IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received April 29, 2022, accepted May 30, 2022, date of publication June 10, 2022, date of current version June 15, 2022.
Digital Object Identifier 10.1109/ACCESS.2022.3182011

Battle of the Bands: A Long-Term Analysis of Frequency Band and Channel Distribution Development in WLANs

SAKU LINDROOS, ANTTI HAKKALA, AND SEPPO VIRTANEN, (Senior Member, IEEE)
Department of Computing, University of Turku, 20014 Turku, Finland
Corresponding author: Saku Lindroos (saku.p.lindroos@utu.fi)

ABSTRACT In this article, we present the results of a long-term analysis of Wireless Local Area Network (WLAN) frequency band and channel distribution development. To the best of our knowledge, no similar research has been published in recent academic publications. Overcrowding of the limited frequency space on the 2.4 GHz band has become a significant issue in WLAN networking. Due to the overabundance of devices operating at 2.4 GHz, avoiding network performance degrading interference has become impossible in densely populated environments. Although the latest 802.11 WLAN standard amendments have emphasised the wider and less congested 5 GHz band, the 2.4 GHz band has stayed as the dominant frequency band. To observe the evolvement of WLAN frequency band and channel utilisation, data collected on nine WLAN surveys conducted between May 2019 and January 2022 was analysed. Furthermore, a simple linear regression model was produced to forecast the future development of WLAN frequency band utilisation. It was hypothesised that there would be an increase in 5 GHz frequency band utilisation as devices compliant with the latest 802.11 standard amendments become widely adopted. The survey results show a significant increase in 5 GHz frequency band utilisation. While the number of networks operating at 2.4 GHz saw a modest 42% increase, the number of networks operating at 5 GHz more than doubled during the survey period. At the end of the study, 35% of all detected networks operated at 5 GHz, compared to 25% at the beginning of the study. Based on the produced linear regression model, the portion of 5 GHz networks in the survey area is expected to reach the level of 2.4 GHz networks by the autumn of 2025.

INDEX TERMS IEEE 802.11, interference, wardriving, wireless LAN, wireless networking.

I. INTRODUCTION

Wireless Local Area Network (WLAN) technology, commonly known by its marketing name Wi-Fi, is undoubtedly one of the most used and well-known wireless networking technologies. The original IEEE 802.11 WLAN standard was ratified in 1997, and three years later in 1999, Apple became the first manufacturer to provide built-in support for WLAN networking in laptop computers [1]. Since then, WLAN networks have become a household commodity.

As WLAN technology has become increasingly affordable over time, various sorts of devices have been introduced into our wireless networks. This outpouring of WLAN capable Internet of Things (IoT) technology has turned our living and working environments into hotbeds of WLAN networking. It has been estimated that the number of in-home WLAN devices will increase up to 17 billion worldwide by the year 2030 from an estimate of 5 billion in-home devices in 2019 [2]. In their 2021 report [3], the Wi-Fi alliance estimates that the global economic value of Wi-Fi products will increase by almost 3 trillion dollars from an estimated 1.96 trillion in 2018 to 4.9 trillion in 2025. The economic value of Wi-Fi in the 27 European Union countries alone is estimated to grow up to grow to 637.2 billion dollars by 2025 from an estimated 457.6 billion in 2021.

The great advantage of WLAN networking is the convenience of connecting a multitude of devices wirelessly, making it possible to seamlessly move devices to another location and create new or expand existing networks. The wireless nature of WLAN communication makes it a compromise of convenience over performance. Because the communicated information propagates through the air in Radio

The associate editor coordinating the review of this manuscript and approving it for publication was Razi Iqbal.

Frequency (RF) waves, instead of being confined to wires, the communication is highly susceptible to various forms of interference and degradation that lower the overall performance of the network. Furthermore, as there is only a limited amount of radio frequency spectrum available for all the devices to operate in, getting access to the spectrum resource can become highly competitive.

WLAN devices communicate on three different segments of the radio frequency spectrum: 2.4 GHz, 5 GHz and 6 GHz. As the use of the 6 GHz frequency band has not yet been allowed in several countries, and very few devices supporting communication on the band are available in the consumer market, it has been excluded from this research. In WLAN networking, the frequency bands are further divided into 20 MHz wide segments known as channels. The 2.4 GHz band holds 14 channels, whereas the higher 5 GHz band is divided into 25 channels. Because the 2.4 GHz band has less overall frequency space than the 5 GHz band, channels on the 2.4 GHz band are packed tightly together with only 5 MHz between each channel's centre frequency, causing the channel frequencies to overlap.

In a densely populated urban environment where hundreds of uncoordinated WLAN Access Points (APs), WLAN clients and various other wireless devices operate on the same frequency band, the shared wireless medium gets congested, limiting the performance of WLAN networks. As more devices occupy the same narrow wireless channels, more often the communicating devices will have to defer from sending data or the sent data gets corrupted because of the interfering signals of other transmitting devices. This has become a significant issue in the 2.4 GHz band where the limited frequency space has become increasingly crowded. Because of the overpopulation of the 2.4 GHz band, the newer amendments of the 802.11 standard shifted their emphasis to the less crowded 5 GHz band. Yet despite the efforts to guide users toward the 5 GHz band, the 2.4 GHz band has kept its place as the dominant frequency band.

In this article, we present the results of a long-term analysis of WLAN frequency band and channel distribution development. For the study, data collected on nine WLAN surveys between May 2019 and January 2022 was analysed to observe changes in frequency band and channel utilisation. Furthermore, a simple linear regression analysis was performed to forecast the future development of WLAN frequency band utilisation. We hypothesise that there will be an increase in 5 GHz frequency band utilisation as devices compliant with the latest 802.11 amendments become increasingly affordable and widely available on the consumer market. The study presents valuable and unique data on the evolvement of WLAN frequency band and channel usage. To the best of our knowledge, no similar survey data about recent changes in the WLAN frequency band utilisation has been published.

II. BANDS AND CHANNELS IN 802.11

WLAN networks must share the limited frequency space on the 2.4 GHz frequency band with multiple wireless communication technologies as well as many other radio frequency applications. While WLAN devices capable of communicating on the 5 GHz band have been available since the early 2000's, to this day, the 2.4 GHz frequency band has stayed dominant in WLAN communication. When an overabundance of various wireless devices on the 2.4 GHz band operate within range, interfering transmissions degrade the performance of WLAN networks. While modern WLAN AP's are often capable of communicating on both 2.4 GHz and 5 GHz frequencies, past regulation, lower manufacturing costs, and the demand for affordable WLAN-enabled IoT devices operating at 2.4 GHz have further increased congestion on the frequency band.

Despite the significance of the issue, very few of the published WLAN survey studies cover frequency band and channel usage. For instance, in his works, Nisbet analyses the evolvement of WLAN security in four separate locations within New Zealand based on surveys conducted in 2004, 2011 and 2013 [4], [5]. The reported survey results disclose WLAN deployment, encryption protocol use and channel utilisation on the 2.4 GHz band but do not further elaborate on frequency band utilisation. Similarly, Sarrafzadeh and Sathu report on a wide variety of WLAN properties but do not disclose channel or frequency band utilisation [6].

In their study, Valchanov, Edikyan and Aleksieva [7] surveyed over 11,000 WLAN networks in Varna, Bulgaria but do not report on channel or frequency band usage. Leca [8] collected data from a total of 100,000 WLANs in Romania and is the only one to report channel utilisation on both 2.4 GHz and 5 GHz frequency bands. Dobrilovic *et al.* [9] compared differences in WLAN security and abundance between the capital cities of Hungary and Serbia, briefly reporting on changes in channel usage on the 2.4 GHz band.

Although frequency band and channel utilisation have been neglected in past WLAN survey studies, various algorithms and schemes for optimising WLAN channel selection and utilisation have been proposed to mitigate the effects of interference on the 2.4 GHz band. Haochao *et al.* [10] propose a new architecture for the Medium Access (MAC) and Physical (PHY) layers to allow devices to effectively contend for the wireless channels in multi-user Multiple-Input and Multiple-Output (MIMO) environments, improving channel utilisation up to 470%. Maturi, Gringoli and Renato [11] successfully propose a scheme for AP's to dynamically select the least occupied channel and migrate the AP and the connected client devices onto the chosen channel.

Saliba, Imad and Houcke [12] present an algorithm for channel load estimation on the 2.4 GHz band to aid in channel selection based on the measured channel load. Mhatre *et al.* [13] introduce an algorithm for transmit power control that assigns higher transmit power for highly congested networks and networks with poor signal conditions over less congested neighbouring networks, improving throughput in congested networks. Similarly, Akella *et al.* [14] present a power control algorithm for congested WLAN deployments, attempting to minimise interference by automatically reducing the transmission power of wireless APs when possible. Haidar *et al.* [15] propose a WLAN channel-assignment algorithm that assigns AP's the least congested channel based on Signal to Interference Ratio measured by the proposed algorithm.

A. THE 802.11 FREQUENCY BANDS AND CHANNELS

In a wired Local Area Network (LAN), the communicated signal is bound to the wires that physically connect the communicating devices. In WLAN communication, data is encoded into RF signals that travel through the air between transmitting and receiving devices. As signals propagate between communicating devices, they must often travel relatively long distances through space and matter as well as contend against other signals. The travelled distance, obstructions and interfering signals cause the signal to attenuate and distort so that it can no longer be detected or interpreted by the receiving device. The majority of current 802.11 WLAN devices operate on the 2.4 GHz and 5 GHz radio frequency bands. Devices compliant with the 802.11b/g/n/ax amendments of the 802.11 standard can operate on the 2.4 GHz frequency band between 2.401 GHz and 2.495 GHz. The 2.4 GHz frequency band is the middle frequency of the licence-free Industrial, Scientific, and Medical (ISM) frequency bands. The 2.4 GHz ISM band is utilised by various other applications and wireless communication systems such as Bluetooth and ZigBee and is therefore highly congested. Because there is only roughly 100 MHz of frequency space to fit large quantities of varying devices, RF interference is prevalent on the 2.4 GHz band.

802.11a/n/ac/ax compliant devices can transmit on the higher 5 GHz frequency band. The band is divided into four sub-bands: the first two 100 MHz wide bands span from 5.150 GHz to 5.250 GHz and 5.250 GHz to 5.350 GHz, the third 255 MHz wide band spans from 5.470 GHz to 5.725 GHz, and the fourth band spans 125 MHz wide from 5.725 GHz to 5.850 GHz. Depending on the regional regulatory bodies, the four bands can have different designations. In literature, the sub-bands are often referred to as the Unlicensed National Information Infrastructure (U-NII) bands: U-NII-1, U-NII-2A, U-NII-2C, and U-NII-3, defined by the United States Federal Communications Commission (FCC). For the sake of clarity, we will use these designations when referring to the 5 GHz sub-bands.

The designated frequency bands are divided into 20 MHz segments known as channels. These 20 MHz wide channels are used for the data transmissions between devices. An 802.11 channel is a range of frequency with a designated centre frequency and 10 MHz of space on both sides of the centre frequency, making up one 20 MHz channel. For instance, channel six on the 2.4 GHz band spans from 2427 MHz to 2447 MHz with a centre frequency of 2437 MHz. The original 802.11 standard and the now legacy 802.11b amendment defined 22 MHz wide channels on the 2.4 GHz band due to the application of a different modulation technique.

The 802.11 standard divides the 2.4 GHz frequency band into 14 channels, numbered from 1 to 14, each channel designated by its centre frequency (Fig. 1). The 5 GHz band is divided into 25 channels: the U-NII-1 and U-NII-2A frequency ranges both hold four 20 MHz channels, the U-NII-2C range holds 12 channels in total, and five channels reside on the U-NII-3 range. The channel numbering scheme on the UNII bands increments the channel number by four: U-NII-1 and U-NII-2A hold channels 36 to 64, U-NII-2C channels 100 to 144, and U-NII-3 channels 149 to 165 (Table 1).

Local regulatory bodies, such as the FCC in the US and the European Telecommunications Standards Institute (ETSI), define which channels are available for use. In most regions, channels either from 1 to 11 or 1 to 13 are permitted on the 2.4 GHz band. Japan is the only region that has permitted the use of channel 14, although only for 802.11b communication. Channel use and availability on the 5 GHz band are considerably more regulated and can greatly differ depending on the local regulations. Many of the regulations consider transmit power limitations as well as restrictions on channel indoor and outdoor use. Furthermore, in many regions, devices operating on the U-NII-2 frequency ranges must use Dynamic Frequency Selection (DFS) to avoid interference with varying radar systems operating on the frequency band. DFS allows WLAN devices to operate on the U-NII-2 frequencies without causing harmful interference. When a DFS capable WLAN access point operating in the U-NII-2 frequency range detects a radar, it halts its operations and migrates to a non-DFS channel to avoid interference. 802.11 operations are not limited to the 20 MHz wide channels. 802.11n/ac/ax compatible devices can be set to operate on 40 MHz wide channels by bonding two 20 MHz channels, doubling the frequency band available for transmissions. In addition, the 802.11ac amendment introduced 80 MHz and 160 MHz channel widths. Just as a 40 MHz channel is created by bonding two 20 MHz channels, an 80 MHz channel bonds together two 40 MHz channels and so on. Because of the limited frequency space, the use of 40 MHz channels is not generally recommended on the 2.4 GHz band.

The channel centre frequencies on the 2.4 GHz band are spaced only 5 MHz apart, causing the channel frequencies to overlap. Channel 14 is an exception to this as its designated centre frequency is 12 MHz apart from channel 13's centre frequency. The channel centre frequencies on the 5 GHz band are spaced 20 MHz apart and are all considered non-overlapping. The 802.11 standard dictates that channels on the 2.4 GHz band are considered non-overlapping if their centre frequencies are separated by 25 MHz, leaving room for three non-overlapping channels. Channels 1, 6 and 11 are commonly referred to as the three non-overlapping channels on the 2.4 GHz band, although other combinations are possible in regions where 13 channels are available. When multiple networks within range operate on the same or adjacent channels, network performance degrades due to interfering transmission.

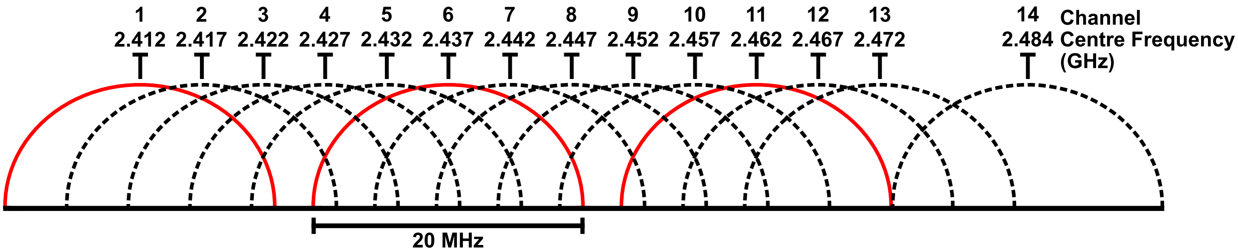


FIGURE 1. Channel designation on the 2.4 GHz frequency band. Non-overlapping channel frequencies in red.

TABLE 1. The 5 GHz frequency band channel designation.

Channel Width	20 MHz	40 MHz	80 MHz	160 MHz
U-NII-1	36	38	42	50
	40			
	44	46		
	48			
U-NII-2A	52	54	58	
	56			
	60	62		
	64			
U-NII-2C	100	102	106	114
	104			
	108	110		
	112			
	116	118	122	
	120			
	124	126		
	128			
	132	134	138	
	136			
	140	142		
	144			
U-NII-3	149	151	155	
	153			
	157	159		
	161			
	165			

B. INTERFERENCE

WLAN networks are half-duplex, meaning that devices cannot transmit and receive data simultaneously and only one device at a time can transmit on the medium. Simultaneous transmissions in the shared frequency band corrupt the transmitted signals, resulting in data loss. To avoid colliding transmissions, WLAN devices use the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) medium access scheme to contend for the wireless medium. When a transmitting WLAN device has determined that the medium is idle, it will choose a random backoff value. The device will then wait for a period of time, based on the backoff value, before transmitting. The device keeps physically monitoring the medium during the backoff time to ensure that no other device begins to transmit. The backoff time value decreases only if the medium is inactive, otherwise, the value is maintained. When the backoff time is depleted, and no activity is detected on the medium, the device can start transmitting. If the medium is active after the timer is depleted, the process resets and a new backoff time is calculated.

Despite the CSMA/CA mechanism, collisions do still occur. Because the transmitting device cannot detect if a collision has occurred, the receiving device must acknowledge the transmitting device that the transmission was successfully received. After a successful transmission, the receiver sends an acknowledgement frame (ACK) to the transmitting device. If the transmitting device does not receive the acknowledgement, it will assume that a collision has ensued and retransmits the original frame, repeating the CSMA/CA procedure.

The 802.11 WLAN standard defines technologies for the bottom layers of the Open Systems Interconnection (OSI) network model: the Physical (PHY) layer and the Medium Access Control (MAC) sublayer of the Data Link layer. The MAC sublayer acts as an interface between the bottom 802.11 PHY layer and the higher layers of the OSI model. The MAC layer operations are responsible for upper-layer data encapsulation, medium access control, security, and data integrity. When an upper-layer data unit is passed to the MAC layer, the upper-layer data is encrypted and encapsulated between the MAC header and Frame Check Sequence (FCS). The FCS is used for data integrity validation, whereas the MAC header contains addressing information as well as frame and sequence control information.

In addition to data transmission, the 802.11 PHY layer operations sense the wireless medium for RF activity and prepare the upper layer data for transmission. Before transmitting the data frame, the transmitting device physically senses RF activity on the medium. If the medium is deemed idle by the transmitting device and its back-off time has depleted, a preamble is sent to the receiving device to synchronise the devices for the incoming transmissions. Data is then transmitted over the wireless medium as series of ones and zeroes modulated onto an RF signal. A receiving device reverses the process and encapsulates data from the demodulated signal for the MAC layer, which in turn passes the data to the upper layers.

Most of the issues that degrade WLAN network performance are related to PHY layer complications, which in turn affect the MAC layer operations. Degradation of RF signals on the PHY layer due to distance, obstacles and interfering signals leads to a situation where the MAC layer frames are retransmitted repeatedly, causing the network's overall throughput to degrade. For instance, If a non-WLAN device operating on the WLAN frequency band is transmitting a strong signal, the interfering RF signal will corrupt WLAN transmissions, leading to excessive frame retransmissions. Furthermore, poor signal conditions force communicating devices to downgrade the used modulation scheme, lowering the network data rate. If a strong enough signal is emitted by an interfering device, WLAN devices will sense the signal during CSMA/CA procedures and defer from transmitting altogether.

When nearby WLAN networks are set to operate on overlapping frequencies, they cause Adjacent Channel Interference (ACI). As discussed in the previous section, there are only three channels on the 2.4 GHz band with non-overlapping frequencies. WLAN networks operating on overlapping adjacent channels cause devices to defer from transmitting and corrupt transmission due to RF interference, leading to unnecessary medium contention, frame retransmissions, and low data rates. ACI is generally not an issue on the 5 GHz band as the channel centre frequencies are farther apart, although channel frequencies will overlap if channel bonding is used.

On the other hand, setting neighbouring networks to operate on the same channel causes Co-Channel Interference (CCI), leading to unnecessary medium contention. When devices hear a transmission on the wireless channel, they must defer from transmitting. Even though the devices are operating as dictated by the CSMA/CA mechanisms, the increased channel contention can severely degrade network performance. Although the effects of CCI could be reduced with proper channel coordination and planning, it is simply unavoidable in densely populated environments when operating on the 2.4 GHz band.

Interference caused by overpopulation of the limited frequency space on the 2.4 GHz band is one of the major causes of poor WLAN performance. Despite the efforts to guide users toward the less congested 5 GHz band, 2.4 GHz has kept its place as the most used frequency. When a multitude of devices operate on the limited frequency space, the possibility for collisions and signal corruption increases, causing excessive MAC layer frame retransmissions that degrade network throughput. Moreover, in a highly congested environment, more time it takes for a single device to get its turn to transmit due to the CSMA/CA medium access procedures, further decreasing network performance. This can become a problem in urban environments where vast numbers of WLAN APs and client devices operate in close proximity.

III. METHODOLOGY

The WLAN survey methodology used in this article is based on a passive wireless network scanning method known as wardriving. The survey system (Fig. 2) is built on common off-the-shelf hardware and freely available software. A comprehensive description of our WLAN survey methodology is presented in our previous work [16] where we discuss in detail the different stages of the WLAN survey process, the required hardware and software and the legality and moral aspects of wardriving. Here we will briefly introduce the principles of wardriving and describe the used WLAN survey methodology.

The term wardriving is derived from the "wardialing" technique introduced in the movie Wargames in 1983 [17]. The lead character in the movie used his computer to detect other network-enabled computer systems by automatically dialling phone numbers in an increasing sequence. In the 1980s, computer networking from remote locations was managed by modems utilising the traditional telephone system. This kind of connectivity made it possible to identify network-enabled computers simply by dialling phone numbers and assessing whether there was another modem responding to the phone call or not. Wardriving takes the method to the modern ages: instead of dialling phone numbers, one can use a WLAN-enabled computer to detect all nearby wireless networks.

To put it simply, wardriving means moving around some chosen geographical region and recording data of the discovered WLAN devices and networks while moving. The gained results are then gathered into databases for statistical purposes. It is also common to visualise the locations of the surveyed networks on a map based on GPS location data. There are two main ways of surveying WLAN networks: passive methods and active methods. With active methods, the scanning system always interacts with the target networks it is surveying. The active interaction may include techniques like sending probe request frames and gathering data from probe responses from the nearby WLAN routers. This method is analogous to the traditional telephone wardialing where an attempt to discover remote systems is made by progressively dialling sequential telephone numbers and storing information for each number where a modem picks up the call.

In passive wireless network scanning, the scanner does not interact with the surrounding networks. The network scanner simply listens to the wireless traffic and extracts information from the wireless networking frames. For example, WLAN devices broadcast beacon frames at regular intervals to announce their presence to other surrounding devices. These frames carry varying information such as the wireless network Service Set Identifier (SSID), supported encryption protocol, used wireless channel, and the device MAC address. For the wireless network scanner to be able to scan the entire WLAN wireless spectrum, the Wireless Network Interface Controller (WNIC) must be set to monitor mode. While in monitor mode, the WNIC can utilise channel hopping to scan all wireless channels available in the spectrum for WLAN devices and networks. In this process, the frames broadcasted by nearby systems can be harvested for information regarding the network they are connected to. The passive WLAN scanning process is analogous to performing a scan of the FM frequency to find broadcasting radio channels.

The term wardriving may sound intimidating to some and thus, the activity may be interpreted by some as malicious with an aim to intrude wireless networks. It is however, quite the opposite: while wardriving could be a part of an attempt to break the security of WLAN networks, it is not per se a criminal act. In fact, wardriving itself is harmless to the surveyed networks, and security professionals as well as hobbyists commonly use it legitimately as a tool for research and analysis. Obviously, while legal, some moral questions still arise concerning the privacy and consent of WLAN network

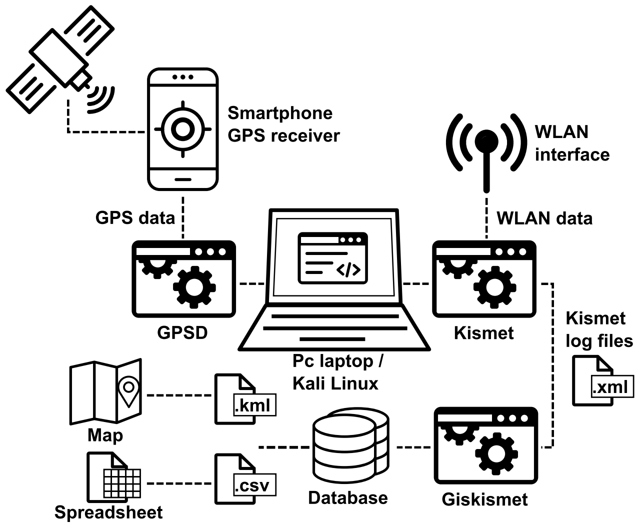


FIGURE 2. The WLAN survey scheme.

owners, and these should be taken into consideration in the process.

We divide the WLAN survey process into three stages: planning and preparation, data collection and data analysis. During the planning and preparation stage, the survey location, mode of transportation, hardware and software are chosen and prepared. Furthermore, as laws and regulations can differ between regions, the legality of surveying WLAN networks is ensured in the planning stage. During the data collection stage, the wardriver surveys the surrounding wireless networks within the predetermined area. After the area has been thoroughly surveyed, the collected data is further processed and analysed. During the data analysis stage, the collected survey data is compiled into databases and refined into statistics. If the wardriving process is accompanied with location (GPS) data collection, the geographical locations of the detected WLANs can be visualised in services like Google Earth or WiGLE.net.

A. THE WLAN SURVEY SYSTEM

The hardware used in our system is composed of a PC laptop, a USB powered WNIC with dual-band capability, and an Android phone for receiving location data (GPS). In this study, we used the TP-Link AC600 Archer T2UH as the WNIC. The WNIC chipset was Mediatek MT610U.

As the survey platform, we have used the Debian based Kali Linux operating system running as a virtualised guest host on top of the laptop's main Windows 10 operating system. VMware Workstation Player was used as the hypervisor software to virtualise the guest operating system. From the Kali Linux software library, the open-source wireless network detector Kismet was used as the WLAN survey software [18], [19]. To incorporate GPS location data with the survey results, the Global Positioning System Daemon (GPSD) was used for collecting GPS location data during the survey sessions [17].

B. SURVEY DATA ACQUISITION AND ANALYSIS

For this article, data from nine WLAN surveys carried out in May 2019, February 2020, June 2020, October 2020, January 2021, March 2021, June 2021 and October 2021 and January 2022 was analysed. The surveys were conducted in the city of Salo, located in southwestern Finland, 155 kilometres west of the capital Helsinki. We chose three different areas within the city to carry out the surveys. By surveying three distinct locations within the city, it is possible to form a more comprehensive picture of the city's WLAN landscape. The three survey locations: the industrial district, the city centre, and the suburb were chosen to represent different locations for typical WLAN deployment and usage.

- Industrial district route (2.9 km): along this route, there are very few private homes. The buildings in the area mostly host commercial operators ranging from gyms, technology start-ups and automotive dealerships to metal workshops
- City centre route (3.7 km): the city centre buildings host private homes as well as administrative officials. In this survey area, in addition to private homes, there are service sector businesses such as restaurants, clubs and florists, and also the market square, a police station and the town hall reside on this route.
- Suburban route (2.2 km): in this area, there are only detached houses and small condominiums that are private homes. The area is considerably more scarcely populated than the city centre.

During each survey session, the locations have been surveyed three consecutive times to ensure the best possible results. After each survey session, the collected data has been imported into SQLite databases. Data from the databases has then been parsed into.csv files and turned into spreadsheets for further statistical analysis.

To forecast frequency band utilisation evolvement in the survey area based on the collected data, a simple linear regression model was produced. Linear regression models are used to establish if there is a statistically significant relationship between two variables. The simple linear regression model $y = \beta_0 + \beta_1 x$ can be used to forecast the future values of the dependent value y based on the known values of the independent variable x. The y-intercept of the regression model β_0 and the slope of the model β_1 are produced by the following formulas where y is the dependent value, x is the independent value and n is the number of observations:

$$\beta_1 = \frac{n\sum x_i y_i - (\sum x_i)(\sum y_i)}{n\sum x_i^2 - (\sum x_i)^2}, \quad \beta_0 = \frac{\sum y_i - \beta_1 \sum x_i}{n}$$

IV. RESULTS

In the following we present the results of the long-term WLAN survey study on the evolvement of WLAN frequency band and channel usage. The overall network deployment in the survey region increased by 64% from 1067 detected networks at the beginning of the survey in May 2019 to 1753 in January 2022 (Table 3). An average of 40 networks per survey

TABLE 2. Frequency band utilisation in the survey areas.

	Industrial district			City centre			Suburb		
	2.4 GHz band	5 GHz band	Total	2.4 GHz band	5 GHz band	Total	2.4 GHz band	5 GHz band	Total
May 2019	163	41	204	514	196	710	124	29	153
February 2020	174	64	238	569	213	782	147	26	173
June 2020	186	69	255	516	195	711	112	17	129
October 2020	226	84	310	604	224	828	131	20	151
January 2021	254	135	389	637	286	923	148	32	180
March 2021	247	101	348	677	306	983	151	40	191
June 2021	245	122	367	685	359	1044	147	36	183
October 2021	242	100	342	701	370	1071	148	58	206
January 2022	236	137	373	730	429	1159	171	50	221
Increase	45%	234%	82.8%	42%	119%	63%	38 %	72%	44%

TABLE 3. Overall frequency band utilisation in the survey region.

	2.4 GHz band	5 GHz band	Total
May 2019	801	266	1067
February 2020	890	303	1193
June 2020	814	281	1095
October 2020	961	328	1289
January 2021	1036	453	1489
March 2021	1075	447	1522
June 2021	1075	517	1592
October 2021	1090	528	1618
January 2022	1137	616	1753
Increase	42%	132%	64%

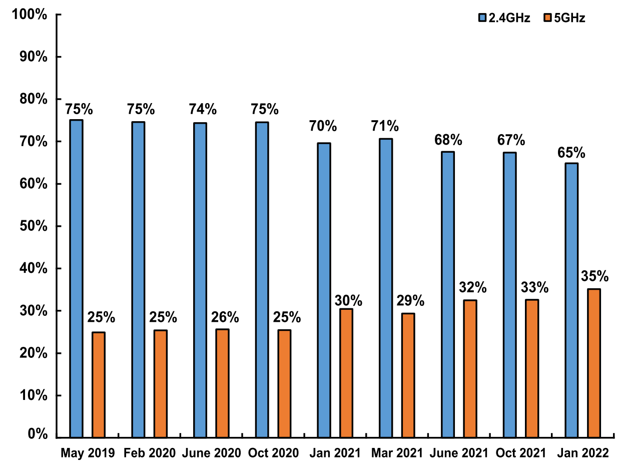


FIGURE 3. Frequency band utilisation evolvement during the survey period.

session were omitted from the survey results due to missing channel information. The missing channel information could be a consequence of frame loss or misinterpretation due to poor signal conditions during the survey.

The survey results show a 132% increase in 5 GHz utilisation from the start of the survey, increasing from 266 networks in May 2019 to 616 in January 2022 (Table 3). A major increase in the number of 5 GHz networks occurred between October 2020 and January 2021, when the number of networks increased by 38% from 328 to 453. Network deployment on the 2.4 GHz band was relatively modest, increasing by 42% from the start of the survey. At the end of the study, 35% of all detected networks operated at 5 GHz, compared to 25% at the beginning of the study (Fig. 3). Of the three survey areas (Table 2), the greatest change was observed in the industrial district, where 5 GHz band utilisation and network deployment increased by over 234% and 83%, respectively. In the city centre, utilisation of the 5 GHz band increased by 119%, and the overall network deployment increased by 63%. While the growth in 5 GHz band utilisation was steady in the industrial district and city centre areas, results in the suburb varied during the survey period. The number of 5 GHz networks in the area peaked at 58 in October 2021, doubling from 29 networking in May 2019.

A simple linear regression model was produced to forecast the utilisation of the 2.4 GHz and 5 GHz frequency bands (Fig.4). For the model, time t in months was used as the independent variable and the percentages of 2.4 GHz and 5 GHz networks presented in Fig. 3 were used as the dependent variable. The linear regression equation for the forecasts on the 2.4 GHz band was $\hat{y} = -0.00344t + 0.7733$ and $\hat{y} = 0.03442t+0.2266$ for the 5 GHz band. The statistical significance of the regression model was proven by evaluating the coefficient of determination value $R^2 = 0, 8144$. Based on our regression model, the portion of 5 GHz networks was predicted to reach the level of 2.4 GHz networks by autumn of 2025.

Fig. 5 shows the average number of devices per channel at 2.4 GHz and 5 GHz. Unsurprisingly, the majority of networks operating on the 2.4 GHz band were set on the three non-overlapping channels 1, 6 and 11, channel one being the most popular of the three (Fig. 5a). On average, roughly two-thirds of the detected networks on the 2.4 GHz band operated on the three non-overlapping channels. Similarly, nearly two-thirds of the detected networks operating on the 5 GHz band were set on the U-NII-1 sub-band channels 36-48, a clear majority operating on channel 36 (Fig. 5b). On average, 167 networks operated on channel 36, while an average of 40 networks utilised the second most popular channel 52.

V. DISCUSSION

Our survey results show a significant increase in 5 GHz band utilisation, confirming our hypothesis. At the beginning of the survey, networks operating on the 2.4 GHz band outnumbered networks on the 5 GHz band three to one, when at the end of the study, the ratio was two to one. The number of networks operating on the 5 GHz band more than doubled during

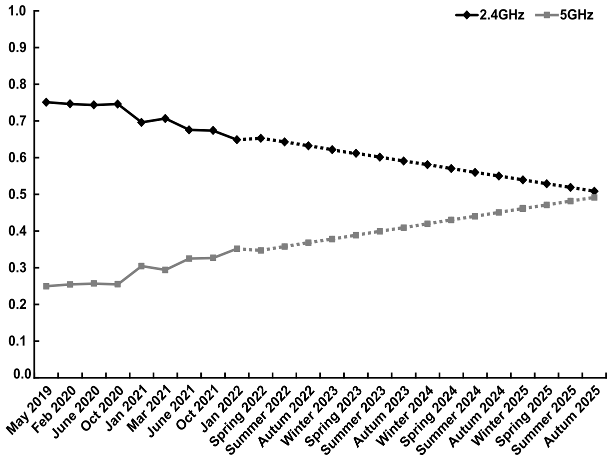
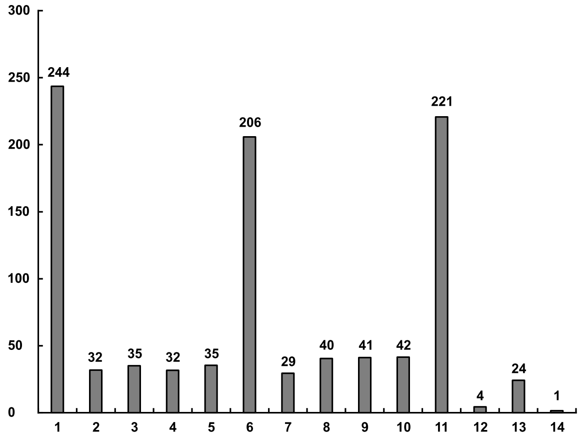
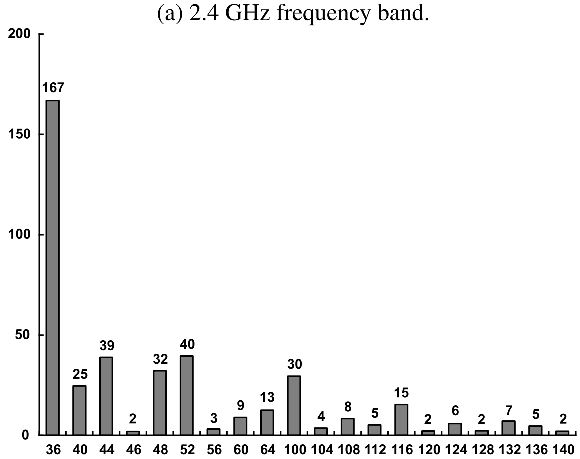


FIGURE 4. **Frequency band utilisation forecast. Forecast values on the dotted line.**



(a) 2.4 GHz frequency band.



(b) 5 GHz frequency band.

FIGURE 5. **Average number of devices per channel.**

the survey, while network deployment on the 2.4 GHz band saw a 42% increase. Of the three individual survey areas, the greatest change was observed in the industrial district, where 5 GHz band utilisation tripled. The substantial growth of 5 GHz band utilisation can be attributed to the fact that devices compliant with the latest 802.11 standard amendments are replacing outdated WLAN devices. This change also contributes to the increased 2.4 GHz band utilisation as most current AP's are capable of operating simultaneously on both frequency bands.

Analysis of WLAN channel utilisation on the 2.4 GHz band did not present any abnormalities. On the 2.4 GHz band, the majority of the detected networks operated on the non-overlapping channels 1, 6 and 11. On the 5 GHz band, channel 36 was the most populated. The popularity of channels 1, 6, 11 and 36 is to be expected as it is common for manufacturers to set devices on these channels as default due to availability in all regions. The high utilisation of the three non-overlapping channels on the 2.4 GHz is a positive result as the effects of co-channel interference are preferable over adjacent channel interference. On the 5 GHz band, the clear overpopulation of channel 36 can cause unnecessary co-channel interference as there are multiple less crowded non-overlapping channels available. Devices operating on the higher frequency band should be more evenly divided between channels to mitigate the effects of interfering transmissions.

The increase trend in 5 GHz utilisation is believed to be even higher than we have predicted based on the data. As higher frequency signals are more susceptible to attenuation when passing through solid objects, several networks operating on the 5 GHz band were potentially left undetected during the survey. Although an increasing number of networks are operating on the 5 GHz band, it does not mean that the number of devices operating on 2.4 GHz will decrease. While most WLAN AP's compliant with the latest 802.11 amendments operate on both frequency bands, many of the current client devices operate only at 2.4 GHz due to lower manufacturing costs, further consolidating the band's popularity. To decrease congestion on the 2.4 GHz band, it would be advisable to migrate 5 GHz capable devices onto the higher frequency band and utilise the 2.4 GHz band for low data rate applications.

VI. CONCLUSION

Because of severe overcrowding of the 2.4 GHz frequency band, WLAN performance degrading interference has become unavoidable in densely populated environments. Despite the efforts to guide users' toward the wider less congested 5 GHz band, the 2.4 GHz band has retained its position as the primary frequency band in WLAN communication. Evident solutions to the problem would be to migrate all capable devices over to the 5 GHz frequency band and proper channel selection.

The long-term analysis and data of WLAN frequency band and channel utilisation evolvement we have presented in this article is unique, and to the best of our knowledge, no similar studies have been previously published. Our survey data shows a significant increase in 5 GHz band utilisation in the survey region, indicating that older WLAN AP's are being replaced by the common consumer. Still, although 5 GHz utilisation more than doubled during the survey, at the same time, the number of 2.4 GHz networks increased by 42%.

Furthermore, at the end of the study, the number of networks operating at 2.4 GHz still outnumbered 5 GHz networks two to one. Based on our simple linear regressions model forecast, the portion of 5 GHz networks in the survey region is predicted to reach the level of 2.4 GHz by late 2025. Despite the increasing trend in 5 GHz band utilisation, to ease congestion on the 2.4 GHz band, more efforts should be put into increasing user's awareness and acceptance of the higher frequency band. In our future work, we will continue to follow the long-term evolvement of the WLAN landscape and examine the types and features of the detected WLAN devices in more detail.

REFERENCES

[1] W. Lemstra, V. Hayes, and J. Groenewegen, *The Innov. Journey Wi-Fi: The Road to Global Success*, 1st ed. Cambridge, U.K.: Cambridge Univ. Press, 2011.

[2] (2019). Businesswire. *Smart Home Will Drive Third Wave in Wireless Home Evolution Strategy Analytics*. Accessed: Apr. 1, 2022. [Online]. Available: https://www.businesswire.com/news/home/20190807005530/en/Smart-Home-Drive-Wave-Wireless-Home-Evolution

[3] (2021). Wi-Fi. *Wi-Fi Global Economic Value to Reach $5 Trillion in 2025*. Accessed: Apr. 1, 2022. [Online]. Available: https://www.wi-fi.org/news-events/newsroom/wi-fi-global-economic-value-to-reach-5-trillion-in-2025

[4] A. Nisbet, "A tale of four cities: Wireless security & growth in new Zealand," in *Proc. Int. Conf. Comput., Netw. Commun. (ICNC)*, Maui, HI, USA, Jan. 2012, pp. 1167–1171.

[5] A. Nisbet, "A 2013 study of wireless network security in New Zealand: Are we there yet?" in *Proc. 11th Austral. Inf. Secur. Manage. Conf. (ISM)*, Perth, WA, Australia, 2013, pp. 75–82.

[6] A. Sarrafzadeh and H. Sathu, "Wireless LAN security status changes in Auckland CBD: A case study," in *Proc. IEEE Int. Conf. Comput. Intell. Comput. Res. (ICCIC)*, Madurai, India, Dec. 2015, pp. 1–6.

[7] H. Valchanov, J. Edikyan, and V. Aleksieva, "A study of Wi-Fi security in city environment," in *Proc. IOP Conf. Mater. Sci. Eng.*, vol. 618, no. 1, Oct. 2019, Art. no. 012031.

[8] C. L. Leca, "Overview of Romania 802.11Wireless security & statistics," *ICST Trans. Secur. Saf.*, vol. 4, no. 12, Dec. 2017, Art. no. 153518.

[9] D. Dobrilovic, Z. Stojanov, S. Jäger, and Z. Rajnai, "A method for comparing and analyzing wireless security situations in two capital cities," *Acta Polytechnica Hungarica*, vol. 13, pp. 67–86, Jan. 2016.

[10] H. Li, K. Wu, Q. Zhang, and L. M. Ni, "CUTS: Improving channel utilization in both time and spatial domains in WLANs," in *Proc. IEEE INFOCOM*, Turin, Italy, Apr. 2013, pp. 1564–1572.

[11] F. Maturi, F. Gringoli, and R. L. Cigno, "A dynamic and autonomous channel selection strategy for interference avoidance in 802.11," in *Proc. Annu. Conf. Wireless Demand Netw. Syst. Services*, Jackson, WY, USA, Feb. 2017, pp. 1–8.

[12] D. Saliba, R. Imad, and S. Houcke, "WiFi channel selection based on load criteria," in *Proc. 20th Int. Symp. Wireless Pers. Multimedia Commun. (WPMC)*, Bali, Indonesia, Dec. 2017, pp. 332–336.

[13] V. P. Mhatre, K. Papagiannaki, and F. Baccelli, "Interference mitigation through power control in high density 802.11 WLANs," in *Proc. IEEE Int. Conf. Comput. Commun. (INFOCOM)*, Anchorage, AK, USA, May 2007, pp. 535–543.

[14] A. Akella, G. Judd, S. Seshan, and P. Steenkiste, "Self-management in chaotic wireless deployments," in *Proc. 11th Annu. Int. Conf. Mobile Comput. Netw. (MobiCom)*, Cologne, Germany, 2005, pp. 185–199.

[15] M. Haidar, R. Ghimire, H. Al-Rizzo, R. Akl, and Y. Chan, "Channel assignment in an IEEE 802.11 WLAN based on signal-to-interference ratio," in *Proc. Can. Conf. Electr. Comput. Eng.*, Niagara Falls, ON, Canada, May 2008, pp. 1169–1174.

[16] S. Lindroos, A. Hakkala, and S. Virtanen, "A systematic methodology for continuous WLAN abundance and security analysis," *Comput. Netw.*, vol. 197, Oct. 2021, Art. no. 108359.

[17] C. Hurley, R. Rogers, F. Thornton, D. Connelly, and B. Baker, *WarDriving and Wireless Penetration Testing*, 1st ed. Rockland, MA, USA: Syngress Publishing, 2007.

[18] B. Sak and R. J. Raghu, *Mastering Kali Linux Wireless Pentesting*, 1st ed. Birmingham, U.K.: Packt Publishing, 2016.

[19] J. Cache, J. Wright, and V. Liu, *Hacking Exposed Wireless, Second Edition: Wireless Security Secrets and Solutions*, 2nd ed. New York, NY, USA: McGraw-Hill, 2010.

SAKU LINDROOS received the B.B.A. degree in business communication and information security from the Turku University of Applied Sciences, Turku, Finland, in 2014, and the M.Sc. (Tech.) degree in networked systems security from the University of Turku, Finland, in 2020, where he is currently pursuing the D.Sc. (Tech.) degree in communication engineering with the Department of Computing. He holds the occupation of a Project Researcher with the University of Turku. His research interests include wireless network security, security and privacy in communication systems, ethical hacking, and computer ethics.

ANTTI HAKKALA received the D.Sc. (Tech.) degree in communication systems from the University of Turku, Finland, in 2017. He is currently a University Teacher in communication systems and cyber security with the Department of Computing, University of Turku. He has over ten year's experience in teaching engineering students on cyber security and communication systems engineering and has supervised over 100 bachelor's and master's theses on cyber security topics. His current research interests include wireless network security, cyber security in autonomous systems, and security and privacy in networked information society.

SEPPO VIRTANEN (Senior Member, IEEE) received the D.Sc. (Tech.) degree in communication systems from the University of Turku, Finland, in 2004. He is currently an Associate Professor in cyber security engineering with the Department of Computing, University of Turku, where he is also the Vice Head of the Department. He has supervised five Ph.D. theses and more than 130 master's theses to completion. His current research interests include cyber security in smart environments, secure network and communication technology, and security technologies for IoT.