel estimation. Since only 52 subcarriers are present, the channel estimation will consist of 52 frequency points.

Newer OFDM PHY versions (HT/VHT/HE) maintain the IEEE 802.11a preamble for backward compatibility and refer to it as the legacy preamble. The legacy preamble spans a 20MHz bandwidth and consists of a legacy STF (L-STF) and legacy LTF (L-LTF), as illustrated in Figure 16.

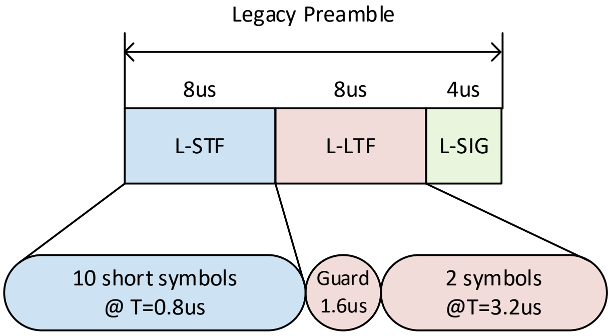


Figure 16. Legacy OFDM PPDU Preamble

As more recently defined OFDM PHY versions (HT/VHT/HE) introduce wider channel bandwidths (up to 160MHz) for backward compatibility, the legacy preamble is duplicated on each 20MHz channel. This allows the receiver to compute 52, 104, 208 or 416 valid L-LTF frequency points, which represent the channel estimation between the two devices.

Also useful for Wi-Fi Sensing are the MIMO training fields present in HT, VHT and HE LTFs, as shown in Figure 18. The MIMO fields are modulated using the full bandwidth (20MHz to 160MHz) and are traditionally used by the receiver to estimate the mapping between the constellation outputs and the receive chains. Since these fields span the full bandwidth, they provide more frequency points. For example, a 20MHz L-LTF contains 52 subcarriers, while a 20MHz HT/VHT-LTF contains 56 subcarriers.

In Appendix A, example measurements are shown for both legacy and VHT training fields, along with how the measurements may change due to motion.

The latest introduction of the HE PHY has the potential to enhance Wi-Fi Sensing. In addition to enabling operation in the 6GHz spectrum, the HE PHY has increased the number of subcarriers per 20MHz bandwidth by 4x [20].

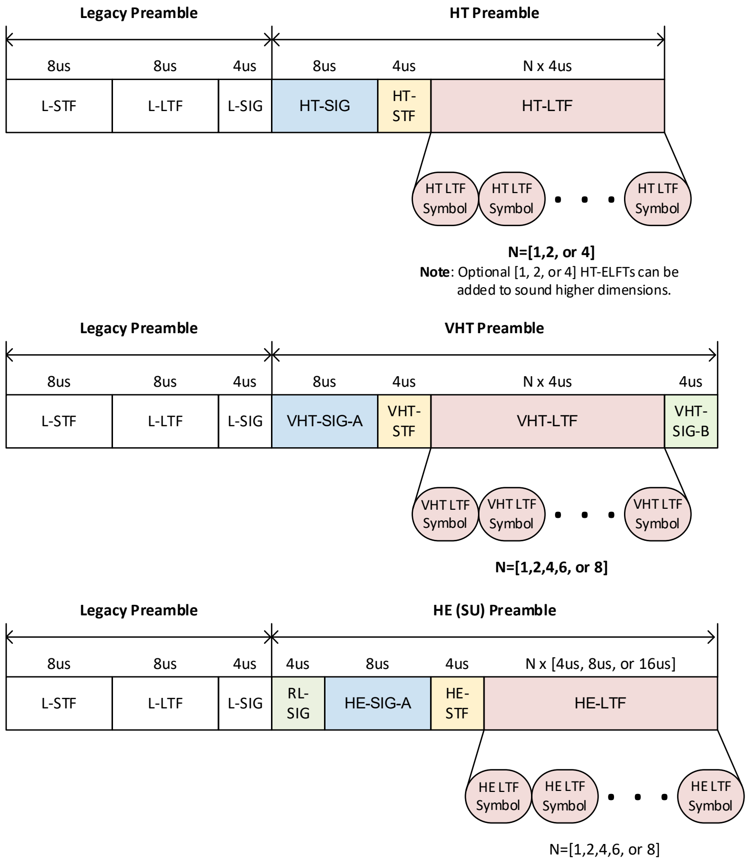


Figure 17. HT/VHT/HE OFDM PPDU Preamble

5.1.2 DSSS-based PHY

The Direct-Sequence-Spread-Spectrum (DSSS) PHY was defined in the IEEE 802.11-1997 standard [23] and is part of the IEEE 802.11b [24] amendment. The DSSS PHY frame does not contain a field dedicated to channel estimation computation the way OFDM-based PHYs do; however, improving performance through multipath reduction has been a heavily researched topic. As a result, there are a number of papers that describe different mechanisms to produce a channel estimation from the DSSS CCK signal, as described in [25].

5.1.3 DMG-Based PHY

IEEE 802.11ad [26] amendment defines a Directional-Multi-Gigabit (DMG) PHY for operation in the 60GHz band. While there are three different modulation schemes (Control, Single-Carrier and OFDM) defined, Control and the Single Carrier PHY are the primary PHY used in 802.11ad (and is also part of the subsequent 802.11ay amendment). Regardless of the modulation scheme, every packet starts with a preamble that consists of a short training field (STF) and a channel estimation field (CEF). The STF is used for timing estimation and AGC adjustment. CEF is used for channel estimation.

Similar to the OFDM-based PHYs, the necessary channel estimation for Wi-Fi Sensing is available following successful reception and processing of the preamble of a packet and can be provided to the higher layers.
The wide channel bandwidth available in 802.11ad/ay significantly improves the performance of Wi-Fi Sensing in terms of the resolution; however, the limited communication range in 60GHz band restricts the Sensing range and coverage.

5.2 MAC Layer Requirements

MAC layer mechanisms are used to obtain information about the connected devices and the roles they play in Wi-Fi sensing. The MAC layer also initiates and drives transmissions required for channel estimation among the devices in the Wi-Fi Sensing network.

5.2.1 Peer Identification

There are multiple aspects related to peer identification required by Wi-Fi Sensing. The first aspect is identifying the devices and the channel estimation mapped to the physical environment between any two devices. Typically, an STA is identified by a 48-bit MAC address. A MAC address is sufficient identification for STAs associated with a Wi-Fi network; however, if the association is lost during the lifetime of the application, then randomized MAC addresses may be used. In this case, a different or more involved mechanism would be required to identify each STA. This identification must match the corresponding channel estimate measurement obtained from the PHY.

The second aspect is identifying the device network role and its connection type, such as whether it is an AP or an STA, or whether it is part of a mesh or a P2P connection. This information is used by the Wi-Fi Sensing agent to decide the best method for conducting measurements.

The third aspect is the identification of Wi-Fi Sensing device capabilities. This information is required from all devices in the network in order for the Wi-Fi Sensing agent to select devices participating in the sensing measurements. Information that is useful for this purpose includes but may not be limited to:

- Whether the device supports sensing capabilities
- Supported measurement rate
- Availability and willingness of the device to participate in sensing measurements

5.2.2 Sensing Transmissions

As described in section 5.1, there are different types of transmissions that can be used for illumination of the Wi-Fi channel and obtaining measurements between two devices. Passive transmissions rely on existing Wi-Fi traffic and do not introduce any new MAC layer requirements. Triggered transmissions, however, rely on additional transmissions. Depending on whether existing packet exchange procedures are used for triggered transmissions or new exchanges are defined, the requirements on the MAC layer will be different.

An example of one existing packet exchange that can be used for triggering invoked transmissions is null data packet (NDP) and ACK exchange. NDP transmission by the Wi-Fi Sensing receiver can be used to invoke a Wi-Fi Sensing transmitter to respond with an ACK, which may then be used to compute a channel estimation. The disadvantage of using ACK packets for channel estimation, in 2.4/5GHz bands, is that the ACKs are only transmitted in legacy mode (Section 5.1.1).
Another example of how an invoked measurement can be triggered is by use of the implicit unidirectional beamforming procedure, first defined in the IEEE 802.11n standard. In this procedure, an STA requests beamforming training by sending a MAC frame with the training request (TRQ) bit set to 1. This triggers the receiving device to send an NDP announcement, followed by an NDP to illuminate the channel. The benefit of this invoked measurement is that it is not limited to the legacy preamble for channel measurements and uses the MIMO training fields, as well.

In pushed measurements, a transmission is triggered by the illuminator to be received by one or multiple Wi-Fi Sensing receivers. Beacon frames are an example of using existing MAC packet exchanges for pushed measurements.

5.2.3 Sensing Measurements

As described in Section 2, to support different use cases, either the AP or STA may take the role of sensing receiver; additionally, there may be multiple sensing receivers required to support the application. Moreover, there may be multiple illuminators involved in the measurements. In order to coordinate the sensing transmissions among the illuminators and the sensing receivers in an efficient way, MAC layer coordination is required. Moreover, many use cases rely on periodic measurements, which require MAC layer scheduling. Coordination and scheduling at the MAC layer should enable different options for conducting sensing measurements among multiple illuminators and sensing receivers, with minimal added overhead, while accounting for the power save state of the devices.

5.3 Wi-Fi Sensing Radio API Requirements

To interact with the MAC and PHY, the Wi-Fi Sensing agent requires an interface to pass the Wi-Fi Sensing control information to the radio and extract the measurement data. The interface is PHY agnostic and, therefore, can be defined in a generic manner and extended to cover different radio driver implementations, including drivers from different chipset vendors. The interface definition should allow for potential additional features or capabilities provided by a specific PHY or a chipset, as well as a path for growing the technology.

Definition of a standard interface/API enables radio firmware and driver developers to ensure compliance and enables reuse of components or common codes, which may be placed into a library. Most Wi-Fi drivers are based on either the wireless-extensions framework or the more recent and actively developed cfg80211 / nl80211 framework. As the system integration components are largely provided, these frameworks enable Wi-Fi driver developers to focus on the hardware aspects of the driver. These frameworks offer great potential as a location for defining a Wi-Fi Sensing API.

Aside from ensuring consistency between radios and drivers, this interface is expected to provide the Wi-Fi Sensing agent the following capabilities.

5.3.1 STA identification and Wi-Fi sensing capability

Peer identification was introduced as a MAC layer requirement in Section 5.2.1. As such, the Wi-Fi Sensing interface should provide the Wi-Fi Sensing agent with STA identification and enable the Wi-Fi Sensing agent to track the physical device in the network (i.e., the AP to which it is connected). Additional information to be provided to the Wi-Fi Sensing agent includes capability and device's availability to participate in the measurements.

5.3.2 Configuration Of Measurement Type

The Wi-Fi Sensing agent requires control of the STAs that will participate in the sensing measurements, as well as what measurement type (passive vs triggered) will be performed. The Wi-Fi Sensing interface should provide such control, either on a global system scale or on a per STA basis in order for the Wi-Fi Sensing agent to conduct Wi-Fi Sensing measurements in the most efficient manner.

5.3.3 Configuration Of Measurement Rate

Based on the specific Wi-Fi Sensing application or use case, different measurement rates may be required. The measurement rate is typically decided by the Wi-Fi Sensing agent, and the interface should support its control. However, to provide the lowest jitter and best efficiency possible, it is best to rely on MAC layer for scheduling.

5.3.4 Configuration Of Measurement Parameters

Wi-Fi Sensing applications may have different measurement parameter requirements (bandwidth, antenna configuration, etc.). The configuration of measurement parameters allows the application to obtain only the data it requires to maintain efficiency. The measurement parameters should be configurable independently for each STA.

5.3.5 Data Extraction From Radio

The number of subcarriers and frequency locations within the channel estimation will follow the format defined in the IEEE 802.11 standard. Obtaining the channel estimation requires some computation, and the result may be chipset specific. The Wi-Fi Sensing interface should be flexible enough for the radio to specify whether the data payload is in time-domain or frequency-domain, the numerical format, etc. By having this knowledge, the Wi-Fi Sensing agent is able to correctly interpret the data.

5.4 Security Considerations

Rogue devices are those that are not authenticated within a network and tend to have malicious intentions, such as hijacking legitimate clients, inducing denial-of-service or performing a man in the middle attack. In the case of Wi-Fi Sensing, a rogue device or rogue Illuminator node can spoof the SSID and/or MAC address of a valid illuminator and transmit false data to the Wi-Fi Sensing receiver. This can be harmful to Wi-Fi Sensing applications, resulting in unintended consequences for the applications and users. Having a mechanism to confirm that the data received by the Wi-Fi Sensing receiver is from an authenticated valid illuminator can improve the robustness of Wi-Fi Sensing use case.

6 Gaps in Existing Wi-Fi Technology

In Section 5, the technology requirements for Wi-Fi Sensing were described. This section identifies technology gaps for support of Wi-Fi Sensing in Wi-Fi standards.

6.1 PHY

As discussed in Section 5, the existing PHYs address the technology requirements of sensing and there is no need to define a new PHY; however, sensing applications would benefit from minor enhancements, which are described here.

Wi-Fi Sensing relies on measurements conducted for channel estimation over time, as described in Section 5.1, to detect variances in channel state due to changes in the environment. As such, it is required that the configuration of the radio remains the same during different instances of measurement. Otherwise, it is not possible to distinguish variances in the channel state due to environmental changes vs. changes in the radio configuration, such as antenna configuration during beamforming.

A mechanism to ensure constant configuration of the radio during different instances of measurement or a mechanism to calibrate the measurements to adjust for changes in radio configuration is a requirement not fully addressed in today’s standards.

As described in Section 5.1, the amount of information provided to the Wi-Fi Sensing agent depends upon the PHY type and the particular measurements specified in the standards today, which were not primarily defined for the purpose of sensing. Wi-Fi Sensing would benefit from additional measurement information that may be defined in future standards to increase the sensing accuracy.

6.2 MAC

6.2.1 Peer Identification

Section 5.2.1 outlined the requirements regarding peer identification. There are two potential gaps in addressing these requirements:

- **Device identification in the presence of MAC address randomization:** In applications with relatively long lifetime, such as home monitoring, reassociation can interrupt the application due to change of MAC address. In such situations, a mechanism would be necessary to identify the STA as it interacts with a given network.
- **Identification of device sensing capabilities:** While it is possible to implement sensing capabilities exchanged as a higher-layer function, since Wi-Fi Sensing measurement is a MAC and PHY feature, having access to the related device capabilities at the MAC layer results in a more efficient implementation of the illumination process.
- **Management Frame Information Elements:** One potential way to enable capability exchange in a standard, compliant manner is through use of Management Frame Information Elements, which can be exchanged during the association process.

6.2.2 Sensing Transmissions

In Section 5.2.2 possible mechanisms and limitations of enabling triggered transmissions in today's Wi-Fi networks were described.

- In the invoked case, as an example the ACK frame (transmitted in response to an NDP frame) can be used as an illuminator packet. However an ACK is always transmitted in legacy mode, providing limited channel measurement information. Having an invoked mechanism defined within the MAC layer, with the capability of using either legacy or MIMO training fields for channel estimation, enhances measurement capabilities.
- In the pushed case, a short frame can be transmitted frequently in a broadcast manner to the Wi-Fi Sensing receivers in the network, enhancing the efficiency of the illumination process. Note: In the current IEEE 802.11 standard, a similar procedure has been defined for HT explicit or VHT beamforming scenarios; however, the mechanism is geared toward the receiver returning an explicit report (such as a compressed beamform report). For the pushed measurement case, it is not desirable to have the beamform report returned, as the information is not relevant or used.

6.2.3 Sensing Measurements

In addition to efficient sensing transmissions, mechanisms for the Sensing receiver to learn the radio configuration of the illuminator and MAC layer mechanisms for coordination and scheduling of the measurements are gaps that need to be addressed.

6.3 Wi-Fi Sensing Radio API

Since Wi-Fi Sensing is a new technology, another large gap is the lack of a standardized interface/API definition. Various chipset vendors have provided hooks or enabled access to the required facilities; however, there currently is no standard interface definition or implementation.

Examining the structure of the current state-of-the-art Linux Wi-Fi drivers revealed that most existing drivers and all current developments are based on a framework called cfg80211 / nl80211. This framework was first developed in late 2006 as a replacement for the original Wi-Fi driver wireless extensions. As described in [27], Figure 18 illustrates the typical Linux Wi-Fi driver architecture.

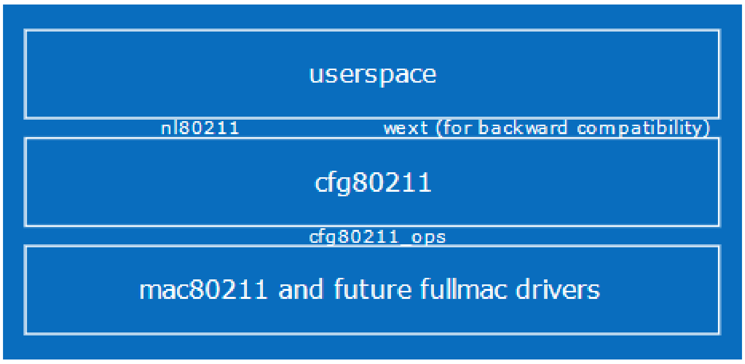

userspace
nl80211
wext (for backward compatibility)
cfg80211
cfg80211_ops
mac80211 and future fullmac drivers

Figure 18. Driver Architecture [27]

The first framework component is called cfg80211 and provides a standard 802.11 configuration API for the driver. This module sits between the low-level radio driver and the userspace components, such as hostapd (AP functionality), wpa supplicant (STA functionality), etc. Driver developers typically use cfg80211 as it interacts with all standard userspace components, thereby eliminating redundant code or components from the drivers. Interaction between the driver and cfg80211 is done through a set of registered callback functions that each driver is required to implement, as well as through exchanging standardized data structures to identify the radio capabilities.

The second component is called nl80211 and provides a standard communication interface for userspace applications to interact with cfg80211 components. A generic netlink interface is used as the transport mechanism, and nl80211 defines the channels and protocol.

To create a standardized Wi-Fi Sensing API in cfg80211 / nl80211 framework, the appropriate place is within the already existing cfg80211 and nl80211 modules. These modules are currently used to define a standard configuration interface to the radio. The required features described in section 5.3 are essentially further radio configuration parameters targeting Wi-Fi Sensing applications.

Furthermore, nl80211 creates multiple generic netlink multicast channels to allow the radio to provide raw data back to userspace. An example of this is the MLME channel, to which the radio driver can publish all received Wi-Fi management frames. In userspace, applications like hostapd are then able to subscribe to this channel and receive the feed of raw management frame data. For Wi-Fi Sensing applications, a similar mechanism can be used to provide the raw radio data from the driver to userspace. The Wi-Fi Sensing agent will be able to subscribe to a channel to obtain this data feed. The type-length-value (TLV) structure of a generic netlink frame also works well for this type of application. It allows radio chipset vendors to provide standardized data, as well as their own custom data, that may be useful for any processing algorithms, such as RSSI, EVM, interference detection, etc.

By defining the Wi-Fi Sensing API in this framework, a standardized configuration and data interface can be made available to any driver based on the cfg80211 / nl80211 framework. It would no longer be required for each driver to define and create a proprietary API and data transport mechanism, nor would it be required for the Wi-Fi Sensing agent to support a vast array of different vendor interfaces, further simplifying and reducing the complexity of both the driver and the userspace software.

6.4 Security Considerations

Section 5.4 identified protection against rogue Wi-Fi Sensing transmitters as a security requirement. While associated STAs are authenticated by the AP, there is no way to know if other STAs are authenticated. for scenarios in which the illuminator node and Wi-Fi Sensing receiver are not an AP and STA associated with one another, addressing the rogue illuminator security threat is a gap.

6.5 Interoperability Testing & Certification

While not a technical requirement, lack of a certification program ensuring interoperability of Wi-Fi Sensing devices, even if all other gaps are addressed, remains a major hurdle for the technology in the market. Development of a certification program is a next step following technology standardization. As discussed in previous sections, while a limited number of applications can be satisfied by passive measurements, the majority of use cases require participation and coordination among multiple devices for best performance.

Successful deployment of Wi-Fi Sensing in the market not only depends on standardization but also a certification program that ensures interoperability of different implementations.

Given market demand, the certification program may be done in phases, starting with simple goals that can be achieved readily and yet benefit the ecosystem, and moving to a more complete scope in future years as additional technical solutions are standardized.

One potential requirement of an early phase certification program would rectify the identified MAC layer gap by having a mechanism to identify Wi-Fi Sensing capabilities of STAs in a network. An example solution addressing this gap would be a definition of a Wi-Fi Sensing Information Element, which would enable Wi-Fi device manufacturers to have their devices participate in Wi-Fi Sensing applications and benefit from the added value.

7 Home Monitoring Case Study

To provide a real-life example, the home monitoring use case described in Section 3.2.1 is provided as a case study. When deploying such a system, there are many variables to consider, including AP/client placement, house size, environment layout, construction materials, etc. Multiple testing approaches can be considered to verify the system performance in the presence of all variables. This section first describes possible testing methodologies, then explains the setup for home monitoring case study, and finally presents results for multiple deployment.

7.1 Testing methodologies

Different approaches for testing of Wi-Fi Sensing include:

Bench and Laboratory Testing

Bench and laboratory testing of the full system are difficult to perform. It is difficult to model a changing channel response that correlates to specific environmental changes without expensive, high-end equipment. Laboratory testing, however, is useful for validation of the PHY and MAC layers and radio APIs.

Real-World Testing

Ideally, Wi-Fi Sensing tests will take place in a well-controlled environment, where interference and signal levels can be regulated. Environments such as semi or fully anechoic chambers are not practical due to size and cost. Also, multipath RF environments are hard to produce inside these chambers.

One solution is to test at a real home in which the environment cannot be controlled, but it can be monitored and reproduced to a certain degree. This method is the best option to create a repeatable test environment by fixing furniture, AP and client positions. Any motion detection testing inside the house should also follow prescribed patterns, using as close to the same route and pacing as previous tests. This allows the tester to establish a baseline performance and, from thereon, measure regressions or improvements.

Deployment Scaling

Testing a single deployment only reveals the performance in one fairly static environment. Testing in multiple environments should be considered to obtain a good sample for testing. Environmental variations that are useful to consider include:

- Single-detached homes with multiple floors and of different sizes
- Townhomes with multiple floors and of different sizes
- Apartments on different levels to simulate multi-directional neighbors
- Different construction materials, drywall, brick, concrete, wood and glass

7.2 Testing And Measurements For Home Monitoring Case Study

The following sections outline the deployment and conducted testing in different environments, as desired by both the real-world testing and deployment scaling topics described above.

The measurement results were obtained through a preliminary evaluation conducted by **Netperian** in conjunction with early-stage prototype technology provided by **Cognitive Systems**.

The objective was to determine Wi-Fi Sensing coverage in each environment, using multiple APs and a number of client STA devices to further illuminate the environment. There are three different environments, real-world homes with different sizes:

- Environment 1: 900 sq/ft multi-dwelling apartment unit
- Environment 2: 3000 sq/ft detached home
- Environment 3: 6000 sq/ft detached home

For each environment, the test procedure is as follows:

- RSSI measurements were sampled throughout the environment
- An adult walked a predefined path throughout the home to map motion detection and intensity within each room
  - Tester used slow walking pace and recorded motion detection every 6ft
  - Tester stopped after entering each room, waited 10 seconds, then walked the perimeter of the room
- Motion detection was divided into 3 categories:
  - No motion, represented by red in the motion heat map
  - Motion, low intensity, represented by yellow in the motion heat map
  - Motion, high intensity, represented by green in the motion heat map

Note that with these measurements, the interpretation of motion intensity is somewhat subjective, as it depends on the algorithm. Both low- and high-intensity areas were capable of detecting motion; however, low-intensity areas detected motion at a lower confidence level than the high-intensity areas.

7.2.1 Environment 1: Description & Results

Environment Description

- Located in a 21-unit low-rise complex
- 5 rooms, excluding bathroom and utility spaces
- The building consisted of brick exterior and wood/drywall interior

Deployment

- Single AP used, representing a typical deployment
- Three or four STA clients used to illuminate the environment
  - Each STA client was a 2.4GHz TP Link Wi-Fi Smart Plug

The apartment layout shown in Figure 19 represents a typical urban environment in a high-density North American neighborhood. Due to the close proximity to adjacent units, it also presents challenges due to interference.

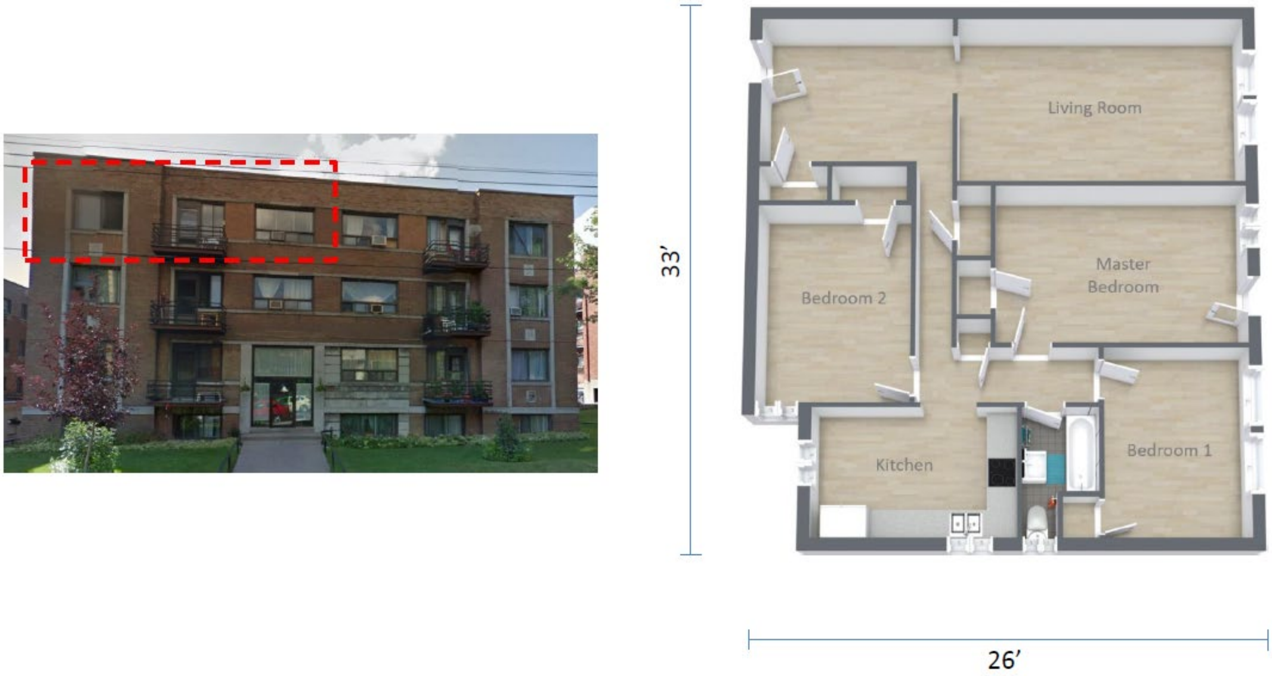


Figure 19. Layout of 900 sq/ft Multi-Dwelling Apartment

Results

The sampled RSSI measurements and motion coverage measurements for Environment 1 are shown below. The RSSI heat map measurement corresponding to environment 1 is shown in Figure 20. Since a single AP is used, and since all connected STA clients are 2.4GHz, only the 2.4 GHz band was measured.

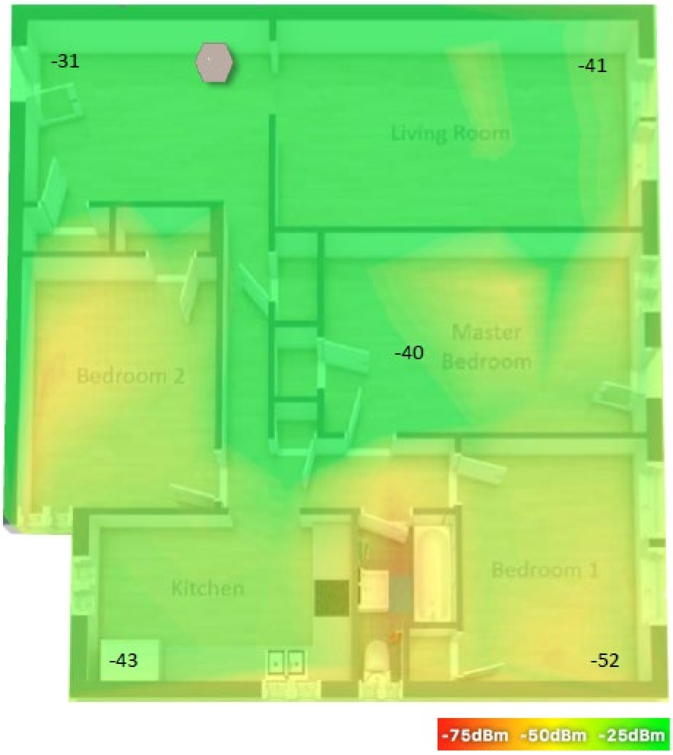


Figure 20. RSSI heat map for 2.4 GHz with 1 AP

The motion coverage map measurement corresponding to environment 1 is shown in Figure 21. Coverage is tested with 3 and 4 connected STA clients. Each STA client is a 2.4GHz device.

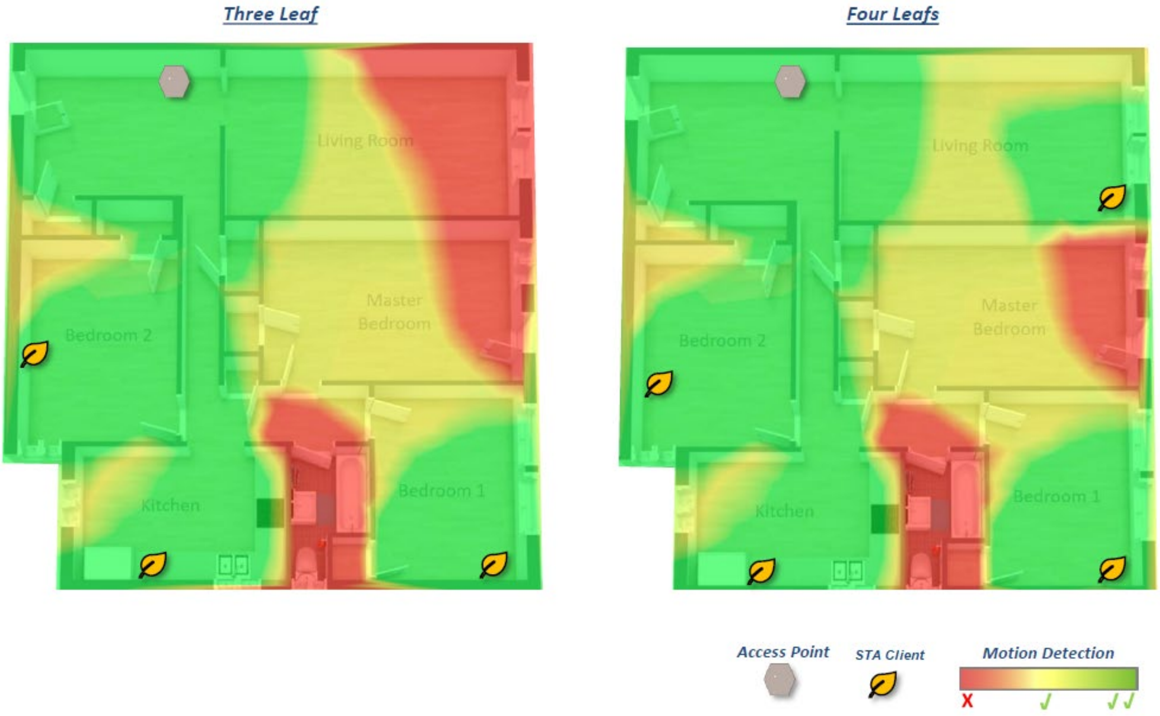


Figure 21. Motion coverage with 1 AP

7.2.2 Environment 2: Description and Results

Environment Description

- 3,000-square feet with 3 floors, including fully finished basement
- 8 rooms, excluding bathrooms and utility spaces
- Brick exterior, wood and drywall interior

Deployment

- 3 APs were used, which represents a large residential area
- Four STA clients were used to illuminate the environment
  - Each STA client was a 2.4GHz TP Link Wi-Fi Smart Plug

The home layout shown in Figure 21 represents a typical suburban environment in a medium-density North American neighborhood. This environment represents a good balance between attenuation from the house structure and interference from surrounding networks.

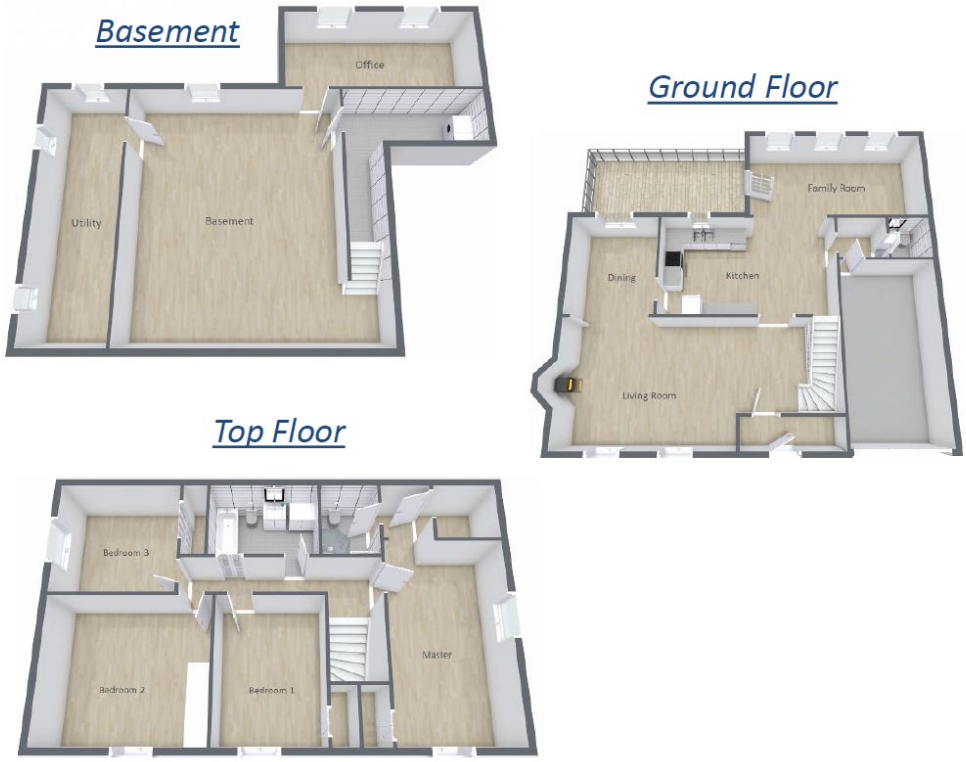


Figure 22. Layout of 3000 sq/ft Detached Home

Results

The RSSI heat map measurements for Environment 2 are shown in Figure 23 and Figure 24. Since all APs are connected via a 5GHz wireless backhaul, and each STA client is connected using the 2.4GHz, the RSSI has been measured in both bands.

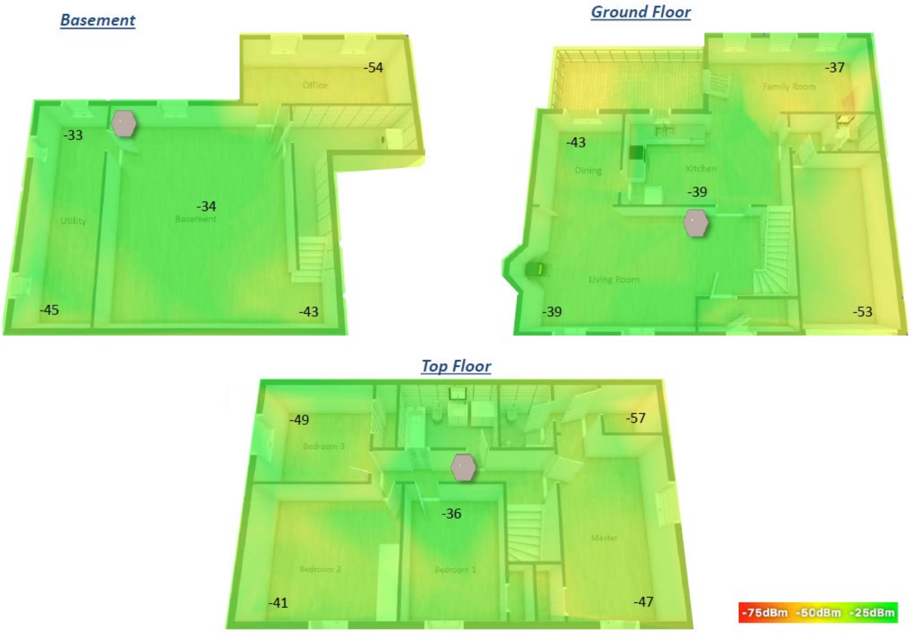


Figure 23. RSSI heat map for 2.4 GHz with 3 Aps

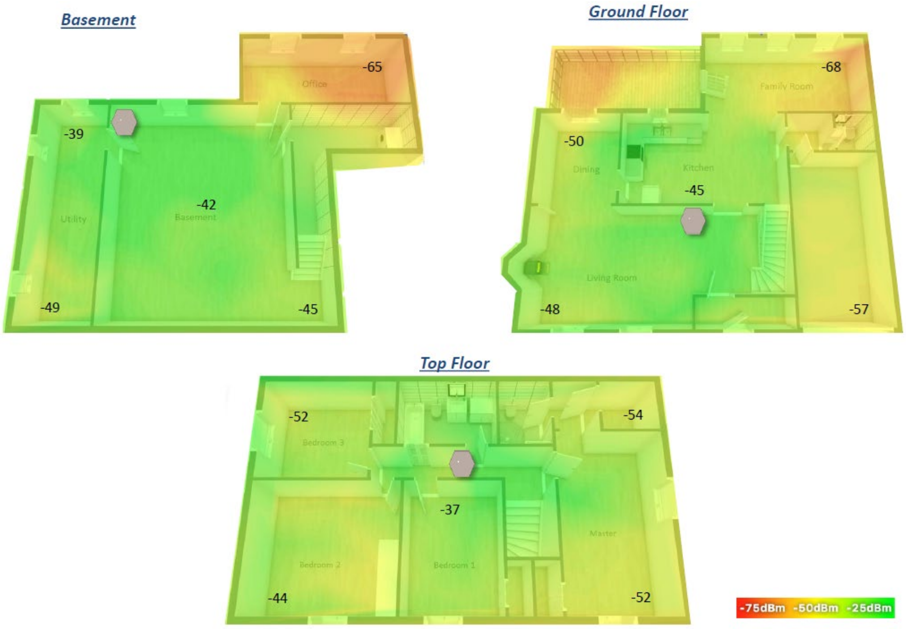


Figure 24. RSSI heat map for 5 GHz with 3 APs

The motion coverage measurements for Environment 2 are shown in Figure 25. Coverage was tested with 3 APs, and 4 connected STA clients. Each AP is connected using a 5GHz wireless backhaul, and each STA client is a 2.4GHz device.

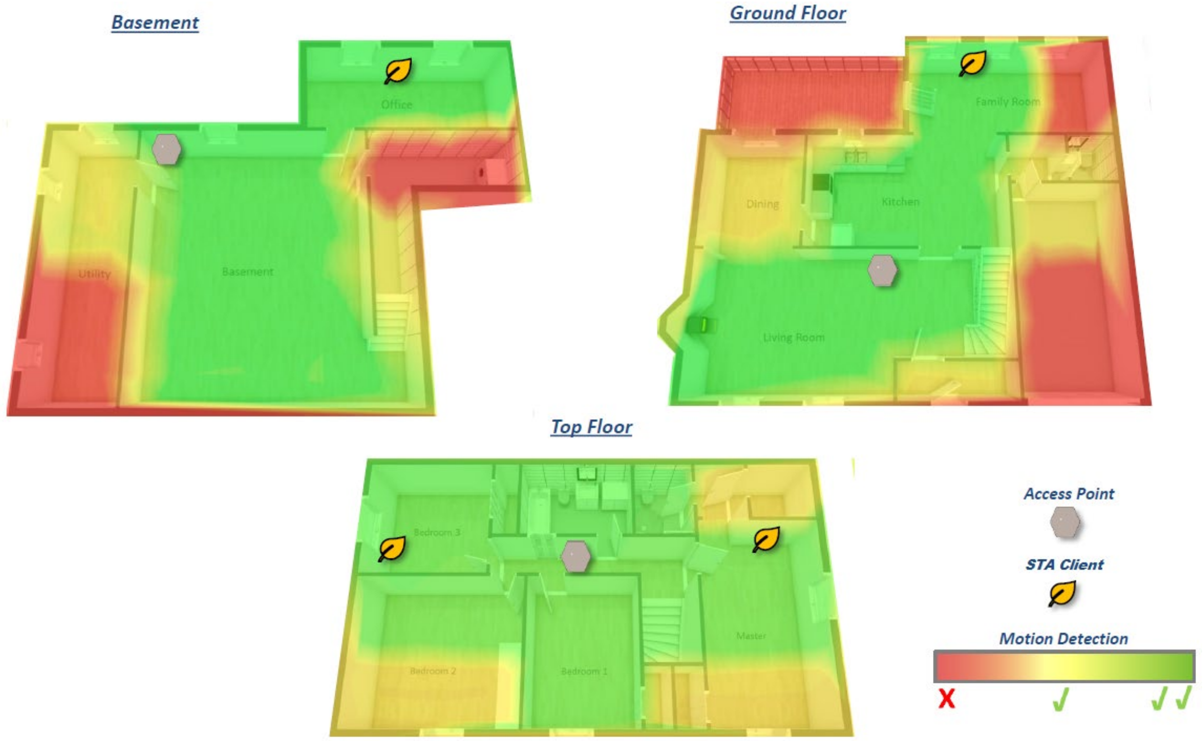


Figure 25. Motion coverage with 3 APs and 4 clients

7.2.3 Environment 3: Description and Results

Environment Description

- 6,000-square feet with 4 floors, including fully finished basement
- 15 rooms, excluding bathrooms and utility spaces
- Stone exterior, wood and drywall interior, stone tile and hardwood flooring, 10ft ceilings

Deployment

- 4 APs were used, representing an above-average residential deployment
- Seven STA clients were used to illuminate the environment
    - Each STA client was a 2.4GHz TP Link Wi-Fi Smart Plug

This house (shown in Figure 26) reflects an upscale home in a high-density setting, which is a good environment for challenging Wi-Fi performance, due to home size and construction materials.

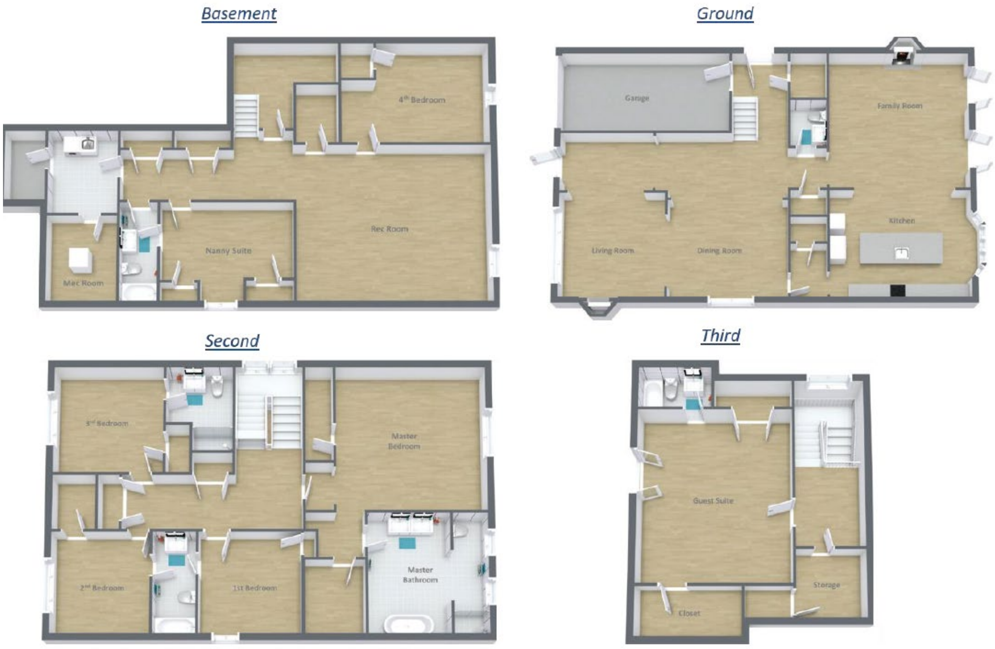


Figure 26. Layout of 6000 sq/ft Detached Home

Results

The RSSI heat map measurements corresponding to Environment 3 are shown in Figure 27 and Figure 28. Since all APs are connected via a 5GHz wireless backhaul, and each STA client is connected using the 2.4GHz, the RSSI has been measured in both bands.

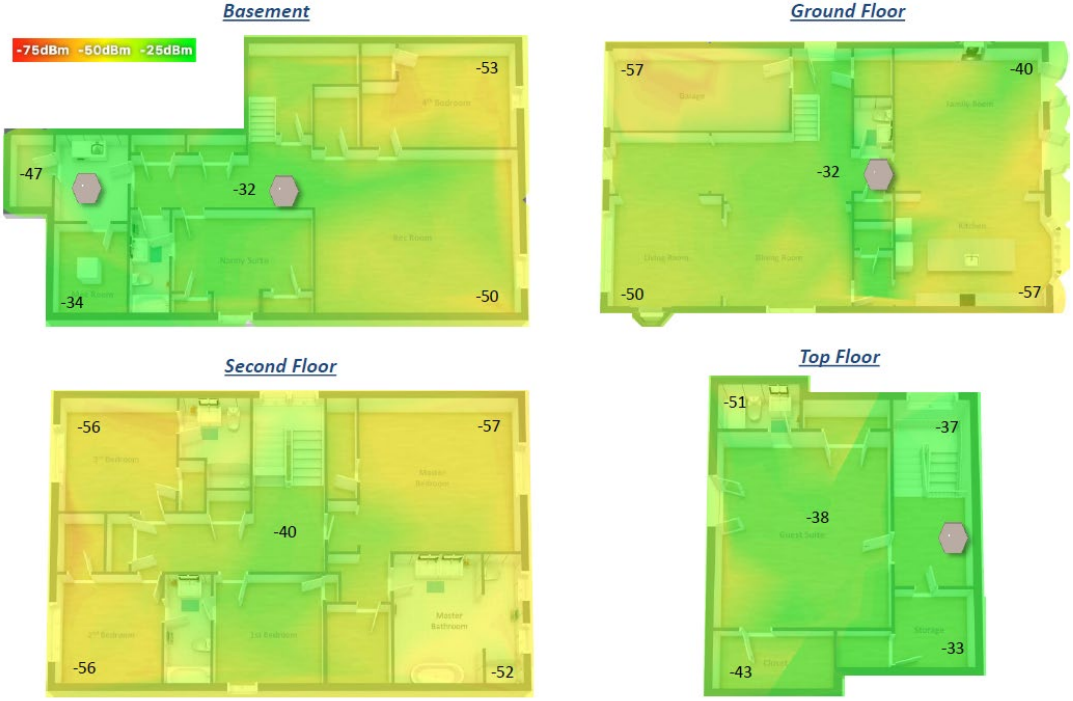


Figure 27. RSSI heat map for 2.4 GHz with 4 APs

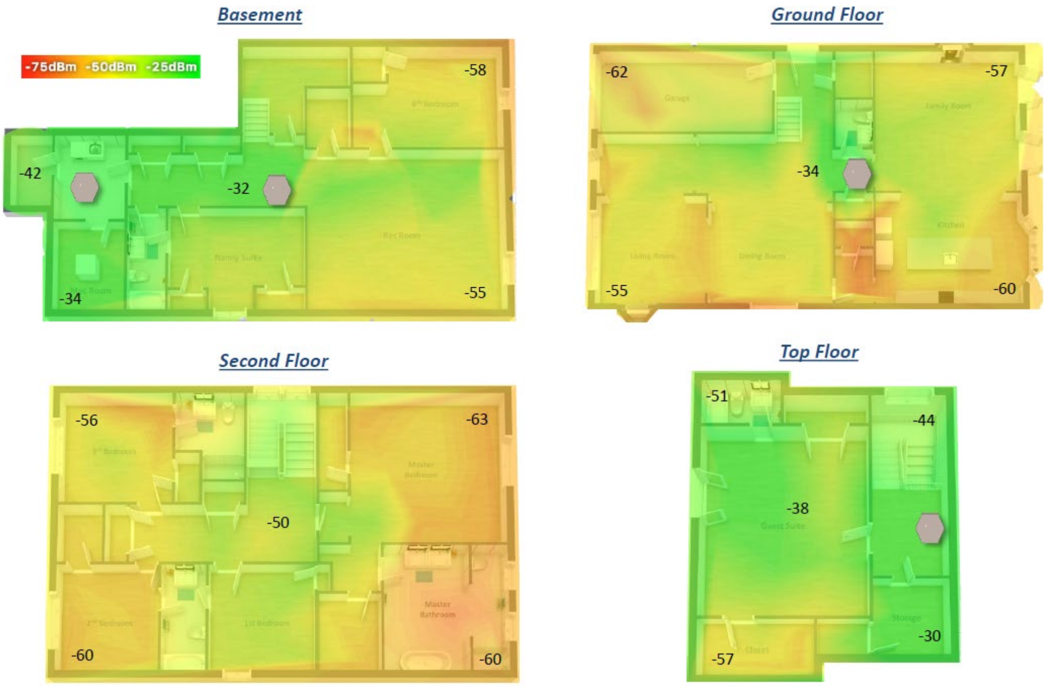


Figure 28. RSSI heat map for 5 GHz with 4 APs

The motion coverage measurements corresponding to Environment 3 are shown in Figure 29. Coverage was tested with 7 connected STA clients. Each AP is connected using a 5 GHz wireless backhaul, and each STA client is a 2.4 GHz device.

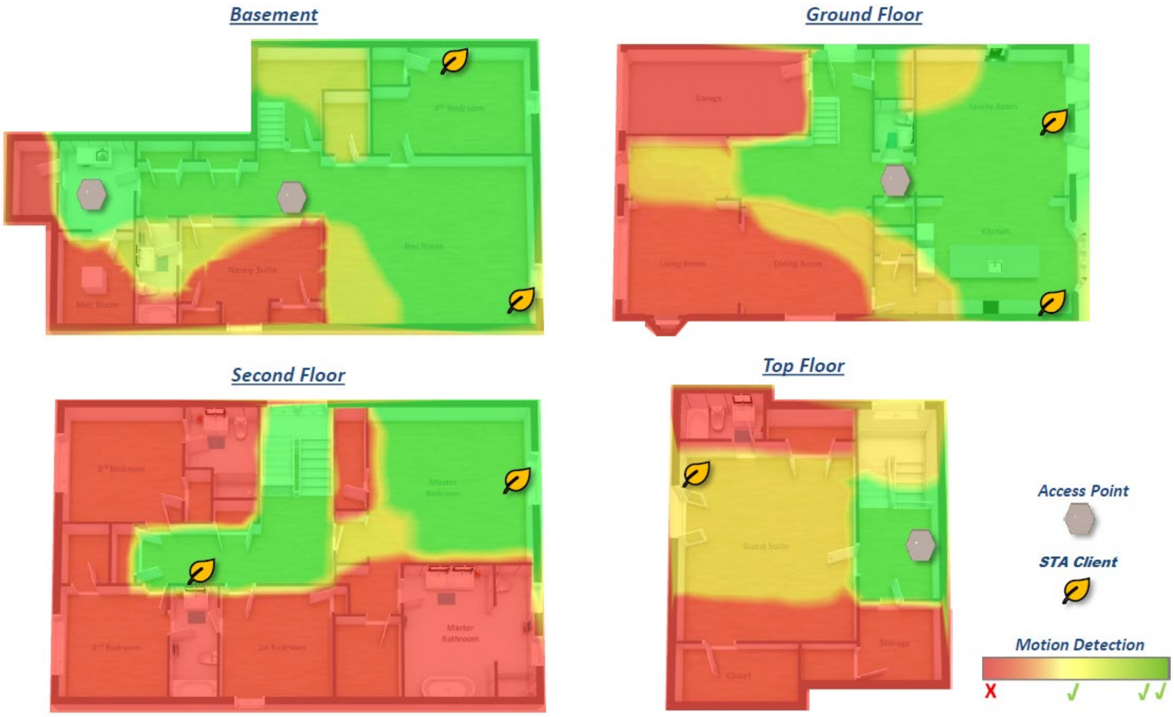


Figure 29. Motion coverage with 4 APs and 7 clients

7.3 Home Monitoring Case Study Conclusions

The measurement results presented in Section 7.2 not only represent execution of a test methodology for the home monitoring application (Section 2.2.1), but also illustrate successful deployment in three different types of home environments, showcasing the merit of Wi-Fi Sensing technology. The results also show that the Wi-Fi Sensing coverage can be extended by adding more illuminators. This property opens the potential to scale coverage to different types of spaces; it also warrants further work to develop deployment and illuminator placement guidelines, as well as mechanisms for coordination among multiple illuminators and receivers.

8 Further Action

Increasing interest in Wi-Fi Sensing has led to an initial analysis of potential use cases for this new technology, the Wi-Fi technology requirements and enablers for the identified use cases, and the existing gaps in today's Wi-Fi standards to meet these requirements.

Based on the analysis captured in this whitepaper, the WBA Wi-Fi Sensing group has compiled a series of recommended next steps to align industry players around enabling and expanding the reach of Wi-Fi Sensing technology in the marketplace. Subject to agreement:

1. The WBA will liaise with Wi-Fi Alliance to understand the opportunity of defining a solution addressing the Wi-Fi Sensing capability exchange requirement as outlined in Section 6.2.1 and developing a certification program around it.
2. The WBA will liaise with the IEEE 802.11 regarding its activities on Wi-Fi Sensing technology and the requirements of a future standard based on the findings of this whitepaper.
3. The WBA will engage with the software community to better understand opportunities to align on a common set of APIs for interacting with the radio for development of Wi-Fi Sensing applications
4. WBA will survey its membership about its views on the opportunities and challenges of conducting trials and creating a test environment for Wi-Fi Sensing technology.

REFERENCES

[1] IEEE Standard for Information technology-- Local and metropolitan area networks-- Specific requirements-- Part 11: Wireless LAN Medium Access Control (MAC)and Physical Layer (PHY) Specifications Amendment 5: Enhancements for Higher Throughput,"*IEEE Std 802.11n-2009 (Amendment to IEEE Std 802.11-2007 as amended by IEEE Std 802.11k-2008, IEEE Std 802.11r-2008, IEEE Std 802.11y-2008, and IEEE Std 802.11w-2009),"* pp.1-565, 29 Oct. 2009

[2] A. Fellah, "*Analyst Angle: 14 benefits of managed Wi-Fi,*" RCR Wireless, Nov. 2018. [Online]. Available: https://www.rcrwireless.com/20181108/analyst-angle/analystangle-4-benefits-managed-wi-fi

[3] M. Vena, "*First Look: Plume Blossoms With New SuperPods And Membership Offering,*" Forbes, June 2018. [Online]. Available: https://www.forbes.com/sites/moorinsights/2018/06/13/first-look-plume-blossoms-with-new-superpods-and-membership-offering

[4] D. Ernst, "*Changing Dynamics of the Smart Home: Opportunities for Service Providers,*" Parks Associates, 2019. [Online]. Available: http://parksassociates.com/whitepapers/calix-wp2019

[5] D. Halperin, W. Hu, A. Sheth, and D. Wetherall, "*Tool Release: Gathering 802.11n Traces with Channel State Information,*" ACM SIGCOMM Computer Communication Review, vol. 41, no. 1, pp. 53, Jan. 2011.

[6] Celeno, "*Celeno announces New Innovation: Wi-Fi Doppler Imaging*", July 2019. [Online]. Available: https://www.celeno.com/media-room/press-releases/celeno-announces-new-innovation-wi-fi-doppler-imaging

[7] CIOReview, "*Cognitive Systems: Motion Sensing with WiFi Devices*", CIOReview, vol. 08, no. 09, pp. 18, March 2019. [Online]. Available: https://magazine.cioreview.com/magazines/March2019/Wireless/

[8] P. Jain and K. Surana, "*Reducing churn in telecom through advanced analytics,*" McKinsey & Company, Dec. 2017. [Online]. Available: https://www.mckinsey.com/industries/telecommunications/our-insights/reducing-churn-in-telecom-through-advanced-analytics/

[9] R. Das, "*Aging 2.0: Live Healthier, Longer And Smarter,*" Forbes, Dec. 2017. [Online]. Available: https://www.forbes.com/sites/reenitadas/2017/08/24/aging-2-0-live-healthier-longer-and-smarter/

[10] S. Sarmah-Hightower, "*These Companies Make Remote Monitoring for Seniors Less Intrusive,*" care.com, 12 Mar. 2018. [Online]. Available: https://www.care.com/c/stories/14960/remote-monitoring-for-seniors/

[11] N. Kaplan, "*Smart Sensors Can Help Seniors Age In Place,*" Forbes, 5 Sept. 2018. [Online]. Available: https://www.forbes.com/sites/forbestechcouncil/2018/09/05/smart-sensors-can-help-seniors-age-in-place/

[12] T. Savoy, "*Technology that can foster aging in place,*" The Washington Post, 26 Feb. 2018. [Online]. Available: https://www.washingtonpost.com/news/where-we-live/wp/2018/02/26/technology-that-can-foster-aging-in-place/

[13] G. Redford, "*New Tech Options are Helping Seniors Age in Place,*" Scientific American, 12 Mar. 2018. [Online]. Available: https://www.scientificamerican.com/article/new-tech-options-are-helping-seniors-age-in-place/

[14] M. Saltzman, "'Aging in place' tech helps seniors live in their home longer," USA Today, 24 June 2017. [Online]. Available: https://www.usatoday.com/story/tech/columnist/saltzman/2017/06/24/aging-place-tech-helps-seniors-live-their-home-longer/103113570/

[15] D. Etherington, "Google's Pixel 4 smartphone will have motion control and face unlock," TechCrunch, 29 July 2019. [Online]. Available: https://techcrunch.com/2019/07/29/googles-pixel-4-smartphone-will-have-motion-control-and-face-unlock/

[16] N. Canpolat et al, "*Wi-Fi 6 Deployment Guidelines & Scenarios,*" Wireless Broadband Alliance, July. 2019. [Online]. https://wballiance.com/resource/wi-fi-6-deployment-guidelines-scenarios/

[17] J. Bahr et al, “*In-Home Wi-Fi Industry Guidelines,*” Wireless Broadband Alliance, Jan. 2019. [Online]. Available: https://wballiance.com/resource/in-home-wi-fi-industry-guidelines-2019

[18] IEEE Standard for Telecommunications and Information Exchange Between Systems - LAN/MAN Specific Requirements - Part 11: Wireless Medium Access Control (MAC) and physical layer (PHY) specifications: High Speed Physical Layer in the 5 GHz band,"*IEEE Std 802.11a-1999,*” pp.1-102, 30 Dec. 1999

[19] 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 4: Enhancements for Very High Throughput for Operation in Bands below 6 GHz.,"*IEEE Std 802.11ac-2013 (Amendment to IEEE Std 802.11-2012, as amended by IEEE Std 802.11ae-2012, IEEE Std 802.11aa-2012, and IEEE Std 802.11ad-2012)*,” pp.1-425, 18 Dec. 2013

[20] IEEE Draft 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 Enhancements for High Efficiency WLAN,"*IEEE P802.11ax/D4.0, February 2019*,” pp.1-746, 12 March 2019

[21] N. Canpolat et al, "*Enhanced Wi-Fi – 802.11ax Decoded. Overview, Features, Use Cases and 5G Context,*" Wireless Broadband Alliance, Jan. 2019. [Online]. Available: https://wballiance.com/resource/in-home-wi-fi-industry-guidelines-2019/

[22] 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 1 GHz 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

[23] IEEE Standard for Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications,"in IEEE Std 802.11-1997,” pp.1-445, 18 Nov. 1997

[24] IEEE Standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Networks - Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Higher Speed Physical Layer (PHY) Extension in the 2.4 GHz Band - Corrigendum 1, "*IEEE Std 802.11b-1999/Cor 1-2001,*” pp.1-24, 7 Nov. 2001

[25] Jun Hu, Aiqun Hu and Qian Ma, "*Channel estimation for wireless LAN with CCK modulation*," International Conference on Neural Networks and Signal Processing, 2003. Proceedings of the 2003, Nanjing, 2003, pp. 1542-1545 Vol.2.

[26] 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 3: Enhancements for Very High Throughput in the 60 GHz Band,"*IEEE Std 802.11ad-2012 (Amendment to IEEE Std 802.11-2012, as amended by IEEE Std 802.11ae-2012 and IEEE Std 802.11aa-2012),*” pp.1-628, 28 Dec. 2012

[27] J. Berg, “*WiFi Control Plane Overview,*” 26 Feb. 2009. [Online]. Available: https://wireless.wiki.kernel.org/_media/en/developers/documentation/control.pdf

APPENDIX

Appendix A Channel Estimation Measurements

Legacy Channel Estimation

Example channel estimation obtained from VHT PHY using Legacy-LTF. The channel estimation is represented in the frequency domain, as a complex number (In-phase and Quadrature). Magnitude and phase for the entire 80 MHz channel are shown in Figure A-1. In this example, each IQ sample is a raw 16-bit signed number, which has not been scaled or normalized.

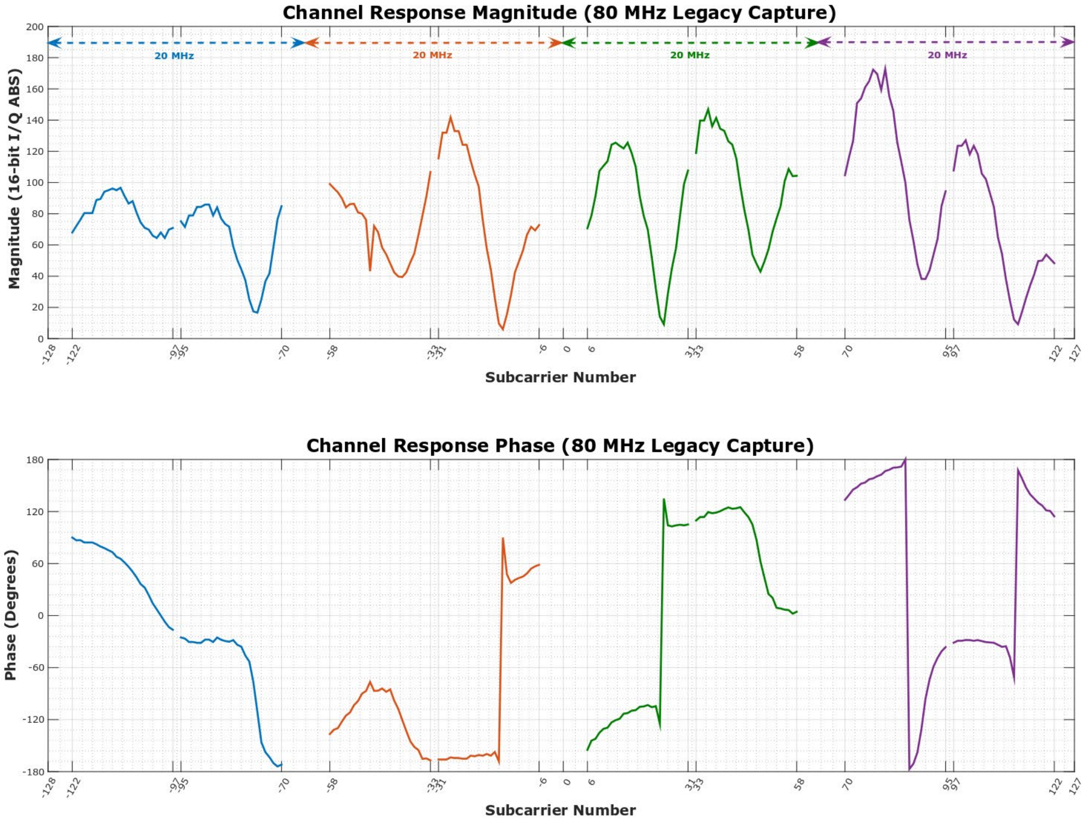


Figure A-1. Legacy Channel Estimation (Duplicated 80 MHz)

VHT Channel Estimation

Example channel estimation obtained from VHT PHY using VHT-LTF. The channel estimation is represented in the frequency domain, as a complex number (In-phase and Quadrature). Magnitude and phase for the entire 80 MHz channel are shown in Figure A-2. In this example, each IQ sample is a raw 16-bit signed number, which has not been scaled or normalized.

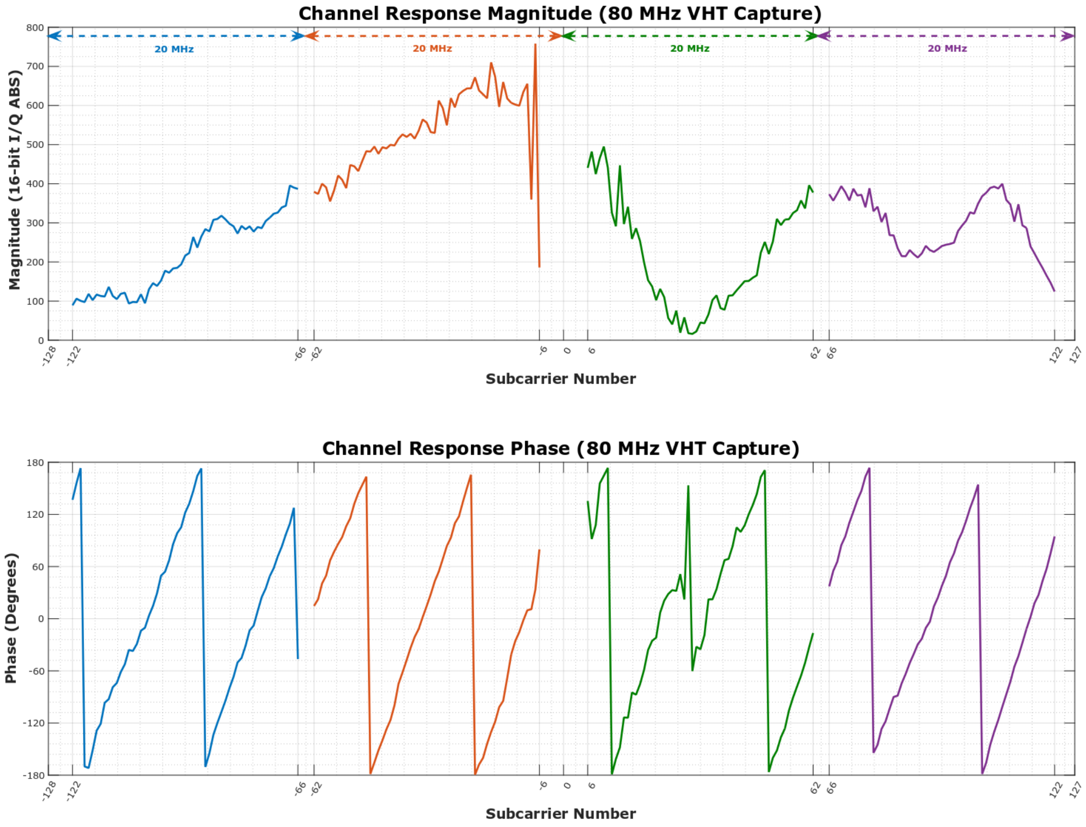


Figure A-2. VHT Channel Estimation (80 MHz)

Channel Estimation Change Due to Motion

Given a specific environment, periodic channel estimation measurements with and without motion have been captured. Figure A-3 and Figure A-4 illustrate the channel estimation magnitude for a static and changing environment respectively. For each plot, the color gradient illustrates the magnitude, X-axis represents frequency, and Y-axis represents the measurement time.

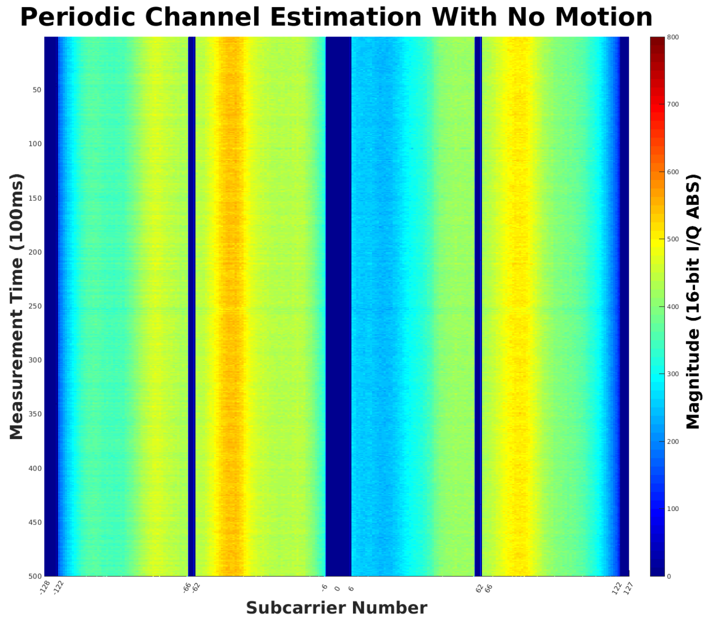


Figure A-3. Periodic Channel Estimation Magnitude with no Motion

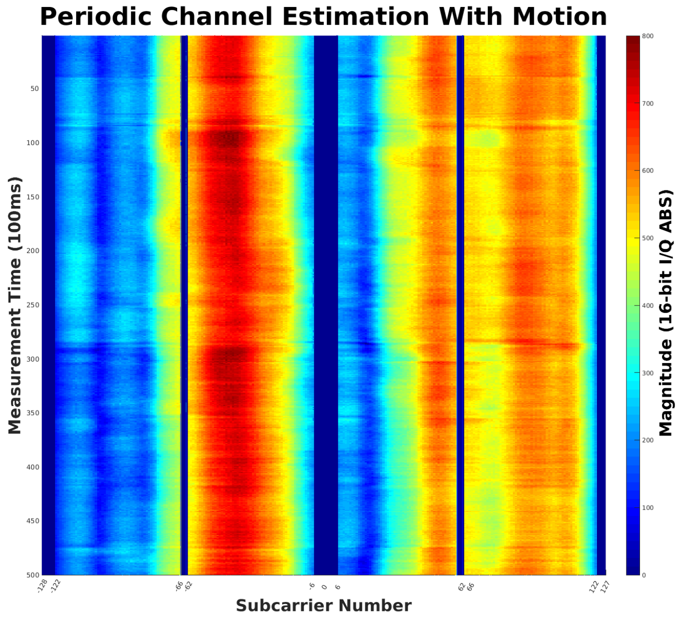


Figure A-4. Periodic Channel Estimation Magnitude with Motion

ACRONYMS AND ABBREVIATIONS

ACRONYM / ABBREVIATION	DEFINITION
AP	Access Point
API	Application Programming Interface
BSS	Basic Service Set
ESS	Extended Service Set
HE	High Efficiency
HT	High Throughput
IBSS	Independent Basic Service Sets
IEEE	Institute of Electrical and Electronics Engineers
IoT	Internet of Things
LTF	Long Training Field
MAC	Media Access Control
MLME	MAC Layer Management Entity
NDP	Null Data Packet
OEM	Original Equipment Manufacturer
OFDM	Orthogonal Frequency Division Multiplexing
P2P	Peer-To-Peer
PBSS	Public Basic Service Set
PHY	Physical Layer
PPDU	Physical Layer Protocol Data Unit
RRM	Radio Resource Management
STA	Station or Node
VHT	Very High Throughput
WBA	Wireless Broadband Alliance
WFA	Wi-Fi Alliance

PARTICIPANT LIST

NAME	COMPANY	ROLE
Chris Beg	Cognitive Systems Corp.	Project Leader & Chief Editor
Bahareh Sadeghi	Intel Corporation	Project Co-Leader
Sandeep Agrawal	Center for Development of Telematics (CDOT)	Project Co-Leader
Josh Redmore	CableLabs	Editorial Team
A R Balalakshmi	Center for Development of Telematics (CDOT)	Editorial Team
Kavita Mathur	Center for Development of Telematics (CDOT)	Editorial Team
Amanda Forsyth	Cognitive Systems Corp	Editorial Team
Paul Lock	Cognitive Systems Corp	Editorial Team
Petra Pohl	Cognitive Systems Corp	Editorial Team
Susan Gallotti	Cognitive Systems Corp	Editorial Team
Taj Manku	Cognitive Systems Corp	Editorial Team
Claudio da Silva	Intel Corporation	Editorial Team
Carlos Cordeiro	Intel Corporation	Editorial Team
Chen Cheng	Intel Corporation	Editorial Team
Pedro Mouta	WBA	Editorial Team
Finbarr Coghlan	Accuris Networks	Project Participant
Ken Kerpez	ASSIA	Project Participant

Irene Morvey	AT&T	Project Participant
Simon Ringland	BT	Project Participant
Deepak Garg	Bharat Sanchar Nigam Limited (BSNL)	Project Participant
Brian Shields	Boingo Wireless	Project Participant
Kishore Raja	Boingo Wireless	Project Participant
Burhan Masood	Broadcom	Project Participant
Michael Sym	BSG Wireless	Project Participant
Luther Smith	CableLabs	Project Participant
Suresh Parathi	Comcast	Project Participant
Paul Polakos	Cisco	Project Participant
Suja S	Center for Development of Telematics (CDOT)	Project Participant
Loay Kreishan	Charter Communications	Project Participant
Praveen Srivastava	Charter Communications	Project Participant
Mohammad Tariq	COX Communications	Project Participant
Lei Wang	Huawei	Project Participant
Tony Xiao Han	Huawei	Project Participant
Steve Namaseevayum	iPass / Pareteum	Project Participant
Alecsander Eitan	Qualcomm	Project Participant
James Pan	Panasonic	Project Participant

David Lopez-Perez	Nokia	Project Participant
Randy Sharpe	Nokia	Project Participant
George Hart	Rogers	Project Participant
Kanwal Sangha	Shaw Communications	Project Participant
Dzung Tran	Smith Micro	Project Participant
Peter Flynn	Viasat	Project Participant
Bruno Tomás	WBA	Project Participant
Tiago Rodrigues	WBA	Project Participant

For other publications please visit:
wballiance.com/resources/wba-white-papers

To participate in future projects, please contact:
pmo@wballiance.com

READ MORE