Masarykova univerzita
Fakulta informatiky

Autoconfiguration in distributed wireless environment

Diploma Thesis

Bc. Tomáš Szaniszlo

Brno, spring 2014

Declaration

Hereby I declare, that this paper is my original authorial work, which I have worked out by my own. All sources, references and literature used or excerpted during elaboration of this work are properly cited and listed in complete reference to the due source.

Bc. Tomáš Szaniszlo

Advisor: RNDr. Jan Kasprzak

Acknowledgement

I would like to thank my thesis advisor RNDr. Jan Kasprzak and my consultant Mgr. Ondrej Faměra for their supervision throughout my work on the thesis, suggestions to its structure, valuable critical comments and practical discussions.

Abstract

In this work an overview of 802.11 networks and their management tools or systems is presented. Further it focuses on description of its physical layer and interference in these networks. Centralized and distributed algorithms for automatic access point channel allocation are designed and implemented. The implementations are compared with manual channel allocation and practically tested in the faculty environment.

Keywords

wireless networks, 802.11, radio frequency, channel allocation, auto-configuration, access points

Contents

1 Introduction

Today end user networks rely more and more on wireless transmission of data compared to wired networks. Modern environment places emphasis on mobility of users who ask for as much uninterrupted connection to the Internet as possible. One of the factors that only supports this development is more and more pervasive presence of networking-capable devices. Due to their continuing miniaturisation, they become so ubiquitous and their power and possibilities significantly increase with the possibility of network connection. This has led to a situation where it is an expected norm for the environment to provide the present devices with Internet access.

There are multiple ways to achieve this goal – mobile networks or Wi-Fi networks to name the two most common ones. These technologies for offering access to network are used in their centralized variant where there is a backbone of distribution network and the clients connect at its outlets, here represented by access points (AP) or base transceiver stations (BTS). Alongside exist also less known alternatives as mesh networks which are nowadays getting in the scope of interest. Mesh networks offer a viable alternative for scenarios where the distribution of connectivity in centralized manner is hard to achieve. [13][21] This is usually due to technological or cost factor.

One of the important aspects of not only a wireless network, but of any network in general, is the quality of service. This characteristic is a complex measure of the quality of network which can be decomposed into multiple simpler metrics like availability, stability, throughput or delay.

This work focuses on 802.11 wireless networks with centralized components – access points – and its aim is to improve the quality of service by making automatic adjustments to the radio configuration of access points.

Radio configuration offers multiple ways of tweaking. The most basic include radio frequency changing, transmission (Tx) power adjustment or antenna orientation adjustment, while techniques such as beamforming, high throughput feature belong to the more advanced ones. Some of these techniques will be described in more

detail in the following chapters.

1.1 Contents outline

In the second chapter of this work we describe networks based on 802.11 standard starting from its general overview, through its various revisions adding significant improvements over the first release. Then we provide some introduction to the more physical and legislative aspects of using 802.11 networks.

The third chapter focuses on the ways of managing these networks. We introduce general ideas and requirements for such systems, continuing with a description of selected management systems and their properties.

The fourth chapter consists of theoretical ideas behind the main aim of the work, i.e. the autoconfiguration of radio frequencies. Theoretical considerations are elaborated on and different approaches to the problem are introduced. Design and analysis of two developed algorithms from different classes of solutions to tackle the problem are presented – centralized and distributed one.

Description of the faculty environment, for which is this work primarily targeted is present in the fourth chapter. Deployment results of the algorithms designed in the fourth chapter to real-world are presented in the fifth chapter together with some implementation notes and importantly, comparison of achieved results by the current, centralized and distributed system. Last part of the chapter is devoted to the discussion of these findings.

The sixth chapter mentions summarizes the results presented in this work and their impact.

2 802.11 networks

2.1 Basic overview

802.11 networks, more commonly known as Wi-Fi (Wireless-Fidelity) networks, represent an ubiquitous form of data transfer over wireless media for low to midrange distances. They are standardized in a set of documents maintained by the Institute of Electrical and Electronics Engineers (IEEE). While IEEE is responsible for designing specifications and requirements for devices using these networks, it does not act as a certification organization that tests conformance of these devices to the standards. This role belongs to Wi-Fi Alliance which is a trade association of numerous manufacturers that also promotes the technology and its adoption.

From the architectural point of view, 802.11 networks offer a few ways of connecting wireless nodes together.

Client-server architecture. The most commonly seen one where there is one central point – access point – and multiple 802.11 wireless clients may connect to it. The access point is usually serves as an entry point to the Internet or local network.

Ad hoc architecture. This architecture is used for connecting two clients together, e.g. to facilitate transfer of data.

Mesh network. Mesh network is a configuration which creates a peer-to-peer arrangement and consists of multiple nodes. Each of these nodes is connected to one or more of other nodes.

The scope of 802.11 standards are physical and data link layers of the ISO/OSI networking model. Therefore its primary objectives are to specify the used radio frequencies, signal encoding, media utilization, nodes addressing, frame format and so on.

Depending on the used revision, 802.11 network allows connections to work in various frequency bands, most often in 2.4 GHz or 5 GHz band, and commonly used variants offer throughput up to 600 Mbps. Connections can be protected using several cryptographic protocols or improved using various techniques like beamforming. 802.11 networks also offer provisions for mobile clients.

2.2 History and revisions

The wonderful thing about standards is that there are so many of them to choose from.
The Unix-Haters Handbook

Soon after the advent of first computers, the need and advantages of connecting them together have been recognized. The first more widespread networks based on telephone connections appeared in 1960s, one example being dataphones from AT&T. [9] However due to its inherent distance limits, it was not deployable in scenarios where the locations to be connected were spread far apart.

2.2.1 ALOHANET

This was the case of computer systems at the University of Hawaii. Computers located at the main island Oahu could not reliably communicate with those on other islands located from 20 to 300 kilometres further. To solve these problems, a new kind of network – ALOHANET – was developed in 1971. ALOHANET offered bandwidth of 24 kBd using band around 400 MHz. [1] It also pioneered Multiple Access (MA) channel access method, later reused in many following networks. [20]

2.2.2 HiperLAN

The next significant moment came in the beginning of 1990s when two competing standards for wireless Local Area Networks appeared. One standard was U.S.-based 802.11 developed by IEEE and it was the precursor of 802.11 as we know it now. The other alternative was Europe-based standard High Performance Radio LAN (HiperLAN) by European Telecommunications Standards Institute (ETSI).

HiperLAN was similar to original 802.11 standard but worked in 5 and 7 GHz bands and it offered more features than 802.11. Although having clear functional advantages, they actually hampered its adoption due to its complexity and implementation cost in favour of 802.11 and HiperLAN got obsoleted soon. However, after industry

accepted 802.11 as the WLAN standard, many of HiperLAN features were later embedded into 802.11.

2.2.3 802.11

From now on we will focus on the 802.11 standard. The first incentive to its development came in 1985 when U.S. Federal Communications Commission allowed unlicensed use of radio bands 900 MHz and 2.4 GHz. [23] This together with the fragmented field of wireless networks led in 1991 to establishment of IEEE LAN MAN Standards Committee with aim to create a common wireless protocol standard.

The first result of the committee came in 1997 when the standard was officially approved as IEEE 802.11-1997. This standard formed the basis of the future 802.11 networks and as a fragment of 802 standards it is titled "Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications".

It was based on the usage of either radio band 2400–2500 MHz utilizing one of Frequency-hopping spread spectrum (FHSS) and Direct sequence spread spectrum (DSSS) techniques or 850–950 nm infrared band. Both bands offered data rate of 1 or 2 Mbps and operational range up to 10 metres. As a media access control mechanism CSMA/CA[1] was chosen. This standard was revised two years later and published as IEEE 802.11-1999. Both 1997 and 1999 standards are now known as IEEE 802.11 legacy.

Further development and improvements of 802.11 legacy standard led to publication of amendments which added new features or improvements. These amendments are designated by lowercase letter as in 802.11g. Each amendment is an incremental document and the features it adds are commonly referred to by its letter. However, at one time, only one current 802.11 standard exists, possibly with a few amendments or recommended practice documents. Every few years, a new iteration of 802.11 standard is published, which incorporates amendments and recommended practices created in the meantime. In the following text we will describe the history of these documents with focus on those related to this work. [19]

1. Carrier Sense Multiple Access, Collision Avoidance – A method for arbitrating access of stations to the medium.

Superseded standards and amendments

- **802.11a – Higher Speed PHY Extension in the 5 GHz Band (1999).** Extends usage of 802.11 into 5 GHz band with data rates from 6 to 54 Mbps using Orthogonal Frequency Division Modulation (OFDM) technique. 5 GHz band was not affected by interference from 802.11 clients and other sources so much as 2.4 GHz which made it easier to achieve higher real speed.

- **802.11b – Higher Speed PHY Extension in the 2.4GHz Band (1999).** Improves data rates in 2.4 GHz bands from 2 Mbps to up to 11 Mbps and no longer offers FHSS modulation technique, leaving DSSS as the only option.

- **802.11d – Operation in Additional Regulatory Domains (2001).** Adds support of per-country regulatory domains which define legislatively allowed characteristics of transmission bands.

- **802.11g – Further Higher Data Rate Extension in the 2.4 GHz Band (2003).** Improves 802.11b bit rates to 11–54 Mbps, on par with 802.11a. Although approved in 2003, it was quickly adopted by manufacturers even before its approval.

- **802.11h – Spectrum and Transmit Power Management Extensions in the 5 GHz Band in Europe (2003).** Adds detection and avoidance of interfering sources in 5 GHz band mostly caused by radars and satellites. To this purpose it introduces Dynamic Frequency Selection (DFS) and Transmit Power Control (TPC) mechanisms.

- **802.11-2007 – 802.11 Standard Maintenance Revision.** Merges amendments a, b, d, g, h, i, j, e of 802.11-1997 into single standard.

- **802.11n – High Throughput (2009).** Increases data rates of transfers over 2.4 and 5 GHz bands to 600 Mbps. This is achieved by increasing bandwidth of communication channels and introducing novel concept of multiple, up to four antennas – multiple-input multiple-output (MIMO).

- **802.11v – Wireless Network Management (2011).** Makes clients aware of the network environment by information exchange, therefore enabling potential improvement of the network as a whole.

Current standards and amendments

- **802.11-2012 – 802.11 Accumulated Maintenance Changes.** Merges amendments k, r, y, w, n, p, z, v, u, s of 802.11-2012 into single standard.
- **802.11ad – Very High Throughput 60GHz (2012).** Extends frequency band of 802.11 to offer data rates 7 Gbps leveraging 2.16 GHz wide communication channels. This revision gained commercial support in form of Wireless Gigabit Alliance (WiGig) trade association.
- **802.11ac – Very High Throughput 6GHz (2013).** Despite its name, this amendment upgrades data rate over 5 GHz band up to 6.77 Gbps by allowing up to 160 MHz wide channels over 8 MIMO streams.

Planned standards and amendments

- **802.11-2015 – ? (2015?).**
- **802.11ah – Sub 1 GHz (2016?).**

Status of 802.11 today

802.11 is a quite complex standard now. To make an illustration of its complexity, the original 802.11-1997 standard had 459 pages and the current 802.11-2012 without current amendments has 2793 pages. Of course, it is not necessary to implement the whole standard; its various parts are often intended for specific or even quite different applications.

The de facto requirements for Wi-Fi devices are set by Wi-Fi Alliance which offers certification programs. Devices that pass this program receive Wi-Fi CERTIFIED label which can be awarded in specific categories like Security, Wi-Fi CERTIFIED ac or Wi-Fi Direct. [27]

2.3 Architecture

In this section we will describe architecture of 802.11 networks in more detail.

From the physical perspective, 802.11 network consists of three main parts – nodes, medium and signal. A node can be any device capable of receiving and transmitting in 802.11 network and adhering to the standard. Wi-Fi devices range from more conventional computers, access points, mobile phones and printers to more peculiar ones as Nabaztag rabbit (information device), refrigerators or even toilets. Ideally, the medium is air, but in real-world deployments the signal between nodes often travels not only through air but it is also attenuated by various obstacles including walls, old wall paints or rain. Information related to the last part of this system, the signal, is covered in the next section.

From the logical perspective, 802.11 network contains stations (STA). Stations are enabled to participate in the network by means of wireless network interface controller (WNIC). Stations are grouped into basic service sets (BSS), a basic building block of 802.11 networks. BSS spans a part of space called Basic Service Area (BSA) in which the stations can communicate with each other. If the network is of a centralized character and contains access point (AP), then the BSS is identified by BSSID which is the MAC address of the access point for the BSS.

The range of access point is limited and together with attenuation of signal due to environmental obstacles, a single AP often does not suffice to fulfil its purpose. In that case multiple access points can be used, each with its own BSS, some of which may overlap. In order to maintain integrity and unity of this network, access points are usually connected together by means of distribution system (DS) which is usually a wired network but can also be a wireless network (wireless distribution network) or they can be connected into a mesh network. Such system of connected BSSes is called Extended service set (ESS) and similarly as BSSes it has assigned an SSID (sometimes denoted ESSID), a string of length at most 32. This concept is illustrated by figure 2.1.

Although mentioned only implicitly, nodes in 802.11 network can assume two roles – a station or an access point. The distinction be-

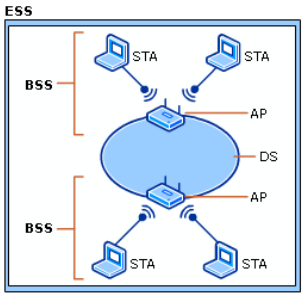

Figure 2.1: BSS and ESS example [22]

tween them is that access points regularly broadcast management frames that enable them to work as the central point of the network and to be found by stations.

2.4 Physical layer

2.4.1 Radio frequency bands

As it has been sketched in the description of 802.11 standards and amendments, there are various ways by which data can be transferred in the medium. For this purpose 802.11 offers multiple frequency bands, modulation techniques, MIMO[2] and other features like High Throughput (HT).

Most common frequency bands, together with other parameters, are summarized in the following table (bit rate is maximum bit rate in Mbps per one stream):

2. Multi-Input Multi-Output – Usage of multiple antennas for transmitting and receiving signal that improves the quality of communication.

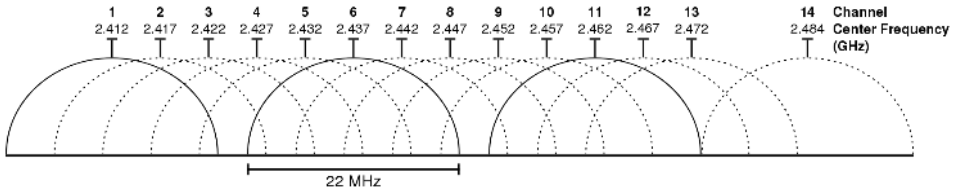

Figure 2.2: Channels in 2.4 GHz band with their power transmission characteristics. [28]

std	band	bw [MHz]	modulation	bit rate	streams
-	2.4 GHz	22	FHSS	2	1
-	900 nm	20	DSSS	2	1
a	5 GHz	20	OFDM	54	1
b	2.4 GHz	22	DSSS	11	1
g	2.4 GHz	20	OFDM, DSSS	54	1
n	2.4 GHz	20/40	OFDM	150	4
n	5 GHz	20/40	OFDM	150	4
ad	60 GHz	2160	SC, OFDM, LPSC	6912	1
ac	6 GHz	20–160	OFDM	867	8

The most commonly encountered bands today are 2.4 GHz and 5 GHz microwave band which we will describe in more detail. Each of these bands is divided into channels which often partially overlap. A channel allows transmission of data stream and is characterized by its central frequency and its width.

The 2.4 GHz band is also called ISM (Industry, Science, Medical) band and it is allocated for unlicensed use. It spans range 2.4–2.5 GHz and for purposes of 802.11 it is divided into 13 channels beginning at 2412 MHz (channel 1), equally spaced by 5 MHz and ending at 2572 MHz (channel 13) as illustrated in figure 2.2. This band is usually quite utilized by multiple access points and further it is subject to various non-802.11 sources of interference like microwaves or Bluetooth.

The other, 5 GHz band, is also called U-NII (Unlicensed National Information Infrastructure) and ranges from 5170 to 5825 GHz. This corresponds to channels from 34 to 165 spaced by 5 MHz, however,

not every channel is allowed for unlicensed use. U-NII band is split into four section – Low, Mid, Worldwide and Upper – and usable channels in each section are are spaced 20 MHz, so only every fourth channel is available.

When using 5 GHz band, coexistence with other non-802.11 devices has to be considered. They include radars, satellites or other networks. Two techniques have been constructed and by amendment h are mandatory for frequencies from 5260 to 5700 MHz due to regulation in Europe and U.S. The first method is DFS (Dynamic Frequency Selection) and it works by selecting channel with low interference, therefore avoiding frequencies used by radars. Another technique is TPC (Transmit Power Control) and it lessens the interference with satellites or other wireless networks by reducing Tx power of the WNIC.

2.4.2 Signal modulation and shape

Depending on the standard/amendment used, the signal can have different characteristics. The only currently used modulations in the 2.4 and 5 GHz bands are DSSS and OFDM.

DSSS (Direct Sequence Spread Spectrum) uses the original signal and composes it with a repeating pattern with much higher frequency. The pattern is already known to the receiver who composes it with received signal again and obtains the original signal. The pattern used is pseudonoise which causes a flat and uniform distribution of power 22 MHz wide.

OFDM (Orthogonal Frequency Division Multiplexing) employs the used band by splitting it into multiple parts. The signal to transmit is divided into subcarriers and each is transmitted using one of these band parts. Their distances are chosen based on the used bandwidth in each one so that there is no interference between them. In 802.11 networks, 52 subcarriers are used. OFDM gradually becomes the preferred method of data transmission with DSSS being only used in the original standard from 1997 and in g amendment while all the other usages employ OFDM.

2.4.3 Signal interference

The 802.11 signal is subject to interference as every signal. The interference can be of two kinds – interference with non-802.11 signals and interference with other 802.11 networks. The non-802.11 interference includes variety of non-signal sources – interference from arcs or sparks that manifests itself in quite wide range of frequencies, power lines interference or interference from microwave ovens that emit 2.45 GHz wavelengths. Signal sources affecting 802.11 networks are Bluetooth devices (operating in the same 2.4 GHz band), wireless cameras, walkie-talkies and so on. [2]

Generally, effects of short-term/burst interference sources are mitigated by the fact that WNIC employ CSMA Medium Access control (MAC) method which detects occupation of the medium and in such cases holds the awaiting transmission until the burst passes. When the interference occurs during the transmission, it is detected by invalid checksum of the frame. The frame is then discarded and due to no acknowledgement received by the receiver, it is retransmitted again. [2]

2.4.4 Signal attenuation

Another negative effect for wireless waves occurs when they pass through obstacles which results in signal attenuation. Useful signal level is measured as a ratio between signal strength and noise strength and it is expressed logarithmically in decibels (dB). Natural attenuation is caused by the weakening of the signal due to distance travelled and the area that the signal spans getting larger. In terms of decibels, the attenuation of signal, after doubling the distance from the sources is

$$10 \log \frac{1}{2^2} = -6 \text{ dB}.$$

Attenuation by obstacles is another factor that has to be accounted for when e.g. designing a network and choosing placement of access points. It strongly depends on the obstacle material – from 2 dB for brick walls to 12 dB for metal doors. [29] [25] Water also attenuates signal which may pose problem for outdoor networks in

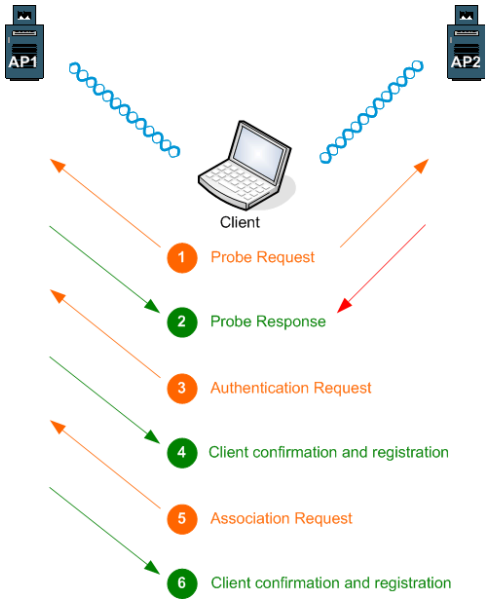

Figure 2.3: Diagram of AP-STA connection process [14]

case of rain or in indoor environments aquariums or to some extent even persons cause attenuation.

A similar, absolute signal strength unit is dBm. It represents strength of signal in decibels compared with a reference signal with power 1 mW. This unit is commonly used for measurements of signal strength and it is almost always negative.

2.5 AP-STA connection

We will describe for us the last important aspect of the 802.11 networks with access points – establishment of the connection between access point and station. This process has a few phases that are illustrated in figure 2.3.

The first phase is **probing** and it begins when the client wants to connect to the network. In one case it does not know the ESSID of the network it wants to connect to. For each channel in the band (2.4 or 5 GHz, eventually some other), it tries to discover which ESSes exist there. It can do so by active or passive scanning. **Active scanning**

involves sending *probe request* into the network and waiting for *probe responses* from access points; this usually takes under 100 milliseconds. **Passive scanning**, on the other hand, leverages the fact that access points periodically broadcast information about themselves into the network. Messages used for this purpose are called *beacons* and common sending interval for them is 100 milliseconds. Therefore in passive scanning, the client station listens for these beacons for some amount of time. In case the client station knows which channel the access point uses and what ESSID it belongs to, it can skip this phase and directly probe the sought network.

The second phase is **authentication**. The original 802.11-1997 standard provides two authentication methods – NULL authentication and authentication using Wired Equivalent Privacy (WEP). The NULL authentication method, as its name suggests, provides no authentication and always succeeds. The second method, WEP is no longer used since it was broken in 2001 and replaced by WPA and WPA2. Therefore NULL authentication is the most commonly used method today while the actual optional authentication takes place after the following association phase.

The third phase is **association** – the client station establishes a link with access point. In this phase the two parties of the communication agree on used physical layer properties of the connection like bit rate, QoS availability and other available features. After this step, the connection itself is established on the data link layer.

In case WPA or WPA2 authentication method is used for the connection, it takes place after the association phase. We will not cover WPA or WPA2 authentication in detail since it is not of interest for this work. However, until it completes, no other than management frames required for authentication are allowed in the communication between station and access point.

3 Management of 802.11 networks

3.1 General considerations

Management of 802.11 networks consists of multiple aspects. From the **physical point of view** it covers areas as access points distribution planning, selection of appropriate access points or antennas in design phase and in deployment phase setting transmission characteristics or choosing used frequency channel. From the **logical point of view**, the software running on the access point, configuration management, interoperability with the other systems in organization, security hardening, monitoring and accounting of the network and its devices, and diagnostics need to be considered.

This section focuses on these aspects of network planning and management, and demonstrates some of the systems that can be utilized for this purpose including open source or commercial systems. As the representatives of commercial management systems manufacturers will be presented HP and Cisco since they are of those most related to the hardware currently used at the faculty – some access points are by Cisco and active network components are mostly HP devices.

The systems that shall be described vary in the range of offered capabilities. Some systems are narrowly focused and provide only one or two of the described 802.11 management aspects. Although this may seem unsatisfactory, it is not always that case – the missing functionality may not be needed or can be provided by other means, e.g. using a combination of these systems. Examples of these systems and tools are iw, horst, Chanalyzer or TamoGraph Site Survey. Many of these tools are open source of available for free.

On the other end of this spectrum are systems that try to cover all or nearly all of these aspects. Complex management systems are usually products of hardware manufacturers and are developed specifically for the manufacturer's hardware. This allows for better integration of individual parts and less variability presents less opportunities for incompatibility problems. Such solutions are either paid or the price for them may be included in the price of the specific hardware required for its operation.

3.2 TamoGraph Site Survey

The first tool we will describe is TamoGraph Site Survey. The tool provides options for performing site survey, i.e. collecting on-site information about 802.11 networks. It is a paid software running under Microsoft Windows and it is developed by Tamosoft.

TamoGraph Site Survey offers three kinds of **site surveys** – predictive, active and passive. When planning a 802.11 wireless network deployment where some guarantee of service quality is needed, it is necessary to perform surveys in order to gather information about the wireless environment.

Predictive site survey is a first step that is done before the deployment and its aim is to predict wireless environment conditions based on the used access point characteristics (e.g. antenna type, used amendment (g/n/...) or channels) and environment obstacles like walls that attenuate signal or known present sources of signal in used bands that can cause interference. Predictive survey can therefore be done without actually visiting the site, only with its plans. The only requirement is that the obstacles have to be manually drawn, usually by retracing the walls and other parts of the environment based on the plan.

On the other hand, the aim of **passive** site survey is to map the existing state of wireless environment where the access points have already been deployed. Passive survey requires physical presence on the site and is performed by walking up the area and gathering information about seen access points and their characteristics. This type of site survey can visualize signal strength, Signal to Noise Ratio (SNR), Signal to Interference ratio (SIR) or noise level. This information can be used to discover problems with service quality on the physical layer.

The last type – **active** site survey – is similar to passive site survey. Besides it needing to be performed in existing wireless environment, the scan not only passively monitors existing wireless access points in the network, but also establishes connections with present access points and performs measurements of the connection quality (e.g. bandwidth, available physical data rate or packet delay). This information may help with detecting access point misconfiguration or problems on the data link or higher layers.

The result of all this scans can be viewed as a heat map visualization[1] of some network performance metric that is drawn onto a custom image that can be ground plan, or it can be summarized in form of a report.

Further option that this software offers is spectrum analysis. For this purpose, a specific USB device WiSpy has to be connected, which allows analysis of 2.4 and 5 GHz frequency spectrum with high resolution.

Besides the spectrum analysis, site surveys are done using the native computer WNIC and no additional specific hardware is needed although TamoGraph requires specific version of WNIC driver in order to work.

The advantage of this software is automatic generation of well-arranged visualizations which can significantly help with planning and tuning of the network or the possibility of specific antenna selection which improves precision of the result due to differing radiation characteristics of antennas. Cons of it include the need for time-consuming walking on the site, though it can hardly be avoided.

3.3 Chanalyzer

Chanalyzer is a spectrum analyser tool developed by MetaGeek. It is a closed source freeware software running under Microsoft Windows. For its functionality it depends on a hardware module that is capable of 2.4 or 5 GHz frequency bands monitoring. Along already mentioned Wi-Spy module, also access points with Cisco CleanAir technology is supported. Cisco CleanAir is an extension of some access points by Cisco which can perform spectrum analysis with high frequency and time resolution. [5]

Similarly, as TamoGraph Site Survey, this tool allows for gathering of information about spectrum usage. Based on the collected data, it is possible to visualise signal density as seen in figure 3.1 and detect the nature of the interference judging by the shape of the two-dimensional density graph over frequency and time domain. [10] This can be crucial for troubleshooting 802.11 interference or signal

1. Usually planar visualisation where areas are coloured depending on the value of measured variable.

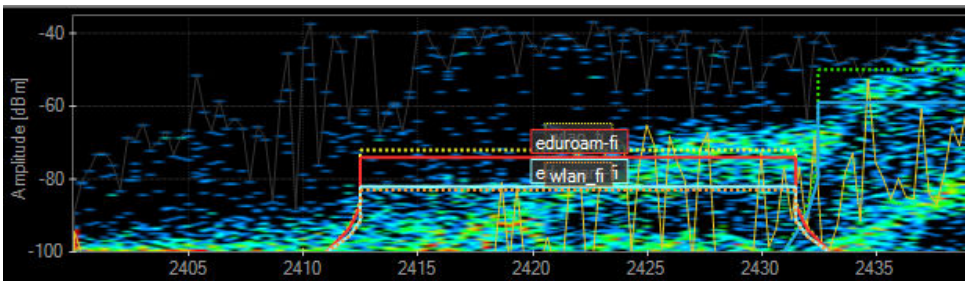

Figure 3.1: Example of beginning of the 2.4 GHz spectrum measured using Chanalyzer and Wi-Spy module.

problems caused by non-802.11 sources which can not be detected by regular WNICs.

3.4 OpenWrt

OpenWrt is a community open source router project that aims to offer a free alternative firmware for broad spectrum of routers and access points. The effort started with proliferation of classic Linksys WRT54G router which had source code for its firmware open sourced. The scope of the project was later broadened with more models from different manufacturers being supported. As of May 2014, 415 devices by 86 manufacturers are supported with support of more devices being possible or being work in progress. OpenWrt is mostly licensed under GPL with other licenses used by included software.

Due to the diversity of hardware on which OpenWrt runs, it needs to support various platforms with instruction sets as MIPS, x86, x86-64 or ARM. In order to use OpenWrt, the device in question needs to be re-flashed so that the original manufacturer's firmware is replaced by the OpenWrt image.

The core of OpenWrt uses Linux kernel and a part of system specific code is based on open-sourced official firmware for WRT54G. Due to the nature of a system intended as a firmware for embedded device, memory limitations have to be taken into account – some access points have only 4 MB of space available on flash memory. Thus

other necessary tools include often minimalistic versions or replacements of common Unix tools like bash (ash), coreutils (BusyBox) and tools specific to networking which we will mention later in this section.

Current version of OpenWrt is 12.09 (codenamed Attitude Adjustment) from April 2013 and uses Linux kernel version 3.3. As an interesting side note, the code names for OpenWrt releases are names of alcoholic cocktails.

Multiple common networking tools are part of the OpenWrt. They cover basic network management (net-tools, iputils, iw), monitoring and diagnostic (iperf, netstat, tcpdump), traffic filtering and management (iptables, ebtables, tc), router servers (bind, dhcp tools, radvd), wireless client/server (hostapd, dibbler, wpa-supplicant, freeradius) or penetration testing (nmap aircrack, kismet) areas. Besides that it supports IPv6, VPN and comes with microperl package which can be used for more user friendly scripting. [24]

Prime strengths of using this system as access point firmware lie in its ubiquity (one of the largest such projects with wide hardware support), broad selection of available packages (software is specifically packaged and can be found in OpenWrt repositories; as of May 2014 it amounts to circa 3500 packages) and extensibility (being Linux-based, other tools can often be ported to OpenWrt when their source code is available) and simpler manageability in heterogeneous environments. Disadvantages include added work required during installation and customization required for target environment, or the fact that the installation of additional software not included in the packages can be time consuming due to dependencies and the packages usually need to be cross-compiled[2]. Another minus is absence of GUI, although this area is covered by projects Gargoyle or LuCI which add GUI front end to OpenWrt.

3.5 DD-WRT

Another widespread tool used as a replacement of vendor-specific firmware for routers and access points is DD-WRT. It has the same

2. Compilation where the target architecture is different than building architecture.

roots as OpenWrt and used WRT54G firmware sources as a basis for further development. Besides it being developed as a community project, it is maintained by developer presenting himself under alias BrainSlayer. As of May 2014, DD-WRT is supported on around 550 devices by 97 manufacturers. [11] DD-WRT is also licensed under GPL.

As of May 2014, the newest version of DD-WRT is "v24 preSP2 [Beta]" from October 2012. However, DD-WRT has different support for various hardware and the latest supported version on given hardware can be determined on the project website.[3] Also, DD-WRT comes in different builds based on the features included, with most interesting builds being: micro build with roughly 1.5 MB image, mini build and standard build with roughly 3.5 MB image. [12]

DD-WRT uses Linux kernel branches 2.4 or 2.6 depending on the build. Networking-related features of DD-WRT include: bandwidth monitoring, dynamic DNS, IPv6, OpenVPN, PPTP, QoS, radvd, tcpdump, UPnP or WPA/WPA2 support, the presence of which depends on the used build.

An advantage of DD-WRT, at least compared to OpenWrt, is that it comes with a GUI front end by default which makes it easier for less console-versed users to work with. Further it is open source, therefore it can be extended when built from source code and in larger builds it comes with many packages. DD-WRT also supports slightly more devices than OpenWrt. However, DD-WRT is somewhat less maintained with respect to the latest release which is year and half old.

3.6 Management of Cisco devices

Cisco is a well-known and one of the largest network equipment manufacturers. Therefore it may come as no surprise that due to its size and variability of its products, it has developed a common firmware for its devices called Cisco IOS.

Its source code is proprietary and it comes in different releases based on the features contained which also affects its pricing or pricing of the hardware. [4] Also images with updated firmware are of-

3. `http://dd-wrt.com/site/support/router-database`

fered as a paid service by Cisco. The current version of Cisco IOS is 15.3 although only older versions from release 12 are used on access points.

Besides the base firmware build, various extensions with added features are available, which may include support for IPSec, IP mobility, IP multicasting, management tools, MPLS (Multiprotocol Label Switching), QoS, VPN or VoIP services. [6]

Cisco offers three ways of managing 802.11 wireless infrastructure. The traditional way consists of largely autonomous access points where most of the processing and management is done on the access points itself equipped with Cisco IOS. This is the case for most of the models from the current Cisco Aironet series. Another way, although currently abandoned, relies on transferring most of the processing from access points to a central point. In such architecture, Lightweight access points are used in tandem with WLAN controller device. Lightweight access points (LAP) work only on the physical layer and parts of MAC which require real-time functionality. The rest of the processing is offloaded to Wireless LAN controller (WLC) device which can control multiple lightweight access points (depending on controller model from hundreds to thousands). [3] [8] This architecture is used for Cisco Aironet 1000 series access points. The most recent architecture uses Cisco Meraki technology which employs cloud approach. It is broader in its scope since it can be used not only to manage wireless access points but also other devices such as switches or routers. [7]

In both cases the control part of the system uses Cisco IOS therefore the core features of the network remain the same. The primary access method to Cisco IOS is through a command line interface which provides access to configuration and monitoring of the device operation. The system offers a few security levels which determine what is the user allowed to do. Cisco IOS interface can be switched between different contexts – e.g. global, interface, VLAN configuration context where commands apply to different objects. Commands in Cisco IOS can be represented in a tree structure since each command can have multiple subcommands or parameters that can further branch into subsubcommands and so on. E.g. `show ip interface brief` lists terse information about interfaces and `ip dhcp relay information option vpn` causes the device

to add a VPN-related option to forwarded DHCP request packets.

Cisco IOS interface provides most of the necessary options for configuring device operation, although the disadvantage is the impossibility to extend or program the device in a specific way, which is possible when Linux-based system is used. Cisco is also known for some of its technologies, besides being proprietary, also being Cisco-specific, so that it poses another obstacle for its integration in heterogeneous networks or for future network diversification. Another disadvantage is the fact that the firmware is paid and when more features are needed, the cost is higher. On the other hand, maintenance of the system is easier with the only main necessary step in configuration being the single configuration file and no firmware re-flashing or other procedures are required.

3.7 Management of HP devices

Another network devices manufacturer we will focus on – HP (Hewlett-Packard) – also offers a complex wireless networking solution. HP has developed an architecture called HP FlexNetwork, which aims to offer centralized management being able to operate not only with their own devices but also with devices by other manufacturers (as of May 2014 over 5000 devices by 150 manufacturers). [18]

It is important to note that this technology covers a far broader range of areas besides wireless networking, including virtualization, cloud computing or data center management. Therefore for purposes of this theses we will focus only on the wireless management, a part of the so called HP FlexManagement. [16]

The management of wireless networks is realized using devices called MSM Controllers (MultiService Mobility Controllers). Its role is predominantly to be a single configuration and monitoring point for devices while offering some centralized functionality (DHCP, DNS services, radio spectrum management and so on). These devices are in turn managed by Intelligent Management Center software (IMC) which can offer a user-friendly web interface to the MSM management options.

We will not explicitly mention all the other basic features that are

present and largely similar to those of Cisco system, but to name some of the interesting ones that are implemented in the MSM controller:

- Wi-Fi Clear Connect – an automatized and centralized radio spectrum management; periodic measurement of radio spectrum is performed and when an interference is detected, the controller decides which channel is less affected and instructs the access point to switch to it; additionally, the number of clients connected to the access points is monitored so that in case of suboptimal distribution, controller changes the Tx power for the access points in order to balance the load. [15]
- Remote configuration and management using multiple channels. [17]
- Logging and diagnostics tools. [17]

For its operation, MSM uses open protocols which simplifies possible interoperation with other systems that also follow the open specifications. On the other hand, it is a proprietary system with closed source code, similarly as Cisco IOS.

4 Autoconfiguration algorithms

In order to improve 802.11 network functioning, we need to pose and answer a few basic questions. We need to determine which factors affect the network quality. In order to be able to meaningfully evaluate the state of the network, we need to design a metric or metrics which signify the network quality or the quality of its components. And based on the knowledge of the network quality determining factors, we need to design a process which will be able to adjust modifiable factors in order to improve some network quality metric. Finally, more from the practical point of view, we need to assess, when or how often will the process run in order find balance between adequate response of the network to environment changes and its usability in case the adjustment process impacts regular network functioning.

A good quality of network connection usually means that the network has low latency, low jitter, high throughput and small packet loss. All ISO/OSI network layers affect these indicators and depending on the type of network used, their effect varies. The physical layer in 802.11 wireless networks is usually the most common source of problems with network quality, therefore in order to improve such connections, it is necessary to understand its various causes.

4.1 Interference and its theoretical properties

The low latency of the network is usually coupled with high throughput. Although they are not directly proportional, low latency improves speed of data transfer due to faster acknowledgements in TCP transfers and hence better utilization of TCP window size[1]. The parameter of the physical medium that reflects this aspect well is Signal to Noise Ratio (SNR). SNR is measured in decibels and represents the ratio between the power of 802.11 signal and the power of background noise in logarithmic scale. According to Shannon-Hartley theorem, a result from information theory, the channel capacity C

1. Used to signal maximal amount of data that can be unacknowledged at one moment.

can be expressed using formula

$$C = B \log_2 \left(1 + \frac{S}{N}\right)$$

where B is channel bandwidth which is in our case fixed (usually 20 or 40 MHz), S is signal power in watts and N is noise power in watts. Unless the network has really low SNR (less than 10), the 1 in the formula is small compared to the fraction and can be neglected resulting in simpler formula

$$C = B \log_2 \left(\frac{S}{N}\right) = \frac{\log_{10} 2}{10} \times B \times \mathrm{SNR} \approx \frac{1}{3} B \times \mathrm{SNR}$$

where SNR is in decibels.

Another measure that is similar to SNR is Signal to Interference Ratio (SIR). This is basically similar to SNR, however it is more of a logical measure than SNR, since it takes into account 802.11 sources of signal. This makes it suitable for environments where interference is more prevalent than random noise.

Packet loss and jitter are also somewhat similar – both can be commonly caused by short burst interference. This can make the wireless medium temporarily unusable, therefore increasing delay and in turn also jitter or cause packets to be dropped thereby increasing packet loss. Burst interference is, however, usually unpredictable and therefore only some provisions can be made to counter it. This is the responsibility of MAC layer[2] which controls access to the communication channel.

Also, another important cause of noise in the channel is caused by other 802.11 access points or connections that occur on the same or near channel. Such interference is called co-channel interference (CCI). Its effect depends on the 802.11 amendment used.

For the faculty environment, we need to consider usage of amendments 802.11g and 802.11n.

In case of 802.11g, the used band is 2.4 GHz and the power distribution over the band forms roughly a half-circle with peak at the central frequency and extending 11 MHz to the both sides (see figure 2.2). 802.11g channels start with 1 at frequency 2.412 GHz and step

2. Media Access Control layer

by 5 MHz up to 13 at 2.472 GHz and then slightly offset channel 14 at 2.484 GHz (this one is however disallowed in Europe). This means there is some CCI present unless the difference between channels is at least 5. Due to this required channel separation, it is possible to operate at most three access points at the same location without them interfering with each other, e.g. using channels 1, 6, 11 which is a common choice.

802.11n can be used both in 2.4 and 5 GHz band. Notably, by employing 5 GHz band, it offers more channels in comparison with 802.11g, and those channels are also further spread. However, we need to consider that 802.11n can use channels 20 or 40 MHz wide, depending on whether High Throughput (HT) is enabled. This causes similar overlaps with adjacent channels so that two used channels have to be separated by at least 8 if no interference is desired. This means only two channels can be used at the same time in the 2.4 GHz band and they would also interfere with transmitters using 802.11g.

The situation is different in the 5 GHz band. Although the channels are spaced by 5 MHz, only every second channel (with frequency being a multiple of 10 MHz is valid). Also, the regulation of this band varies per regions. E.g. in Europe and U.S., only channels that are multiples of four are allowed in U-NII Low part of the band. Therefore every allowed channel can be used in U-NII low part or every second allowed channel in other parts. This holds when HT is not used; with HT, the distances need to be doubled.

4.2 Usable inputs for the algorithms

Based on this analysis, the prime aim is to achieve high SNR, which in practice ideally means high SNR both spatially and temporally.

However, measurement of SNR is in practice complicated since we would have to measure it at multiple, ideally homogeneously or suitably placed positions in the space. This is not possible without either manual site survey or placing additional devices on often unsuitable places where they could be a hindrance.

Wireless clients, which are usually mobile, could be theoretically used for this purpose and would exactly represent real positions of

wireless clients. However, without their cooperation it is not possible. Although the 802.11v amendment allows exchange of information about radio spectrum between 802.11 nodes, it is rarely implemented today and not often implemented in common customer devices. Wireless module Ubiquiti SR71-A used in our system does not implement it likewise. [26]

Therefore we need to choose a different measurable. One obvious possible choice for monitoring devices are be the access points themselves since they are necessarily spread over the network and most access points are capable of wireless medium scanning.

With respect to the present faculty system, we list a few methods that can be used to determine the suitability of a channel for use and that the access points can measure per channel: signal to noise ratio, signal to interference ratio, channel utilization and signal strength of other seen access points.

SNR and SIR have already been described. However, after performing measurement on the access points used at the faculty, it was found that probably the driver or the wireless card does not make this information available. Therefore this makes this metric performed in this way unsuitable for our environment.

Channel utilization is a measure that shows how often is the channel used for 802.11 communication. This value does not take into account non-802.11 interference sources. On the other hand, its advantage is that it takes into account 802.11 MAC layer and reports ”logical” utilization including the protocol overhead instead of the ”physical” utilization based only on 802.11 signal seen.

Signal strength of other seen access points is another measure that can be used indirectly. When an access points sees another that operates on the same or close channel as itself, it means that they compete for the bandwidth in the area between them. Of course, this negatively affects the quality of network. Therefore it is desirable to move the access point to a less used channel if possible. Another advantage of this measure is that we can see overlaps in the BSSes of access points and we can potentially also modify Tx power of the access points.

From the named approaches, we have chosen signal strength as a metric that we will base our algorithms on. Its advantage over channel utilization is that it offers more structured information and it can

also take CCI into account.

4.3 Possible approaches

Our aim will therefore be to to implement an algorithm that will modify used channels on the access points so that overall state of the network will be improved. Two algorithmic approaches are possible for solving this problem.

Currently, the channel assignment is done manually during the infrastructure deployment, based on assessment of the plans and potential interference. Adjustments to the configuration are usually only made upon problem report is received and the situation is analysed.

A traditional algorithm approach would consist of centralized process which gathers data from access points, processes them all on a central server and then based on the result signals access points to adjusts channel when necessary. This has the advantage of having a global picture of the situation and allows for simpler further processing of retrieved data, e.g. for visualizing access point visibility.

The other approach that leverages the nature of the problem is distributed process. Each access point can measure its environment, evaluate its situation locally and make a decision for itself, possibly while communicating with other access points.

We will design both centralized and distributed algorithm, and in chapter 5 compare their performance with each other and also with the current state of management.

4.4 Centralized algorithm

The design of the algorithm has been already outlined in the previous section. The first step is the gathering of data which is uninteresting from the theoretical point of view and it is of concern mainly for the implementation part. The same holds for the last third step – the channel adjustment. Therefore we will describe here only the second part that merits theoretical description – the centralized algorithm.

The algorithm will be designed as a greedy algorithm that will gradually assign new channels to our access points, based on the

computed interference with other access points with already assigned channel. A cut-off for low signal strength connections will be used.

Now we will state the problem more formally. We denote the set of access points $A = A_f \cup A_o$, where A_o is the set of our access points and A_f the set of foreign access points ($A_f \cap A_o = \emptyset$). Let $\sigma : A_o \times A \rightarrow R$ denote a partial function that for our access point a and another access point b returns the signal strength in dBm with which a sees b. If a does not see b, it is not defined. Let $f_{fix} : A_f \rightarrow N$ denote a function returning used channel for given foreign access point and $f : A_o \rightarrow N$ denote a function returning channel that the algorithm will assign to given (our) access point. Band_channels represents a set of possible channel in used band, min_dbm minimum seen signal strength (a negative real number) that is taken into account in the algorithm and intf_dist is the smallest distance between channels that do not have CCI.

4.4.1 Pseudocode

```
function main(Ao, Ap, A, sigma, Band_channels,
              min_dbm, intf_dist):
    // prepare a set of "sights"
    Q = {}
    for x in Ao, y in A:
        if defined sigma(x, y)
                && defined sigma(y, x):
            t = (sigma(x, y) + sigma(y, x)) / 2
        elseif defined sigma(x, y):
            t = sigma(x, y)
        elseif defined sigma(y, x):
            t = sigma(y, x)

        Q = Q union {({x,y}, t)}

    // calculate best channel
    f_fin = undefined function
    Q_stat = Q
    while (non empty Q):
```

```
        (T, s) = an element from Q with maximal s
        T = T and Ao
        for a in T:
            if not defined f_fin(a):
                for ch in Band_channels:
                    i_ch = interference_index(a, ch,
                        f_fix, f_fin, A, Q_stat,
                        min_dbm, intf_dist)
                f_fin(a) = (first) channel
                    with smallest i_m
        Q = Q \ (T, s)

    return f_fin

function distance_effect(a, b, intf_dist):
    return max(0, intf_dist - abs(a - b))

function interference_index(a, ch, f_fix, f_fin, A,
        min_dbm, intf_dist):
    index = 0
    for x in A:
        case
            defined f_fix(x):
                m = f_fix(x)
            defined f_fin(x):
                m = f_fin(x)
            default:
                m = 0
        case
            exists element (T, s) in Q_stat
                    such that T = {a,x}:
                intf = s
            default:
                intf = 0
        index = index + (intf - min_dbm)
            * distance_effect(m, ch, intf_dist)
    return index
```

4.4.2 Analysis

The greediness of the algorithm with respect to the seen signal strength was chosen in order to minimize the chance of high interference for access points which are susceptible to it due to strong signal seen from other access point(s). When greedy algorithm is chosen, the order in which we choose access point for channel allocation is the most sensible for our purpose.

Another aspect, a cut-off for low signal strength connection, is only a practical measure that rules out from consideration signals that could cause only insignificant interference. With the sensitivity of the WNIC -90 dBm, a sensible values is -75 dBm or -80 dBm. This speeds up the algorithm to some extent since fewer edges have to be considered.

Now we will determine the time complexity of the algorithm. Choice of appropriate data structure for Q has to be considered since it can significantly affect the complexity. Operations that are performed on Q are create empty, add element, check if empty, remove maximal element. These operation have good complexity for Fibonacci heap: create empty ($\mathcal{O}(1)$), add element ($\mathcal{O}(1)$), check if empty ($\mathcal{O}(1)$), remove maximal element (amortized $\mathcal{O}(\log n)$ where n is size of the heap). For brevity, we will overload A, A_o, B, Q to represent also the size of the respective sets (Band_channels denotes B).

The preparation part of main consists of for cycle repeating AA_o times and each iteration can be done in $\mathcal{O}(1)$. The channel selection consists of creating copy of Q ($\mathcal{O}(AA_o)$) as a hash Q_{stat} and while cycle performed $\mathcal{O}(AA_o)$ times with check condition in $\mathcal{O}(1)$. Each iteration takes $\mathcal{O}(\log Q)$ amortized for maximal element deletion, $\mathcal{O}(A_o)$ for intersection and A_oB times time needed for interference_index. Interference_index can be performed in $A(\mathcal{O}(1)) + \mathcal{O}(1)$ giving $\mathcal{O}(A)$. Therefore we have total complexity

$$AA_o\mathcal{O}(1)+\mathcal{O}(AA_o)+\mathcal{O}(AA_o)(\mathcal{O}(1)+A_o+\mathcal{O}(A_o)B\mathcal{O}(A)+\mathcal{O}(\log AA_o))$$

which after simplification gives $\mathcal{O}((AA_o)^2B)$ or $\mathcal{O}(A^4B)$. Therefore the algorithm has quartic worst-case complexity in number of all (both our and foreign) access points. It also has linear complexity in the number of band channels, however, we can take this factor to be constant since in practice it is fixed.

4.5 Distributed algorithm

Distributed algorithm is based on a similar principle as the centralized algorithm, i.e. that it tries to use channel with the least interference and conditions the change with a probability calculated by the potential achieved gain of the change. The process consists of three steps:

- measurement of seen signal strengths,
- calculation of best channel with respect to interference,
- conditional change of the channel of access point (with probability proportional to the difference between the current and lowest possible interference).

This process is done repeatedly with variable delay between the runs in order to desynchronise runs with those on other access points. Synchronization is undesirable since during the scans the scanning access point may not be seen by other scanning access points.

Again, let us introduce notation for this algorithm. Band_channels represents a set of possible channel in used band, min_dbm minimum seen signal strength (a negative real number) that is taken into account in the algorithm and intf_dist is the smallest distance between channels that do not have CCI. Further we use three functions the implementation of which is uninteresting from the theoretical point of view. do_scan() performs scan of spectrum in given band and returns a pair of functions where the first returns channel and the second seen signal strength for given access point. active_channel() returns currently used channel and change_channel() sets it.

4.6 Pseudocode

```
function distance_effect(a, b, intf_dist):
    return max(0, intf_dist - abs(a - b))

function interference_index(ch, f_fix, sigma1,
```

```
        min_dbm, intf_dist):
    index = 0
    for x in dom f_fix:
        index = index + distance_effect(f_fix(x),
            ch, intf_dist) * (sigma1(x) - min_dbm)
    return index

function channel_change_probability(i_act, i_min)
    max_p = 0.75
    intf_diff = (_act - i_min) / 100

    # usual sigmoid with values from 0 to 1
    # around -4 it is almost zero and around 4
    # it is almost one
    sigmoid = 2 / (1 + exp(-intf_diff)) - 1

    return sigmoid * max_p
}


function main(Band_channels, min_dbm, intf_dist)
    while running_time() < max_running_time do:
        (f_fix, sigma1) = do_scan(Band_channels)
        a = active_channel()

        for ch in Band_channels:
            i_ch = interference_index(ch, f_fix,
                sigma1, min_dbm, intf_dist)
        m = (first) channel with smallest i_m

        p = channel_change_probability(i_a, i_m)
        if (random(0..1) <= p)
            change_channel(m)
        sleep(random(min_sleep..max_sleep))
```

4.6.1 Analysis

The aim of this algorithm is quite simple – to improve the local state by adjusting the channel where the interference is the lowest. From a naive approach it differs in the introduction of probability of change instead of unconditional change when a better channel is available. Its purpose is to make system more stable and not to overreact to minuscule differences of interference in channels when a change of channel would have negligible effect. Note that in this algorithm we do not differentiate between our and foreign access points since we act locally.

The probability with which a channel change is made was inspired by sigmoid function. It was chosen as a function of interference difference intf_diff so that it roughly linearly rises for smaller intf_diff (circa 0–100) and the curve slope slowly decreases until values around 400 where it is close to maximum and asymptotically reaches maximal set probability. The maximum probability was chosen to be 0.75 so that a channel change is not always made and a chance for the environment to change is given (e.g. we could have two access points at the same channel and if the maximum probability would be 1, they would both change channel, possibly to the same new one).

Since one pass of this algorithm would in most cases result in nearly no change, we let it repeat for a fixed duration of time on every access point. That way this repeated process has chance to globally improve the state by allowing more iterations for a change to propagate.

Since the running time of this algorithm is basically bounded by max_running_time + max_sleep, we can consider it to be of constant time complexity. However, for comparison, computational part of one iteration of the while cycle has complexity $\mathcal{O}(1)+BA_f\mathcal{O}(1)$ therefore $\mathcal{O}(BA_f)$ where A_f denotes upper limit on number of seen access points.

5 Deployment

5.1 Wireless environment

The practical realisation of this work takes place at Faculty of Informatics at Masaryk University. The management of the faculty wireless network is under the competence of Computer Systems Unit (CSU). We will briefly describe the environment, used hardware and conditions which affect local wireless network.

From the physical point of view, the faculty is currently located in two buildings. Nine of their floors and three larger lecture rooms are relevant for us due to their coverage with 802.11 network. The floors are allocated for smaller offices which creates an indoor environment with higher attenuation of wireless signal. This described area is covered by approximately 40 access points, with usually four access points per floor.

Faculty access points broadcast two networks. The first is open faculty network with ESSID wlan_fi and the other network is a part of a worldwide academic network Eduroam (ESSID eduroam-fi). Both are operated over 2.4 and 5 GHz bands.

The wireless networking in the buildings is not exclusively under administration by CSU. Two floors of one part of the Botanicka building are occupied by Institute of Computer Science (ICS) which provides its own wireless network (ESSIDs eduroam and MUNI). Also, in the second faculty building Gotex, the SITOLA laboratory has its own network (ESSID sitola) on a floor where it is located.

Besides these university-related networks, there are about 80 networks with different ESSIDs detectable. This count reduces to 15 if we take into account only those that are visible from some of our access points with signal strength at least -70 dBm. They are usually transmitted from access points in the closest of neighbouring buildings or by other organizations that are located in the Gotex building.

Most of these are stable networks, i.e. they occurred during all scans done in a range of a few weeks. Therefore the foreign wireless environment is relatively static. There has been some decrease in seen networks between March and May. This can be explained by the office containers that were located in the neighbourhood of the

faculty and were removed in meantime.

5.2 Faculty wireless system

5.2.1 Access point hardware

Historically, the network consisted mainly of Compex and Cisco access points but due to problems with their stability, they were gradually replaced with RouterStation and finally by RouterBoard devices.

Currently significant majority of the network consists of RouterBoard systems. RouterBoard is an embedded motherboard manufactured by MikroTik. Model used at the faculty is RB433AH[1] and offers 680 MHz CPU with MIPS architecture and 128 MB RAM. Permanent memory is available in form of microSD card slot. Three 100 Mbps Ethernet ports are available and wireless network is provided by miniPCI card Ubiquiti SR71-A [26]. The miniPCI card is connected to omnidirectional dual band MIMO antenna HP J9659A with 2.5/6 dBi gain[2]. Power is supplied to the system using PoE (Power over Ethernet). The hardware of the system supports operation according to 802.11a/b/g/n amendments and g and n are currently in operation.

5.2.2 Used management system

The last example of a wireless management system we will describe, will be the currently used system at the faculty. Since it is the system we will improve on, we will describe it in more detail, including the hardware and software realization of access points.

Firmware used on this system is a custom build of OpenWrt 12.09. The system is extended by a few scripts that facilitate management and configuration. When introducing a new access point into the system, it has to be configured to boot over network using DHCP. Upon its physical installation to its operational position, some configuration hast to by done. An IP and IPv6 address has to be chosen together with the DNS name (derived from the location of access

1. `http://routerboard.com/RB433AH`
2. Antenna gain represents the increase of Tx power achieved by the antenna and is specified for 2.4 and 5 GHz bands separately.

point). MAC address of the access points is entered into the Faculty administration system and DHCP is enabled. Now only configuration settings for WNICs remain - the Tx power and used channels are configured for 2.4 and 5 GHz bands. Now, upon these steps are completed, the access point is ready for operation. After powering it up, it is able to provide full service within one minute after the start.

The system boots over PXE[3] and after getting boot information from DHCP server, it loads its firmware over TFTP given in DHCP response. The firmware and all information necessary for the system operation is retrieved on boot using the TFTP and configuration server, so that no data needs to be retained on the system flash memory. However, due to the space constraints, the size of firmware image is limited to about 6 MB. The configuration data specific for the access point are retrieved over HTTP during the initialization phase based on the requester's IP address.

Another interesting property of the system is that after the preboot phase where IPv4 address received from DHCP server is used, the booted firmware no longer requires it and the system operates in IPv6-only mode.[4]

Besides OpenWrt base, the firmware contains some basic packages: netifd (network interface configuration daemon), iw (wireless interface tool), wireless-tools (older alternative to iw), iptables and ip6tables (packet filtering tools), openssh (Secure Shell daemon), crda (regulatory domain configuration tool), dhcp-client and dibbler (DHCP v4 and v6 clients), microperl (minimalistic version of Perl), wpa_supplicant (WPA/WPA2 encryption support), hostapd (daemon implementing AAA[5] services).

The system used for the management of access points is a part of a larger custom developed system *Faculty Administration (Fadmin)* that is used at the faculty as a multi-purpose system for management of faculty resources. The system includes management of devices, software tools, user accounts, groups or their permissions. Its code

3. Preboot eXecution Environment – a mechanism that allows system boot over network.

4. Naturally, the system can forward either IPv4 or IPv6 packets from and to the wireless clients. The IPv6 operation pertains only to the operation of the access point itself.

5. AAA – Authentication, Authorization and Accounting.

base is written mostly in Perl and it can be controlled using a web front end and command-line scripts.

A few parts of Fadmin are used in the management of wireless network. An application **ip** is used for management of IP adressess/devices, e.g. to configure DHCP and MAC address for a device, including possible TFTP-related DHCP options. Script **wifi_cards** is used to configure radio parameters (channel and Tx power). To provide an overview of the status of access points, an application **wireless_manage** can be used. It provides listing of all access points together with possibility of their restart (preformed using remote SSH command execution) and MRTG graphs of network traffic and number of users for both ESSIDs (wlan_fi and eduroam-fi). Another part of the Fadmin system is Nagios which monitors basic health indicators of access points – SSH and SNMP. Nagios and MRTG are automatically configured based on the information about access points in the database to facilitate installation of new access points.

5.3 Measurement and comparison methodology

In the next sections, we will continue with evaluation of wireless network status in three cases – current state, the result of centralized and the result of distributed algorithm. In order to do so, we have to find a suitable metric to compare them. Logical choices for such metrics are those that were described in section 4.1 since they reflect the aspects of the wireless network which we want to optimize.

To summarize, SNR, SIR, channel utilization and signal strength of other seen access points were considered. For routine automatic measurements, channel utilization and signal strengths performed on APs are suitable. On the other hand, measurement of SNR and SIR has to be done manually by means of passive survey.

We will do the comparison of results of our work using SIR as the primary metric and also evaluate the results using indirect metric that is used as a "driving force" by the algorithms, i.e. signal strength of other access points and the interference derived from that.

For the measurement of SIR, we will use TamoGraph site survey tool which is capable of performing passive site surveys and visual-

izing measured SIR. Since site surveys are time consuming and our environment spans on nine floors and three lecture rooms, we will conduct the measurements only on one representative floor.

For this purpose, we have chosen the 3rd floor in building part B. The motivation behind this is that according to preliminary measurements, the access points on this floor see the largest amount of access points compared with other floors. This makes the situation more complex and the results more interesting. The floor is around 65 meters long and consists of a 50 metres long hall and a 10 metres long computer lecture room at the end of the hall. The hall houses three access points located at the ceiling at roughly equal distances (circa 10 metres). The last access point on the floor is located in the computer lecture room.

The measurement of signal strength seen will be visualized in form of a visibility graph between access points where we will denote access points by nodes and edges will represent the signal strength of access points seen. A graph visualization program GraphViz[6] was used for this purpose. Note that we will use the same cut-off as in the algorithm – all edges with signal strength less than -75 dBm are discarded.

We will only present results for the 2.4 GHz band since it is more crowded and therefore the results of the algorithm are more interesting due to higher constraints on the channel assignment.

5.4 Current system results

Here we will describe the status of wireless environment before any changes made by our work. Only manual selection of appropriate channels was done during network deployment and the channels are sometimes changed if necessary when users report problems with signal quality.

In figure 5.1 we can see the heat map visualisation of SIR in 2.4 GHz band. Notably, the interference is strongest in the hall which is a consequence of overreaching signal from access points from surrounding floors. Some interference is also present at the end of the computer lecture room which is mostly due to the interference with

6. `http://graphviz.net/`

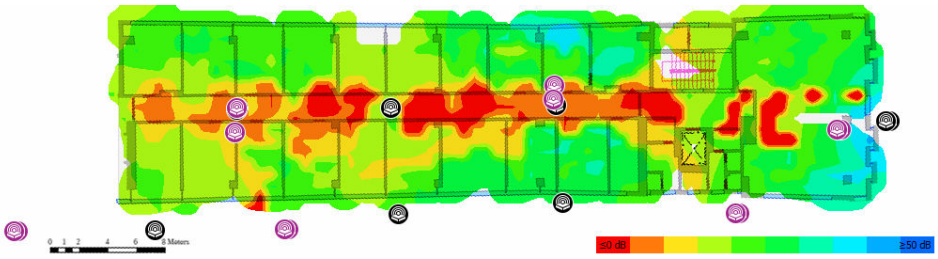

Figure 5.1: SIR heat map for floor B3 – current status

the closest access point in the hall and a few access points from other floors.

Further we evaluate the access point visibility graph restricted to our access points on the B3 floor and access points seen by them. We can see the graph in the figure 5.2.

The square nodes are our RouterStation access points and we name them using their host names. The elliptic nodes are access points either not under our control or they belong to few of our non-RouterStation access points and we name them by their broadcast ESSID. Finally, all access points have their used channel shown in the second line. The signal strength (in dBm and with stripped minus sign) seen between APs is denoted as a label on the edge.

Currently there are two more problematic (red) edges connecting APs with the same channel and signal strength -65 dBm, and five (yellow) edges connecting APs with channel difference 2 and signal strengths between -56 and -71 dBm.

5.5 Centralized algorithm results

Now a presentation of wireless environment status after we have run the centralized algorithm will follow.

In the figure 5.3 we can see the result of Signal to Interference Ratio done by measurement on the B3 floor in 2.4 GHz band.

By visual inspection of the heat map we can see that the red areas have shrunk and some have disappeared. This means that after the change of channels, quality of signal in these areas has improved.

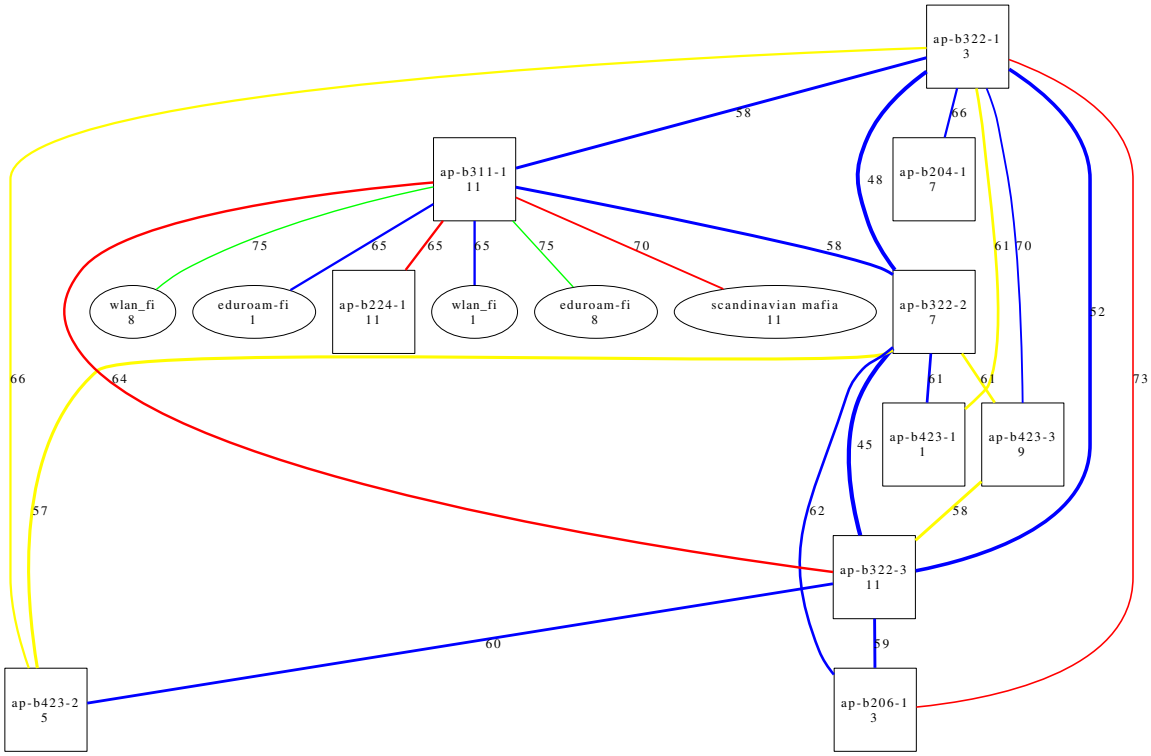

Figure 5.2: AP visibility graph for floor B3 – current status

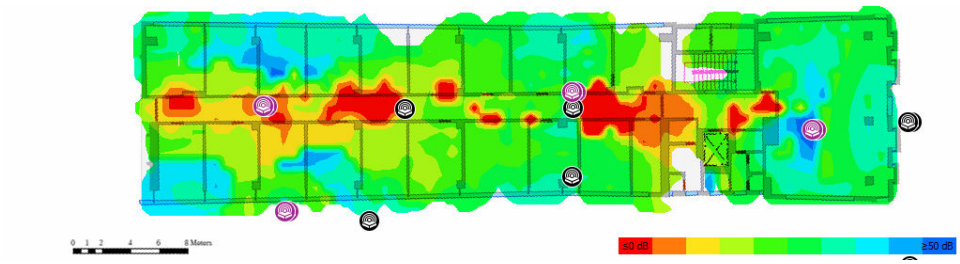

Figure 5.3: SIR heat map for floor B3 – centralized algorithm

The change we see is an improvement by 5-20 dBm and in lecture room it is even over 40 dBm.

Next we can see that in the graph in figure 5.4 of access points visibility calculated after the run of centralized algorithm. In this graph, the channels in the nodes labels have either not changed or have changed as shown. The interference situation has improved and overall "connections" between access points are weaker due to channels being further apart. Now there are only two "red" edges and three "yellow" edges. This indicates a good improvement over the previous state.

5.5.1 Implementation notes

The centralized algorithm needs to gather information from access points, perform global computation and accordingly change the used channel on access points. Also, due to the architecture of the access points system, the change has to be done also in the database in order for it to be permanent (otherwise the former setting would be applied only until next AP reboot).

Faculty server Thetis, which is the main faculty management server, is a natural choice for the environment in which the script will run. It hosts a database `administrativa` where settings for access points are stored and also other configuration scripts related to access points.

Languages chosen for the implementation are Perl and shell. Perl is used for the more complex task of implementing the algorithm since it lends itself well for the implementation due to native support of arithmetic and at the same time easy integration with shell tools. Although the used access points support only a minimalistic version of Perl – Microperl – it suffices for our purpose and furthermore facilitates the implementation over more low-level languages like C. If written in C, the program would have to be either cross-compiled or a compiler would have to be present on the access point, which is, however, undesirable due to the space constraints. Lastly, shell is used as a glue tool for calling programs from Perl since the `system` call caused undesirable mangling of program arguments.

The implementation consists of a few scripts. The first part, gathering of necessary scan data, is done using bash script **call_scan.sh**

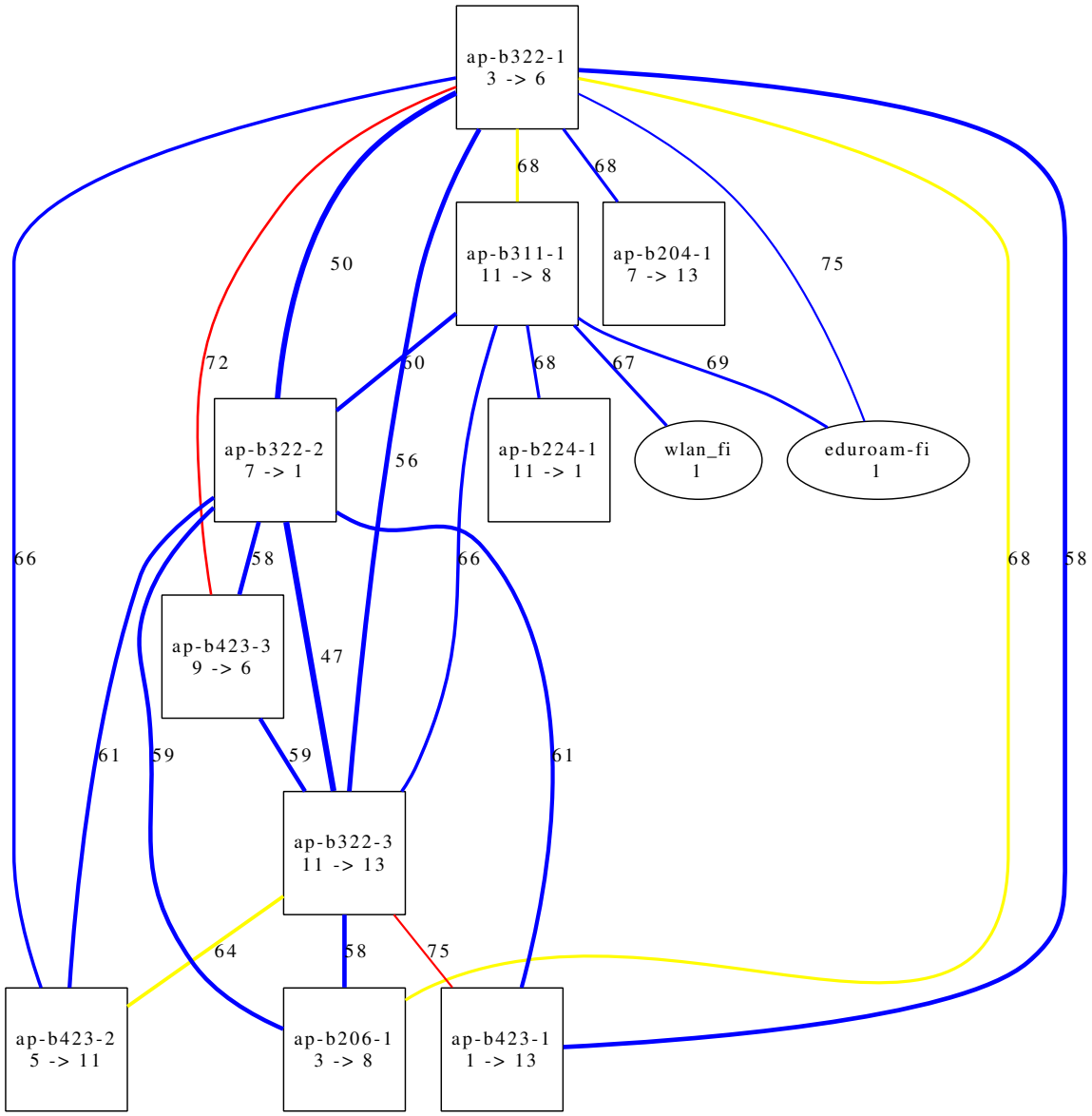

Figure 5.4: AP visibility graph for floor B3 – centralized algorithm

which connects to the access points through SSH (using SSH key). It copies Perl script **scan.pl** to the access point and runs it there. The task of next script **scan.pl** is to gather information about the device itself, namely the present physical and logical wireless devices, their radio settings and BSSIDs. After this preparation, scan of the frequency band is performed.

The scanning is performed using standard `iw scan` command. It offers either active or passive scanning which are described in more detail in section 2.5. A disadvantage of scanning is that it puts the access point in a mode where it temporarily can not fulfil its access point role since it needs to switch to different channels. The scan can be done either for the whole band in which the wireless card operates or only for given channel. Scan of each channel takes 60 milliseconds. Depending on the bands scanned, it takes 0.8 seconds for 2.4 GHz band and 1.2 seconds for 5 GHz.

The effect of this delay depends on the usage of the wireless network. In our situation, the network is not or is only marginally used during night. It opens possibility for scanning during this period since it will have nearly no impact on the usability. However, if network usability is a concern, a delay of at least one second[7] can be inserted between each scan which minimizes the length of continuous outage.

Since we can perform the scans during night and get a good picture of the network, with stable devices that affect our access points most, we have chosen scanning in one pass without pauses. It is also important to note that when an access point scans a band, it operates in different channels and does not broadcast beacons such as in normal operation. Therefore it would not be detected by another scanning access point. This basically enforces serialization of scanning on access points if we do not want to miss access points this way. Fortunately, this is not a significant problem since each scan takes two seconds.

Finally, the data are loaded by Perl script **assign_channels.pl** which runs the algorithm described in section 4.4 and modifies channel for access points when necessary. The modification consists of a

7. The delay has to be integral number of seconds since there is no easy way to achieve exact sub-second delays in this scenario.

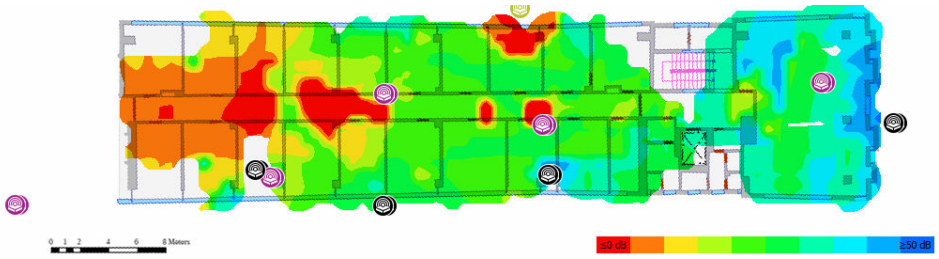

Figure 5.5: SIR heat map for floor B3 – distributed algorithm

change in the database and reload of the access point. During the reload, new configuration is retrieved from Thetis using HTTPS and wireless interfaces are restarted using an already existing custom tool **get_config_from_fa.pl**. This last operation needs to be considered from the point of service outage since restart of interface includes restart of hostapd daemon providing access point services and the whole operation takes around eight seconds.[8]

The whole run of this process is dominated by the scanning part and in the environment of the faculty with 35 access points it takes around two minutes.

Running of this process is controlled on the server and in order to minimize interference with normal usage of network, we suggest daily or possibly weekly runs during night. Since the dynamics of access point changes in the environment is fairly steady, weekly runs are well suited for this purpose. The process is scheduled for running using cron daemon.

5.6 Distributed algorithm results

Finally, we will present results of the distributed algorithm. Again, the SIR heat map in 2.4 GHz band for floor B3 is presented in figure 5.5.

When we compare this SIR heat map with the one for manual

8. During the course of this work, an inefficiency was found (and repaired) in the custom tool which resulted in the restart being performed twice, taking around 16 seconds.

channel assignment, it is also an improvement, although not as clear as with the centralized algorithm. The problem is the area on the left side of the map that has actually increased SIR. However, we were unable to find an explanation for this worsening. Also on the visibility graph we could not find a possible AP that could cause the heightened interference.

In the next figure 5.6 we see the visibility graph as the result of the distributed algorithm run. Unlike centralized algorithm, we denote only the new channel after the change. This is due to the nature of the algorithm which did not have all the information about APs together. No two access points that see each other have the same channel. There are two access points with channel distance 1 (orange edge), however, with very low seen signal strength and three (yellow) edges with channel difference 2 and signal strength ranging from -58 to -66 dBm.

5.6.1 Implementation notes

The distributed algorithm is by its nature run on the access points. When designing programs for access points, we have to consider specific and more constrained conditions in which our programs will run. Another factor to consider is that we have already written a centralized channel allocation algorithm. In order to maintain consistency with this implementation and to be able to reuse written code, Perl and shell support is desirable. Since both Perl (in form of microperl) and shell (in form of ash) are present, we have chosen these languages to write necessary programs.

To reiterate, the process runs for a fixed time during which scanning of the band, calculation of channel change probability, conditional channel change and random wait are repeatedly performed.

The implementation consists of a main script and two helper scripts. The main script **choose_channel_distrib.pl** consists of initialization part where parameters like the band on which to operate (2.4/5 GHz), parametrization of random waits. Gathering information some basic information about the access point (host name, information about present WNICs) follows. Then a loop is entered which performs the actual run of the channel change algorithm described in section 4.6. After the loop finishes, the current channel for our access

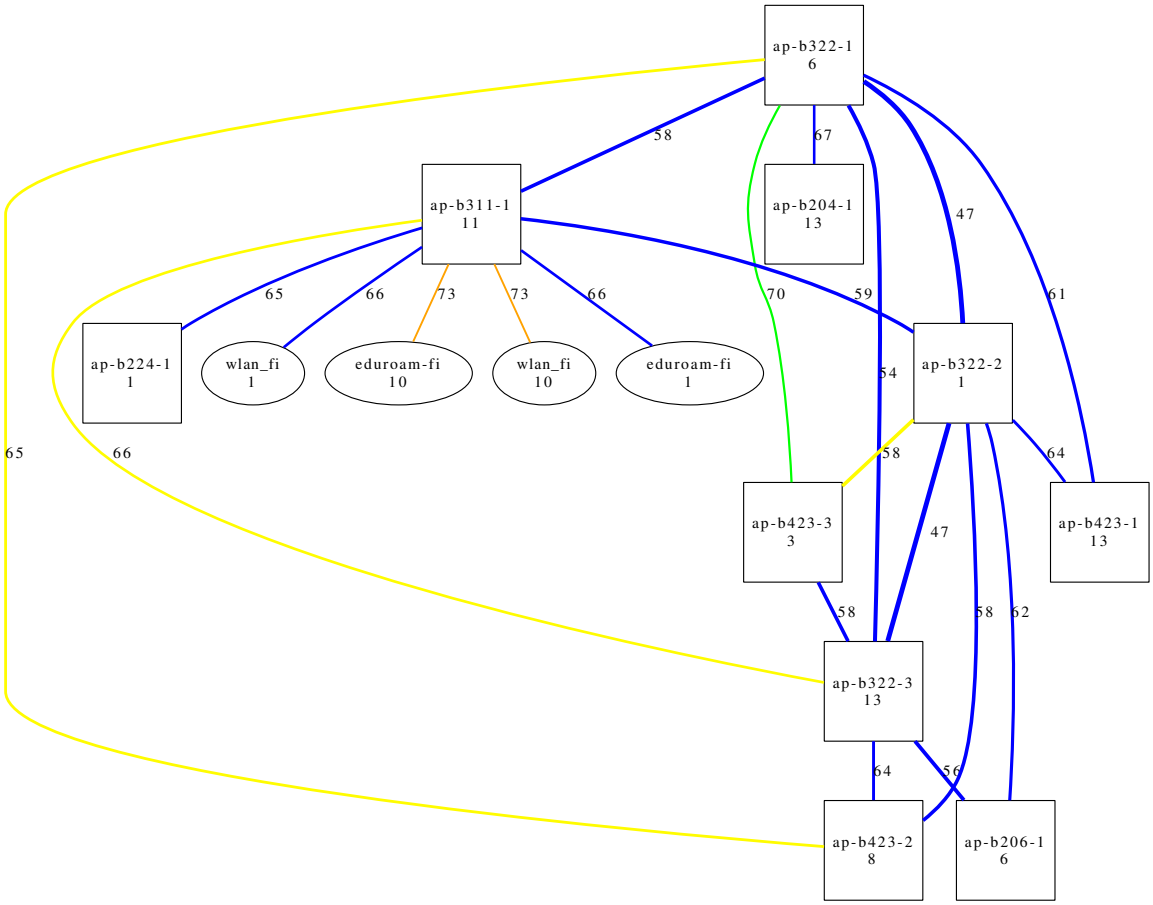

Figure 5.6: AP visibility graph for floor B3 – distributed algorithm

point is changed in database on server Thetis.

The helper scripts **change_channel.sh** and **change_channel_db.sh** are used for similar reasons as in centralized algorithm (Perl would otherwise mangle arguments to Perl call **system**).

Runs of distributed version of algorithm are controlled by cron present on the access points and started at the same time. Similarly as for centralized algorithm, we also consider that an acceptable choice for running the algorithm is daily or weekly with weekly periodicity being sufficient. As for the time parameters, we have set the whole running time to be 30 minutes and each sleep between two iterations to be random with even distribution between 45 and 90 seconds. This leads to the expected number of the iterations to be 27 in one run.

5.7 Additional developed tools

During the development of centralized algorithm a few additional useful tools were developed that proved useful mostly for testing/debugging or visualisation purpose.

One such tool is Perl script **graph_scan.pl** which processes results of call_scan.pl script and visualises them in form of a visibility graph of access points. Besides being able to graphically see which access points are close to which, the tool also draws the edges with different style depending on the signal strength and channels. The colour of the edge signifies the channel distance between neighbouring access points and its width the signal strength with which one access points sees the other. This script transforms the data from access points into a .dot file (GraphViz graph notation file format) and calls GraphViz tool **dot** to convert it into an image.

Another tool is **distrib_in_tmuxes.sh** which allows to observe the progress of distributed algorithm execution. The tool opens up a tmux session with a pane for each access point.[9] In each pane the same commands are run – necessary scripts are copied to the access point and then choose_channel_distrib.pl is run.

9. Tmux is a terminal multiplexer tool which allows to open multiple shells in one terminal with all of them being visible at the same time.

5.8 Discussion

We have tested three approaches to channel allocation – manual, centralized algorithm and distributed algorithm. For each of these we have performed measurements in order to be able to compare them.

As it may have been expected, both centralized and distributed algorithm performed better than manual channel selection. This holds especially in cases when multiple access points operate near each other. The number of visibility connections grows roughly quadratically and it becomes hard to manually assign appropriate channel to each of them and automated process can perform in this situation significantly better. Another fact that shows up is that not only the classical three channels 1, 6 and 11 got selected in the automatic process. This is again due to larger amount of APs and more visibility connections between them.

When we compare centralized and distributed algorithm, we can see that the centralized performed better. The areas with lower SIR are larger and also the second metric – APs visibility show somewhat more favourable results for centralized algorithm. One of the problems of the distributed algorithm may be that the total running time and the range for sleep time set the expected number of iterations too low for the system to converge to even better state. Another possibility is that the probability coefficient max_p was chosen too low and therefore the system was too conservative. This offers some room for further testing and tuning of the parameters of the distributed algorithm.

Another possible choice would be to modify the algorithm in a more radical way so that e.g. the channel change would not be done immediately but after gathering more information, potentially by making communication between access points possible.

However, our task to improve the channel allocation has been successful and demonstrably the centralized algorithm was able to surpass the results of the manual channel selection. Therefore we have chosen to deploy the centralized algorithm in the faculty environment running weekly during weekends. This algorithm is also more practical and more controllable since it runs on one system and the number of access points is too high for it to be impractical.

5.8.1 Deployment in a new faculty building

During the end of the this term, the construction of new faculty building has finished. The electrical part of the construction project included only structured cabling. Active and passive network elements together with access points will be provided by the faculty. The new building has eight floors, seven of which will be covered by wireless network. Each of these floors has around larger 15 rooms. Wireless coverage of this building will be supplied by over 80 access points.

Therefore planning of the network and its deployment will be needed. For this purpose, the output of this work will be used to select appropriate channels for the access points. This will alleviate some of the manual work that was needed during the deployment of new access points in the old building.

6 Summary

In this work we have presented the reader with approaches to improve 802.11 wireless networks.

The first overview part of the work described 802.11 networks including its origins, standards and basic description of its physical layer focusing on interference and attenuation of signal. A brief description of tools that can aid in management of 802.11 network were presented including some open and commercial firmware or management systems.

In the second part, we presented starting points for the development of a process that would improve channel allocation for access points which was manual up to now. After considering possible approaches a centralized and a distributed algorithm was designed. These algorithms are based on measurement run on access points which are spread over the environment. The measured information is signal strength of seen access point. Based on this data, both algorithms employ a similar idea – they choose a new channel based on predicted interference on possible channels in used band.

The centralized algorithm sequentially runs on a server and assigns new channels to our access points in a greedy manner - channels are assigned to access points in order of maximum signal they see from another access point. The distributed algorithm for a fixed time repeatedly evaluates the state of environment and with probability proportional to the possible decrease of interference changes its channel to the best available.

A description of faculty wireless environment and system is followed by the presentation of measured results of manual, centralized and distributed channel allocation method and implementation notes. We have found that the centralized algorithm offers favourable results when assessed using signal to interference ratio (SIR) and interference derived from visibility between access points.

The centralized algorithm developed in this work will be implemented into the faculty wireless management system. It will also be used during deployment of wireless networking in newly built faculty building which will extend the current wireless network.

Therefore the benefits brought by this work are: automated chan-

nel allocation in current building, facilitation of initial channel allocation in the new building, visualisation of access point visibility and possibility to automatically react to changed wireless environment conditions.

7 Appendices

Scripts implemented during this work and described in the text of the work are present on the attached optical medium.

Bibliography

[1] N. Abramson. THE ALOHA SYSTEM – Another alternative for computer communications. In *Proc. 1970 Fall Joint Computer Conference*, page 282. AFIPS Press, 1970. <http://robotics.eecs.berkeley.edu/~pister/290Q/Papers/MAC%20protocols/ALOHA%20abramson%201970.pdf> [cit. 2014-05-20].

[2] Cisco Systems. *20 Myths of Wi-Fi Interference*, 2007. <http://www.cisco.com/c/en/us/products/collateral/wireless/spectrum-expert-wi-fi/prod_white_paper0900aecd807395a9.htm> [cit. 2014-05-20].

[3] Cisco Systems. *Lightweight Access Point FAQ*, 2010. <http://www.cisco.com/c/en/us/support/docs/wireless/aironet-1200-series/70278-lap-faq.html> [cit. 2014-05-20].

[4] Cisco Systems. *Cisco IOS Software Reference Guide*, 2012. <http://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/ios-software-releases-12-4-mainline/whitepaper_C11-719867.html> [cit. 2014-05-20].

[5] Cisco Systems. *Cisco CleanAir Technology: Intelligence in Action*, 2014. <http://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/cleanair-technology/white_paper_c11-59926> [cit. 2014-05-20].

[6] Cisco Systems. *Cisco IOS Technologies*, 2014. <http://www.cisco.com/c/en/us/products/ios-nx-os-software/ios-technologies/index.html> [cit. 2014-05-20].

[7] Cisco Systems. *Cisco Meraki Cloud Architecture*, 2014. <https://meraki.cisco.com/products/architecture/> [cit. 2014-05-20].

[8] Cisco Systems. *Compare Products and Solutions*, 2014. <http://www.cisco.com/c/en/us/products/wireless/buyers-guide.html> [cit. 2014-05-20].

[9] Computer History Museum. *Timeline of Computer History: Networking Entries*, 2006. <http://www.computerhistory.org/timeline/?category=net> [cit. 2014-05-20].

[10] J. Crane. *Chanalyzer + Wi-Spy User Guide – MetaGeek Support*, 2014. <http://support.metageek.net/hc/en-us/articles/201872824-Chanalyzer-Wi-Spy-User-Guide> [cit. 2014-05-20].

[11] DD-WRT Community. *DD-WRT: Supported Devices*, 2014. <http://www.dd-wrt.com/wiki/index.php/Supported_Devices> [cit. 2014-05-20].

[12] DD-WRT Community. *What is DD-WRT? V24_pre_sp2 K24*, 2014. <http://www.dd-wrt.com/wiki/index.php/What_is_DD-WRT%3F #V24_pre_sp2_K24> [cit. 2014-05-20].

[13] Fabfolk, Inc. *FabFi*, 2011. <http://fabfi.fabfolk.com/> [cit. 2014-05-20].

[14] R. Haden. *Wi-Fi Security – Open Authentication [image]*. <http://www.rhyshaden.com/wifisec.htm> [cit. 2014-05-20].

[15] Hewlett-Packard Development Company. *Connect with confidence with HP Wi-Fi Clear Connect*, 2013. <http://h20195.www2.hp.com/V2/GetPDF.aspx/4AA4-5077ENW.pdf> [cit. 2014-05-20].

[16] Hewlett-Packard Development Company. *HP FlexNetwork Architecture*, 2014. <http://h17007.www1.hp.com/us/en/networking/solutions/flexnetwork/index.aspx> [cit. 2014-05-20].

[17] Hewlett-Packard Development Company. *HP MSM Controller Series Quickspecs*, 2014. <http://h18000.www1.hp.com/products/quickspecs/13271_div/13271_div.pdf> [cit. 2014-05-20].

[18] Hewlett-Packard Development Company. *HP Readies Client Networks for Virtualization, Multimedia and Mobile Devices*, 2014. <http://www8.hp.com/nz/en/hp-news/press-release.html?id=1093946> [cit. 2014-05-20].

[19] IEEE. *Official IEEE 802.11 Working Group Project Timelines*, 2014. <http://grouper.ieee.org/groups/802/11/Reports/802.11_Timelines.htm> [cit. 2014-05-20].

[20] Ch. Jackson. *Dynamic Sharing of Radio Spectrum: A Brief History [Draft]*. 2002. <http://www.jacksons.net/working%20papers/Dynamic%20Sharing%20%202002%20version.pdf> [cit. 2014-05-20].

[21] Meraka Institute. *Wireless Africa*, 2009. <http://wirelessafrica.meraka.org.za/> [cit. 2014-05-20].

[22] Microsoft. *How 802.11 Wireless Works – 802.11 Architecture [image]*, 2003. <http://technet.microsoft.com/en-us/library/cc757419%28v=ws.10%29.aspx> [cit. 2014-05-20].

[23] The Editors of Encyclopaedia Britannica. *Wi-Fi (networking technology)*. 2013. <http://www.britannica.com/EBchecked/topic/1473553/Wi-Fi> [cit. 2014-05-20].

[24] OpenWrt project. *Listing of generic OpenWrt packages for version 12.09*, 2014. <http://downloads.openwrt.org/attitude_adjustment/12.09/atheros/generic/packages/> [cit. 2014-05-20].

[25] J. C. Stein. *Indoor Radio WLAN Performance. Part II: Range Performance in a Dense Office Environment*. <http://erasme.org/IMG/experience_attenuation.pdf> [cit. 2014-05-20].

[26] Ubiquiti Networks. *SR71-A Outdoor 3x3 802.11n MIMO mini-PCI Module. Datasheet.*, 2014. <http://www.ubnt.com/downloads/sr71a_datasheet.pdf> [cit. 2014-05-20].

[27] Wi-Fi Alliance. *Discover Wi-Fi*, 2014. <http://www.wi-fi.org/discover-wi-fi> [cit. 2014-05-20].

[28] Wikipedia contributors. *Wikipedia – 2.4 GHz Wi-Fi channels (802.11b,g WLAN) [image]*, 2009. <http://commons.wikimedia.org/wiki/File:2.4_GHz_Wi-Fi_channels_%28802.11b,g_WLAN%29.svg> [cit. 2014-05-20].

[29] R. Wilson. *Propagation Losses Through Common Building Materials: 2.4 GHz vs 5 GHz*. 2002. <http://www.ko4bb.com/Manuals/05)_GPS_Timing/E10589_Propagation_Losses_2_and_5GHz.pdf> [cit. 2014-05-20].