Milan GRENAR, Miloslav FILKA

Brno University of Technology

doi:10.15199/48.2015.06.26

The most frequent shortcomings of Wi-Fi operators

Abstract. *This paper is focused to the most frequent shortcomings of WiFi technology operators seen by monitoring of broadband data transmission in frequency bands 2.4 GHz up to 66 GHz. The used process of measuring an evaluation of measured data summarized by the devices used by Czech Telecommunication Office for inspection and supervision is performed next. The paper is concluded by real examples of various shortcomings and mistakes.*

Streszczenie. *W artykule analizowano najczęściej pojawiające się wady technologii WiFi występujące w paśmie 2.4 GHz - 66 GHz. Badano układy stosowane przez Czeski Urząd Telekomunikacji.* ***Najczęstsze defekty występujące wśród operatorów sieci WiFi w Czeskim Systemie Telekomunikacji***

Keywords: broadband data transmission, Wi-Fi, spectrum analysis, interference,
Słowa kluczowe: sieci bezprzewodowe, WiFi, zakłócenia I interferencje.

Introduction

The frequency spectrum in the Czech Republic is regulated by the national regulator - Czech Telecommunication Office (next CTU), which deployed the network of stationary un-manned monitoring stations, (SNMS) and two stationary manned stations (SOMS). The measured data are sent there periodically and processed. The individual regional departments of CTU are equipped by mobile manned monitoring stations (MOMS) with measuring equipment Rohde & Schwarz together with Hewlett Packard computing technology enabling the measurement up to 6 GHz. Except these MOMS are used mobile unmanned monitoring stations (MNMS) in localities not covered by regular stationary SNMS. The vehicles with MOMS serve for precise identification of the disturbing sources as well as usage of not approved and therefore colliding frequencies.

General License VO-R/12/09.2010-12 is supervised by CTU frequently. First of all is used by WiFi technology, which is very popular at all. Almost every user utilizes WiFi in his notebook, by smart phones of various producers or in routers as well as by xDSL or Cable modems for covering flats or buildings. This technology is widely used by internet service providers (ISP) for covering of villages or various town sites due to the very slow introduction of ADSL technology more than decade ago.

CTU regional office in South Moravia supervises more than 550 ISPs while vast majority of them utilizes 2.5 GHz and 5 GHz bands. Annual report of CTÚ for 2010 performs, that BB internet by WLL technologies (WiFi, FWA) is sharing by 25.7%, what is the second highest in the whole stake of all technologies. DSL itself with ADSL as well as newly VDSL first sharing 28.8% and mobile networks (CDMA, UMTS) as third share 19.4%. The other technologies behind are losing with less than 10% share of the stake.

The brief feature of General License Nr. VO-R/12/09.2010-12 for broadband data transmission in bands 2.4 GHz up to 66 GHz

This general license defines requirements for device operation related to the exploitation of radio frequencies for broad-band data transmitters (station) by physical persons as well as legal entities.

Concrete requirements defined by General Licence Nr. VO-R/12/09.2010-12 [1]

General License Nr. VO-R/12/09.2010-12 defines following requirements:

a) The station may be operated without individual license for radio frequencies utilizing;
b) Technical parameters of stations – see Table. 1.

Table 1. Technical parameters of stations

Mark	Frequency band	Radiated wattage	Maximal spectral density e.i.r.p.	Other requirements
a	2400.0 - 2483.5 MHz	100 mW mean e.i.r.p.	10 mW/1 MHz 100 mW/100 kHz	systems with DSSS or OFDM systems FHSS
b	5150 - 5250 MHz	200 mW mean e.i.r.p	10 mW/MHz (mean spectral density in random span of 1 MHz)	
c	5250 - 5350 MHz	200 mW mean e.i.r.p.	10 mW/MHz (mean spectral density in random span of 1 MHz)	For internal use only.
d	5470 - 5725 MHz	1 W mean e.i.r.p.	50 mW/MHz (mean spectral density in random span of 1 MHz)	—
e	17.1–17.3 GHz	100 mW mean e.i.r.p.	—	—
f	57 - 66 GHz	40 dBm mean e.i.r.p.	13 dBm/MHz (mean spectral density)	Fixed outdoor installations are excluded

c) The stations are obliged to keep maximal radiated wattage e.i.r.p. and maximal mean spectral density by random combination of output power of transmitter and used antenna;
d) The stations are not allowed to be operated with additional amplifiers of high frequency wattage as well as re-transmitters;
e) The stations of band marked c) and d) in the Table 1 shall be equipped by automatic output wattage regulation, which is able to suppress interference 3 dB min. against maximal allowed output wattage. In case of no automatic regulation of wattage used the max. allowed mean e.i.r.p. is to be decreased to limit of e.i.r.p. 3 dB lower for above mentioned bands c and d;
f) For bands c) d) and f) shall be used methods for access

to the spectrum as well as the reduction of interference enabling equal outcome as techniques described in harmonized standards. Suppression of interference techniques in bands c) and d) should equalize the probability of choose of concrete channel of all accessible ones to secure the equal spread of spectrum load as well as to ensure the compatible operation with systems of radio determination;

g) The stations are operated with shared frequencies;

h) The operation of the station is not provided by protection against interference inflicted by radio stations of other radio link services operated in accordance with individual license for radio frequencies utilizing or by another broadband station.

Actual situation of Wi-Fi exploitation in CZ

The situation in frequency bands 2.4 GHz and 5 GHz is not comparable anywhere abroad. Large number of ISPs in electronic communication (see above) is focused into this technology due to the simple reason: the frequency usage is not charged and costs for used technology are very friendly.

2.4 GHz band is frequently exploited by ISPs due to the low number of channels; therefore some ISPs are changing it for 5 GHz. Just low number of channels in first band forced ISPs to higher radiated wattage to secure connectivity to APs (access point) and consequently interfere with other ISPs.

The band 5 GHz has more channels, but it is divided – see Table VO-R/12/09.2010-12 [1] – into indoor and outdoor frequencies. Sometimes ISPs uses indoor frequencies in the outside due to their ignorance or the lack of channels.

CTU as the administrator of spectrum monitors radio transmitters by following procedure: In. case of disruption on, VO-R/12/09.2010-12 follows state supervision and summons for remedy. CTU launches administrative procedure in case of summons neglecting.

Monitoring & Equipment

There is important to choose the reference measuring points where the intensity of electromagnetic field will be measured. Those localities shall be defined positively for possible consequent state supervision (city, street, home number, the height of antenna).

Antenna shall be positioned:

- In direct visibility of transmitter VRZ;
- In the axis of radiated bundle;
- In the main direction of radiation.

The devices N – Stream Mikrotom, Mikrotic Router-Board RB433 are used for detection and identification of Wi-Fi.

For measurement in bands 2.4 GHz and 5 GHz are used measuring sets of calibrated antenna with defined correction, signal supplying line and, measuring device, which shall be calibrated in predefined time intervals. The supplying line shall be used with known parameters (attenuation) for frequency span of measured signals.

The following devices and components are used for measurements:

- Spectrum analyzer R&S FSQ8;
- Spectrum analyzer R&S FSH6.

Most frequently used antennas:

- Omnidirectional vertical type Alvarion;
- Panel antenna DCom ZZS 5G;
- 5 GHz Alfa 12 dBi;
- Directional antenna 5 GHz;
- R&S HL 040, Andrew T 2400;

Other used components:

- Low noise amplifier DCom LNA 250406;
- Directional coupling CD-202-402-10N.

Methods of Power Measurements [4]**:**

This measurement is realizable by following two methods:

1. The measuring device FSH6 is coupled through directional splitter with measured equipment. The power inside the channel is calculated or is measured directly through power probe.
2. When the first method is not utilizable due to the absence of transmitting equipment or the antenna is integrated into the covering of transmitter (for outdoor version), the power may be calculated. This method is exact and verified. CTU provided several tests, where calculated and measured values were evaluated:

$$EIRP = P + b - G + L \text{ [dB]}, \quad (1)$$

where: P is measured power (across whole frequency span OBW) [dBm]; bis the loss of cable – analyzer [dB]; G is the gain of measuring antenna [dBi]; L is the propagation loss in the open space = 20logr + 20logE + 32.45 [dB]; E= 10 logP - 20 logr + 77 [MHz]; r is distance [km].

Every technician of the CTU measuring group has Excel file with macros, which is able to calculate demanded results. See Fig. 1.

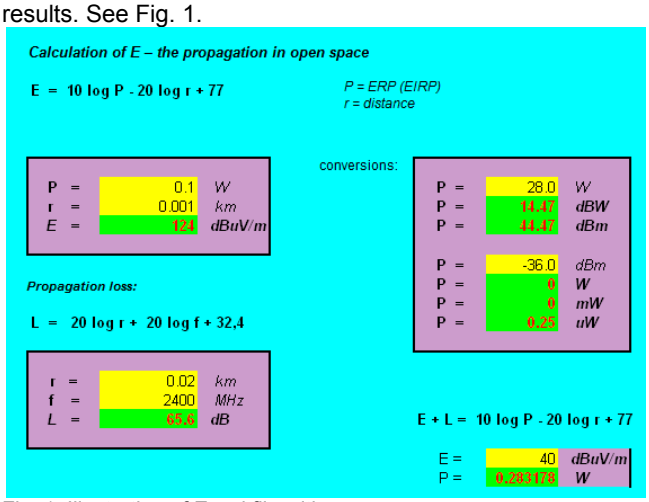

Fig. 1. Illustration of Excel file with macros

The most frequent cases of violation of License Nr. VO-R/12/09.2010-12 for broadband data transmission in bands 2.4 GHz up to 66 GHz

The violation of the total radiated power EIRP by 2.4 GHz [2]

In the following map – see Picture 2 – are pointed stations of supervised transmitters together with reference measuring points. These measurements supervise if the EIRP of measured station was not changed before measurement (where the arrangement of the term of supervision is necessary).

Fig. 2. The map with reference measuring points and measured stations

Technical parameters of measured equipment

1. Planet WA-1911 placed in the address: Tr. D. Hrdinu 27
2. WL-1120 AP placed in the address: Tr. D. Hrdinu 36

Measured values – see Fig. 3 up to 8:

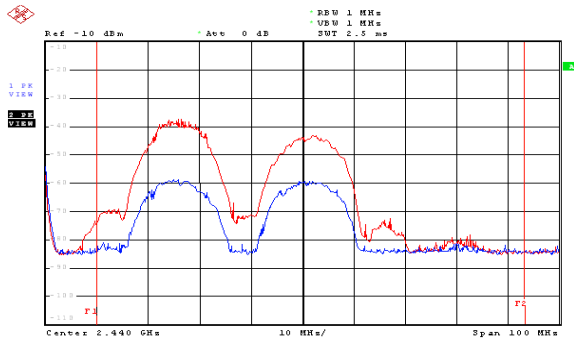

Fig. 3. Spectrum of signals on measuring point 1 Polarization: red - vertical / blue - horizontal

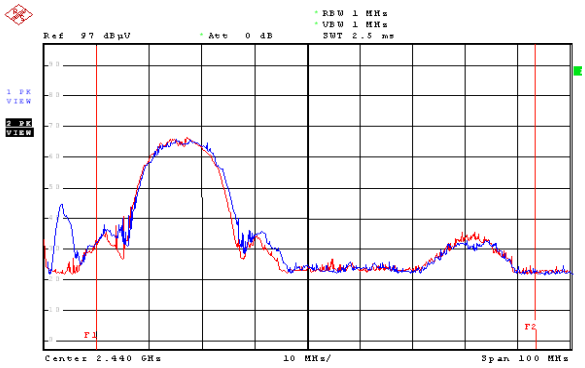

Fig. 4. Spectrum signals on measuring point 2. Red=measurement a day before control, blue=measurementat in the day of control.

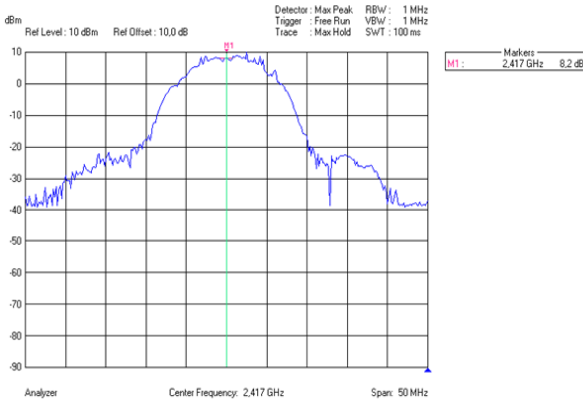

Fig. 5. Planet WA-1911. The measurement of peak power density

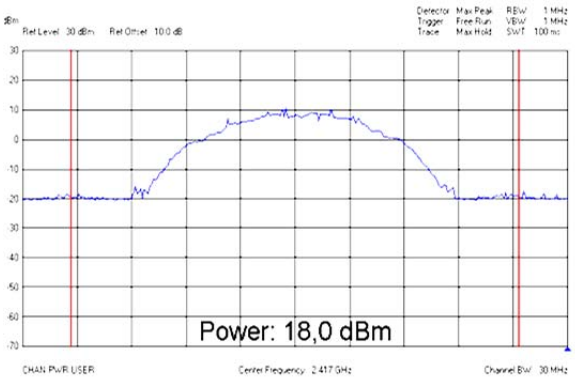

Fig. 6. Planet WA-1911 Measurement of total spectral power TX

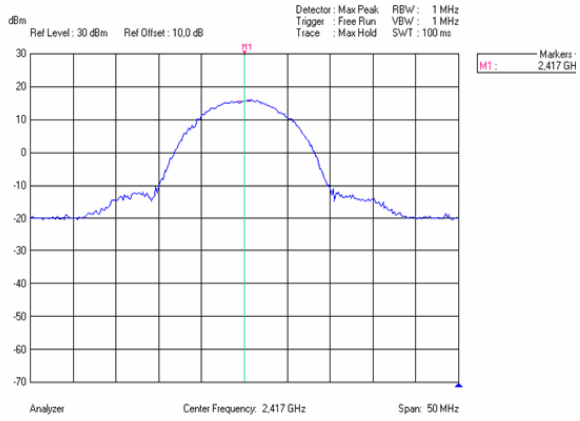

Fig. 7. WL-1120 AP Measurement of peak spectral power density

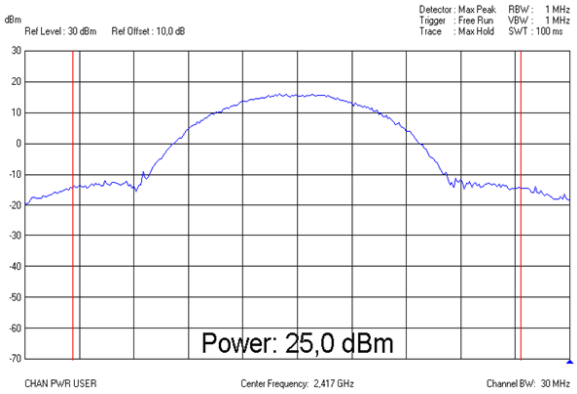

Fig. 8. WL-1120 AP Measurement of total power TX

Shortly before launching of measurements on transmitter station during first day the spectrum was supervised on both measuring points as it is evident from the Fig. 4. No change of EIRP was occurred; therefore the measurement of transmitter station performs real operational status. (No preventive correction of EIRP was discovered).

Shortened record and calculation

1. Measured equipment

Sort: RLAN 802.11b Wireless access point.
Type: Planet WAP-1911.
Production Nr.:xxxxxxxxxx.
Version of transmission: DSSS, 80MOG1DXN.

Antenna

Sort: omnidirectional.
Type of antenna: model MSA -12PF.
The height above surface: 7 m.
Polarization /lowering: V.
Main direction of radiation: -°.
Gain (data of producer):12 dBi.
Loss of supplying coupling: 2.0 dB.

Measured values

Output power of transmitter: -12.0 dBW.
Peak EIRP (calculation): -12.0 + 12.0 – 2.0 = -2 dBW.
Peak spectral power density: -21.8 dBW/1 MHz.
Peak spectral density EIRP: -21.8 + 12.0 – 2.0.
= -11.8 dBW/ 1 MHz.
Frequency: 2417 MHz.
Frequency deviation: -

2. Measured equipment
Sort: RLAN 802.11b Wireless access point.
Type: WL-1120 AP.
Production Nr: xxxxxxxxxxxx.

Version of transmission: DSSS, 120KG1DAN (in accordance with Declaration of Conformity).
Sort: omnidirectional
Type of antenna: model MSA -12PF.
The height above surface: 15 m.
Polarization / lowering: V.
Main direction of radiation: -°.
Gain (data of producer):12 dBi.
Loss of supplying coupling: 2.0 dB.
Measured values
Output power of transmitter: -5.0 dBW.
Peak EIRP (calculation): -5.0 + 12.0 – 2.0 = 5.0 dBW.
Peak spectral power density: -14.2 dBW/1MHz.
Peak spectral density EIRP: -14.2 + 12.0 – 2.0.
= -4.2 dBW/ 1 MHz.
Frequency: 2417 MHz.
Frequency deviation: -

Evaluation of monitoring
The informative survey is completed in following Table 2:
Table 2. Results of Monitoring

Type of Transmitter	EIRP (dBW)	S_{EIRP} (dBW/1MHz)
Planet WAP-1911	-2.0	-11.8
WL-1120 AP	5.0	-4.2

As it is evident from the above published results in the Table 2, both cases are resulting out of limits VO-R/12/09.2010-12 which are:
Total radiated power EIRP: max. -10 dBW;
Peak spectral power density: max. -20 dBW/1MHz.

Unauthorized frequency utilizing

The violation of General Authorization Nr. VO-R/12/09.2010-12 due to the exploitation of the band 5150-5350 MHz appointed for indoor operation outside [5].

The following records depict spectra of signals measured in distance roughly 100 m off the transmitter (the exact description of the reference measuring point) – see Fig. 9.

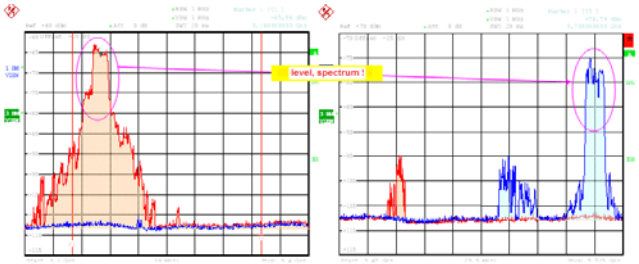

Fig. 9. Spectrum of transmitted signals before and after retuning

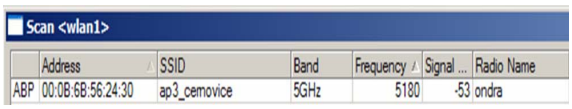

Fig. 10. Before frequency retuning

The print screen below performed below is the result of signal analysis of analogue mikrotic with MAC addresses and SSID of RLAN networks before as well after retuning – see Fig. 10 and Fig. 11.

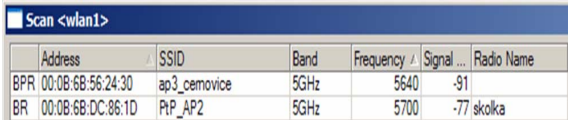

Fig. 11. After frequency retuning

The transmitter operating on the frequency 5180 MHz for local covering of the village was retuned to 5600 MHz to be conformed to General Authorization VO-R/12/09.2010-12.

Interference due to the deliberate sending of de-authentication packets

Next violation is disturbing of WiFi network operation. This situation occurs in smaller towns or villages with several active ISPs. Limited number of potential clients and a great competition leads to the unfair methods between them. The most serious infliction is deliberate technical violation of the counterparts operation.

These investigations demand plenty of time. There is possible to describe on incident. The ISP announced long term and irregular interference, while their clients were losing often their connection to their access point.

The results of this investigation proved, that these deaut. packets were transmitted with identical source MAC addresses to the MAC addresses of access points of disturbed network. The ISP of disturbing transmitter retuned it on to 5 GHz channels of competing ISP. He paralyzed WiFi competing network successfully by systematic transmitting of deauthentication packets.

The transmitters with source MAC addresses of disturbed access points were located as standby APs of disturbing ISP. The identification and ownership of disturbing devices was verified consequently by switching of this device. – See Fig. 12 and Fig. 13.

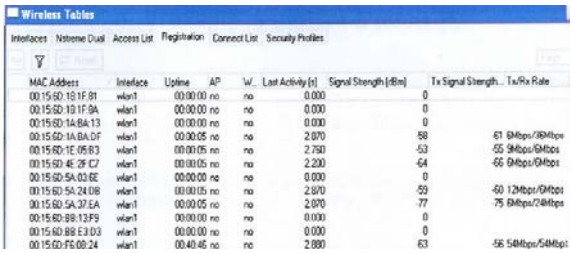

Fig. 12. Dropouts of AP communication
(Notice: The column „Uptime" performs time of client's connection which corresponds with interval of deaut. packets transmission. The longer period of last client corresponds probably with worst radio visibility to the source of Deaut. packets.)

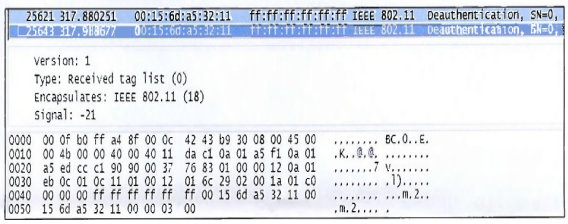

Fig. 13. Details of deaut. packet
(Notice: The value of received power to input of radio receiver – 21 dBm during the local testing.)

The method of packet capture was used using Mikrotic device (with directional antenna for defining of azimuth by max. value of received power) supported analysis and seeking of the source of disturbance. This device was set to transmit-ting frequency of disturbed AP. The received packets were sent immediately into „Open source software" Wireshark immediate analysis.

This analysis verified the fact that disconnection of clients is caused by deliberately transmitted deaut. packets with identical MAC source address corresponding to AP.

Conclusion

This paper summarizes most frequent violations of WiFi networks by ISPs themselves.

1. The overrun of transmitted power due to the incorrect adjustment of AP or by using unsuitable antenna. The one-way attenuation element is to be used with powerful antenna for longer distances. There is possible to set different loss for transmitting orientation (from 3 up to 34 dB) and receiving orientation (from 3 up to 4dB).

2. ISP shall be heedful by setting of AP to use indoor frequencies surely inside strictly. The outer usage is prohibited.

3. ISP may be punished by administrative proceeding and following process with police for deliberate disturbing of competing network internet services. The number of such ISPs offering broadband internet is high, the number of such of-fences is increasing too.

REFERENCES

[1] Všeobecné oprávnění č. VO-R/12/09.2010-12 k využívání rádiových kmitočtů a k provozování zařízení pro širokopásmový přenos dat v pásmech 2,4 GHz až 66 GHz, Praha. 29.09.2010; (General Authorization Nr. VO-R/12/09.2010-12, Prague, September 29th 2010.)

[2] Grenar, M., Reports of CTU describing violation of General Authorization VO-R/12/09.2010-12.

[3] Zandl, P., Bezdrátové sítě WiFi – praktický průvodce, Praha 2008

[4] Pužmanová, R., Širokopásmový internet, Praha 2009

[5] Pužmanová, R., Bezpečnost bezdrátové komunikace, Praha 2010

***Authors**: Ing. Milan Grenar and prof. Ing. Miloslav Filka, CSc., Brno University of technology, Faculty of Electrical Engineering and Communication, Departement of Telecomunications, Technicka 3058/12, 616 00 Brno, Czech republic. E-mails: xgrena03@stud.feec.vutbr.cz and filka@feec.vutbr.cz.*