Channel allocation technique for eliminating interference caused by RLANs on meteorological radars in 5 GHz band

ZOLTÁN HORVÁTH, DÁVID VARGA

Budapest University of Technology and Economics, Department of Telecommunications
horvathz@hit.bme.hu, varga.david@duvinet.hu

Keywords: 802.11a, interference, meteorological radar, RLAN, WLAN, Wi-Fi, 5 GHz band, RTS/CTS, DFS, 802.11h

Meteorological radars are used for short term weather prediction in Hungary and all over the world. These radars can be jammed by RLAN devices (e.g. home Wi-Fi routers). We introduce the background of this problem, and analyze the weakness of the current solution (DFS – Dynamic Frequency Selection). We analyze it theoretically by modeling the radar operation and RLAN traffic, and we also show its high efficiency in practice, based on well-known IEEE 802.11 RTS/CTS mechanism.

1. Introduction

The introduction of modern meteorological radars has revolutionized accurate short-term forecasts. But at that time nobody thought, that the quickly spread wireless networks (further: Wi-Fi – Wireless Fidelity, WLAN – Wireless Local Area Network, RLAN – Radio Local Area Network) [4] would affect negatively the performance of radar systems – in a large number of countries worldwide [1-3 and 9-15].

In the beginning of the next section (Subsection 2.1) we show how this interference appears on the screen of meteorological radars, and discuss the serious consequences it may cause. We also specify the origins of the interference from a technical point of view. Of course, as the problem expanded, engineers tried to come up with a solution. This led to the development of DFS (Dynamic Frequency Selection), which is a standardized method introduced in IEEE 802.11h.

Of course, the WLAN devices need to comply with it, so DFS compliance tests were introduced in the ETSI 301 893 documents. The ETSI standard is still under development. Almost every year or two a newer version is revealed, trying to make the tests be more similar to real life events. The details of DFS are discussed in Subsection 2.2.

Unfortunately, the DFS still can not provide enough protection for the radar systems; many WLAN devices don't perfectly comply with the standards. We summarize the problems with DFS (identified by us) in Subsection 2.3. The next subsection presents some of the solutions we proposed, that could possibly detect and even filter WLAN interference at the radar systems. Some of these solutions are easier to manage, some are only

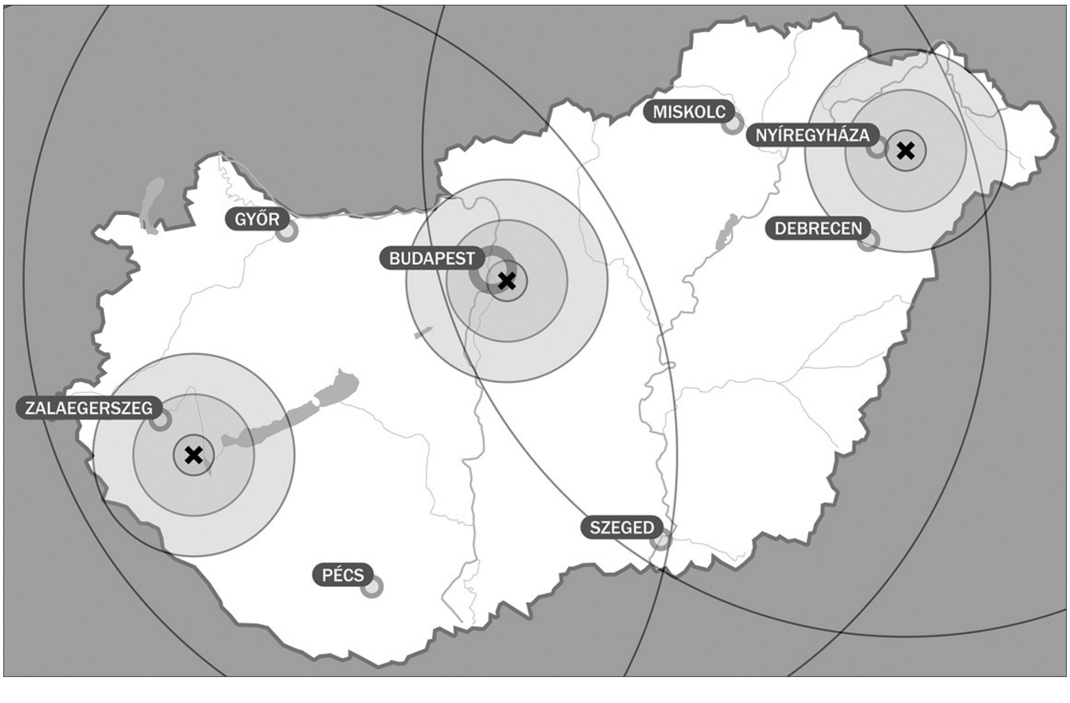


Figure 1.
The three meteorological radars in Hungary
The concentric circles show affected areas with 10, 30 and 50 km radius and 240 km radius as maximum of radars observation range around the three meteorological radars in Hungary (Pogányvár, Budapest and Napkor).

theoretical, and could not be implemented because of the technical parameters of the radars.

As the main topic of this paper, in Section 3 and 4 we introduce a method, which does not only detect and filter WLAN interference, but also eliminates it before it could actually happen. We present here a preventive solution, which is based on channel allocation. It can reserve the channel for the radar while the measurements are done, by silencing the WLAN transmitters in direction. In Section 3 we present the overview of the main idea and some background information for the next section (Section 4), in which we introduce the allocation technique in detail using traffic models and estimation, and present some evaluation of it. Finally, conclusions are summarized in Section 5.

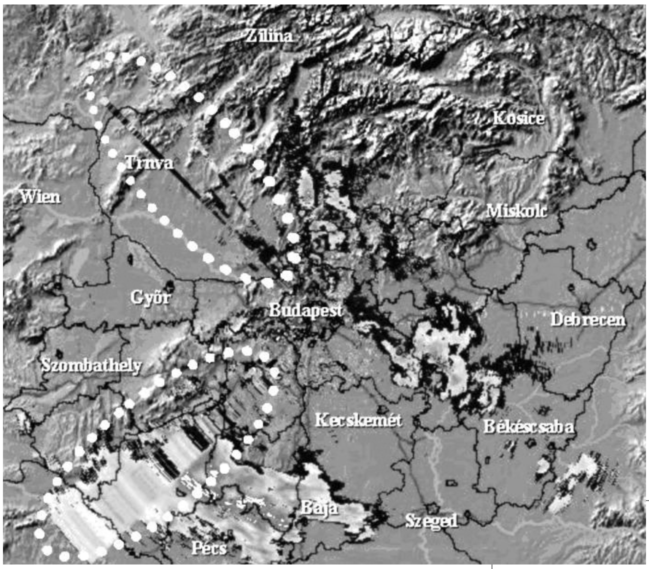
2. Interference and some solutions

2.1 Introduction of the interference

As part of the European weather forecast system, there are three weather radars in operation in Hungary under the supervision of Hungarian Meteorological Service (OMSZ) and several others throughout Europe and all over the word. The locations of the Hungarian radars are shown in *Figure 1*. These radars measure the atmosphere precipitation. Radar operation is detailed in Subsection 3.3.

Figure 2.
RLAN interference in the picture of the meteorological radar

There are not only clouds in the picture but also strips and sectors are shown marked by dotted curves. They are caused by RLAN interference, and inhibit observing of the precipitation.



Based on the information and pictures provided by the OMSZ, *Figure 2* shows the influence of the strays on a rough radar image. Each shade means a different dBZ level, corresponding to the intensity of the reflected signal. If the shade represents a larger numerical value, it means higher received signal strength [16,18].

The jammed layers indicate significant quantity of rain, so their influence is rather disturbing. It is also dangerous when the signals reflected by precipitation are combined with the ones from the strays (see in the left bottom of Figure 2) and as a result we may come to a false conclusion regarding the quantity of the precipitation. This may cause significant problems in the weather forecast and pre-estimations.

The layers and sectors appearing in the images are mostly caused by IEEE 802.11a standard WLAN devices located close to ground and operating within the radar's frequency range [1-3 and 9-10]. One of the (frequently used) frequency bands where the meteorological radars may operate is between 5600-5650 MHz, which overlaps with 3 of the 802.11a channels (No. 120, 124 and 128) [17]. They are shown in *Figure 3*.

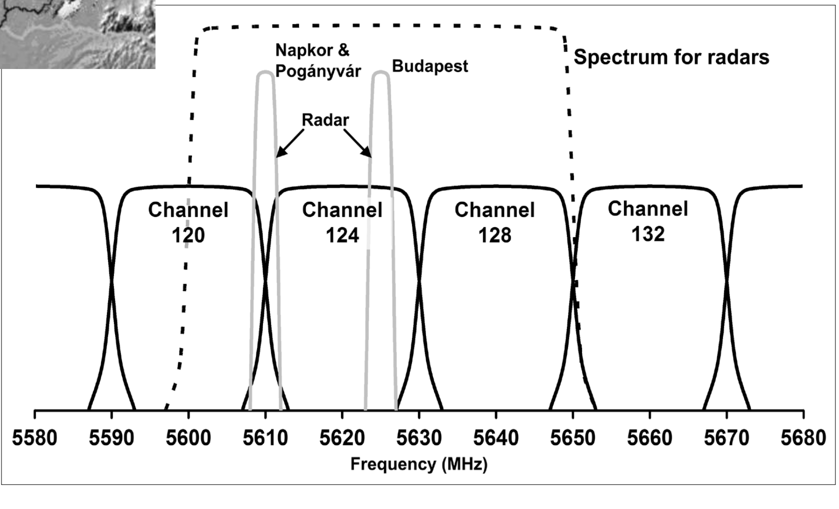
2.2 DFS to solve the problem

A method has been standardized to solve this problem. Dynamic Frequency Selection (DFS) has become the technological solution to resolve the interference issues between meteorological radar systems and WLAN devices. There are two standards related to DFS: the IEEE 802.11h standard and the ETSI EN 301 893 directives.

The IEEE 802.11h standard is [4] an amendment to the original 802.11 standard [4] which deals with the radio spectrum and power management operations in detail. It defines new processes, message types and frame types to be implemented. Although the main function of the standard is to cooperate with European radar systems, it also offers a possibility to have a uniformly used

Figure 3.
Usage of the frequency band by 802.11a channels and the meteorological radars in Hungary

The 5600-5650 MHz band for meteorological radars and the three affected 802.11a channels (No. 120, 124 and 128) are shown in the picture. There are two narrow frequency bands used by the three Hungarian meteorological stations (Pogányvár, Budapest and Napkor).



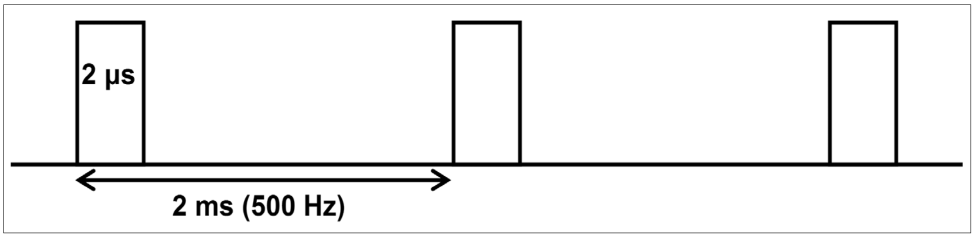


Figure 4.
A sample of radar signals for DFS compatibility tests

Similar DFS test patterns are defined in ETSI directive [5-8]. This one specifies 2 µs pulses with 2 ms repetition time (500 Hz repetition frequency).

radio spectrum, and to manage coverage or power consumption with Transmit Power Control (TPC).

The standard defines horizontal and vertical communication protocols (between stations and within a station, respectively), but it allows the manufacturers to choose their own implementation. It does not even define the conditions (e.g. radar signal detecting), that start the extended functions in the devices. The ETSI EN 301 393 documents [5-8] contain information regarding these conditions [11-15].

The ETSI EN 301 893 standards summarize the functional requirements, that every radio access network operating in the 5 GHz band has to meet. These requirements consist of the specification of transmitted signals, but also contain methods of spectrum management, such as DFS. In practice, a device is marked DFS compatible, if it passes the DFS tests of the actual ETSI EN 301 893 standard (further: ETSI). On the other hand, it is questionable whether this DFS compatibility provides enough protection for meteorological radars.

2.3 Problems regarding DFS

We examined the efficiency of DFS using ETSI v1.4.1 [7] both theoretically and in practice [3], and found that the following problems still exist. We introduce briefly these already known and those revealed by us problems here. One of the known issues is that the minimum pulse width for testing against DFS is 0.8 µs, but Hungarian and other radars also use 0.4 µs for better radar resolution, which is harder to detect [1-3, 6-9 and 11-15]. A sample of a radar signal (as ETSI DFS test pattern) is shown in *Figure 4.*

We found that Channel Availability Check time is only 60 seconds in ETSI v1.2.3 [5], v1.3.1 [6] and v1.4.1 [7], but it can be shorter than the radar rotation period [15]. (Note that this has been changed to 10 minutes in ETSI v1.5.1 [8].)

We found also that DFS Slave devices are not required to sense radar signals. In some scenarios, when a DFS Slave device faces the radar, and the radar signal is too weak at the DFS Master, the WLAN devices will not switch the channel, and the DFS Slave will continuously jam the radar [3].

We collected more than 50 certificates of 802.11a WLAN devices on the market, and most of them only complied with older, v1.2.3 [5] or v1.3.1 [6] versions of ETSI. This means, that even if the device was called DFS compatible at the time it was designed, it would not certainly pass the newer versions of ETSI. But these devices are still in operation, or even can be bought and used.

There were some devices we actually tested, and some of them let the end user enable or disable DFS or Radar signal detection, although this function should be automatically and always enabled.

2.4 Our proposed solutions

As we can see, DFS can not, and probably never will provide a perfect solution against radar interference. We came up with some ideas, which are detailed in [3]. Here we provide a quick overview of them.

If we also detect signals in the full 20 MHz wide 802.11a channel, which embraces the 1.25 MHz wide spectrum of the radar, and we sense signals there at the moment when we receive the reflected radar signals, we may say that there was also WLAN interference. In this case the result of those radar measurements can be ignored.

Interference can also be detected or filtered in time scale, if we only look for reflected radar signals in the time period when they could have returned after reflected by hydrometeors. This possible time period can be calculated from the typical minimum and maximum height of the clouds in the actual season, and the altitude angle of the radar. Interference can also be detected or filtered if precipitation maps are received from other sources, including satellites or terrestrial optical camera system, which can observe without this interference. If we use more radars to scan a selected area, then by comparing the different measurements we are able to detect or filter the interference. This can be done by specific algorithms, or majority voting in case of using at least three radars.

There is a chance to separate radar and WLAN signals, if we use some kind of modulation on the radar signals and we detect the reflected signals via an appropriate demodulator. This way WLAN interference would only cause higher noise in demodulation. Unfortunately this method would require the modification of the radar signals in a way that current magnetron based meteorological radars are unable to provide.

The possible solutions mentioned above are useful only for detecting and filtering the already existing interference. Unlike, using our proposed method discussed in Section 3 and 4, we may eliminate the interference before it even existed.

3. Background of channel allocation for interference elimination

3.1 Overview of channel allocation

The basic idea behind channel allocation is to defer the transmission of the WLAN devices for the time the radar faces their direction thus we have to allocate that time slot to the radar. This can be done by sending out information to the WLAN stations prior to the critical interval, which forces them to be silent until the radar turns over them.

This allocation transmission should not affect the operation of the radar; therefore the idle time of the radar should be used.

This transmission can be continuous in space domain with an omnidirectional antenna or a fast rotation directional antenna not synchronized with the radar position. Alternatively, this transmission can be concentrated to the direction where the radar measures, which is better, because it does not affect the WLANs which do not jam the radar at the time. In this case the allocation transmission should be synchronized with the radar rotation spatially. The allocation beam should forerun the radar beam for silencing RLANs at time of radar measurements, or should be identical with it (see Figure 9). In this case the radar antenna can be used to transmit channel allocation indication. In this paper we discuss this possibility.

For this allocation we try to use the RTS/CTS mechanism of 802.11, which sets the NAV of the WLAN stations, thus silencing them for a time as necessary. This mechanism is mandatory implemented in all of the WLAN devices.

3.2 Overview of RTS/CTS mechanism in WLAN

The optional RTS/CTS mechanism in 802.11 [4] is basically used to prevent the hidden terminal problem. This problem refers to a scenario, where ‘A’ wants to send data to ‘B’, and ‘C’ is also in the range of ‘B’, but out of the range of ‘A’ *(Figure 5)*.

Without RTS/CTS it is possible, that after ‘A’ starts to transmit, ‘C’ also starts transmitting, since it senses that the media is free, and creates interference at ‘B’. Using the mechanism, prior to sending the actual data, ‘A’ sends a RTS (Request To Send) frame, telling everyone in its range the duration of its following data frame (and belongings, e.g. ACK, SIFSs). Then ‘B’ sends the CTS (Clear To Send) as a reply, which stations in its range will receive. This way, every station in the range of ‘A’ and ‘B’ should not transmit, while ‘A’ transmits its data.

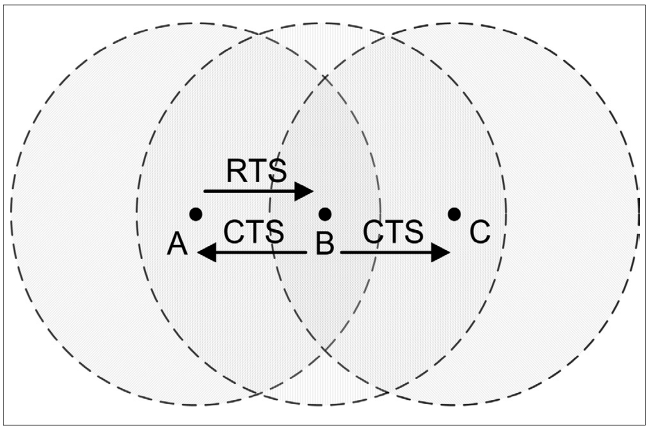


Figure 5.
Hidden terminal problem and RTS/CTS mechanism as a solution

At first node ‘A’ sends RTS to node ‘B’ requesting channel allocation. Node ‘B’ sends CTS indicating that it received RTS and node ‘A’ get the channel. Node ‘C’ received CTS, too.

The RTS/CTS mechanism is generally used in environments where stations in the same network may exist out of each others range.

The mechanism and timing parameters can be seen in *Figure 6*.

3.3 Introduction of weather radar operation

During operation the radar rotates at a specific altitude angle (elevation) or scans a given sector and then raises the elevation.

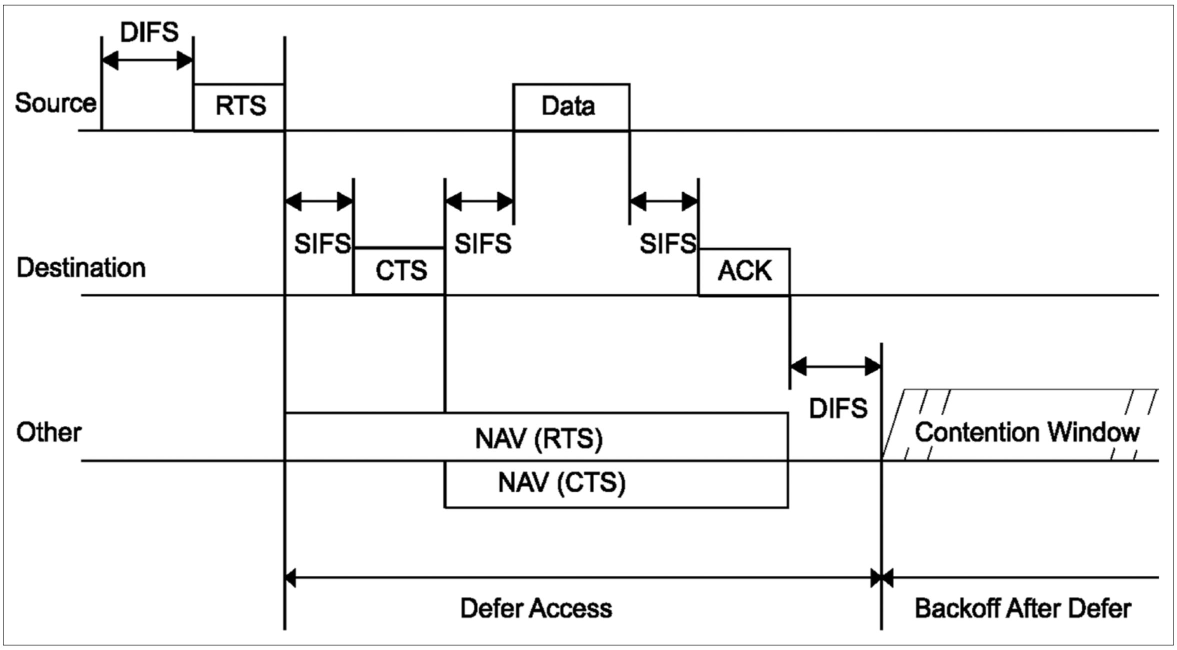


Figure 6.
Timing of RTS, CTS, data, ACK frames and NAV (IEEE 802.11, 2007, Fig. 9-7 [4])

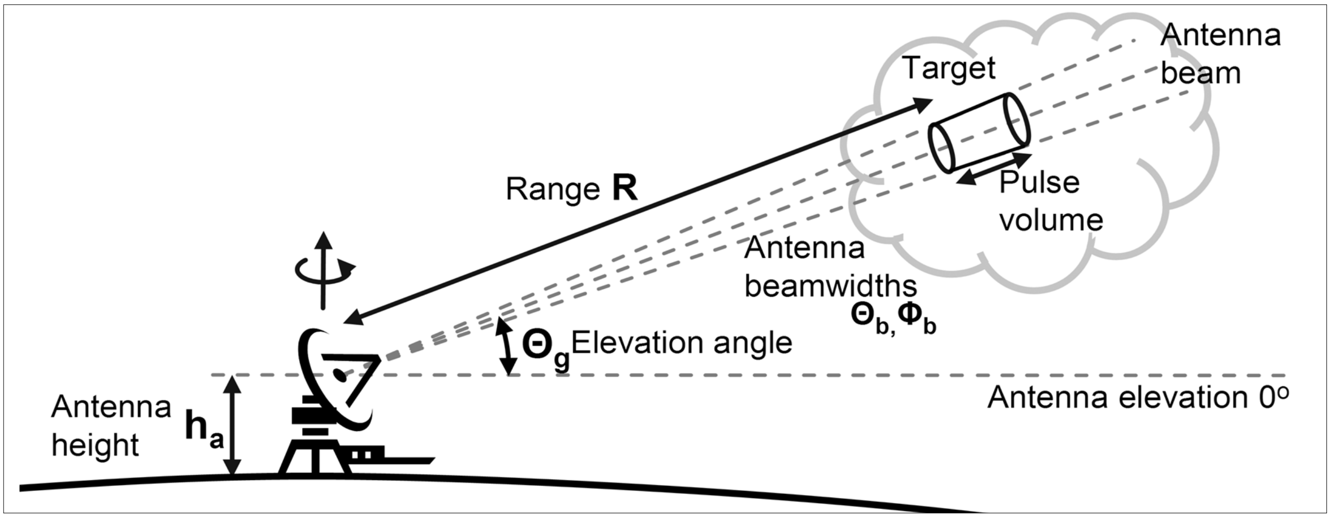


Figure 7. Parameters and operation of meteorological radars
A radar in operation continuously rotates and after each rotation increases elevation angle.

Figure 7 illustrates this operation. In the meantime it transmits radar pulses and receives echoes, reflected by hydrometeors (raindrop, ice) and attenuated by absorption and free space loss (see Fig. 8) [14,16].

Figure 8 shows radar operation in time domain. Each transmitted radar pulse is followed by the echo of it. This backscattering is limited in time by the attenuation and radar signal sensitivity. After each and before the next measurement there is an idle period that will be called 'InterMeasurement Gap' (IMG). In our channel allocation technique this gap is used, so the radar operation and functionality is not affected.

4. Modeling, analysis and evaluation

For analyzing and evaluating the proposed solution building a model is indispensable.

4.1 Modeling radar and RLAN traffic

At first radar and RLAN traffic are described by their timing and other parameters.

4.1.1 Modeling radar operation

As introduced in Subsection 3.3 the radar antenna rotates under operation. Rotation speed is given in RPM (Rotation per Minute) generally in most of the radar specifications. This value – denoted by 'β' – is needed in degree/sec (°/s) measure for further calculation.

$$\beta = \frac{RPM \cdot 360}{60} = RPM \cdot 6 \qquad [°/s]\ (1)$$

Another main parameter of the radars is the horizontal beam width (α) measured in degrees (°). These parameters are shown in *Figure 9*.

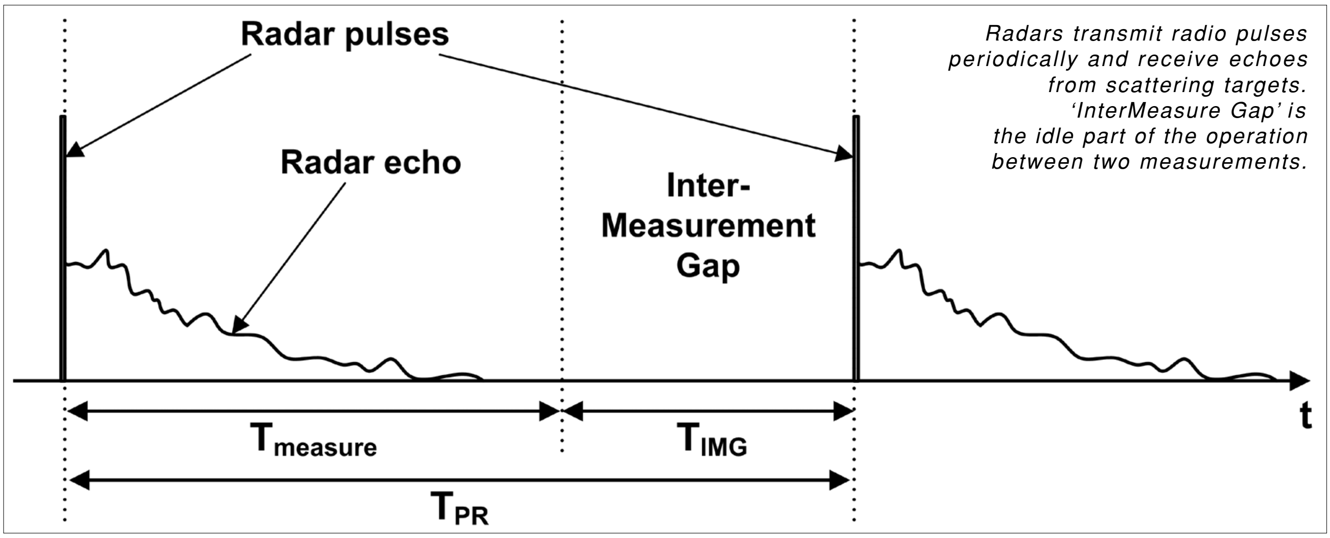
Every radar rotation has a period, when the radar scans a specific point, as described in Subsection 3.3. This 'Contacted Time' (T_{cont}) is constant for each point:

$$T_{cont} = \frac{\alpha}{\beta} \qquad [s]\ (2)$$

During this period radars periodically transmit pulses. This is specified as 'Pulse Repetition Frequency' (PRF) in Hz (1/s). It has the same meaning as Pulse Repetition (PR) Time (T_{PR}):

$$T_{PR} = \frac{1}{PRF} \qquad [s]\ (3)$$

Figure 8. Transmitted and received signal of radars in time domain



Radars transmit radio pulses periodically and receive echoes from scattering targets. 'InterMeasure Gap' is the idle part of the operation between two measurements.

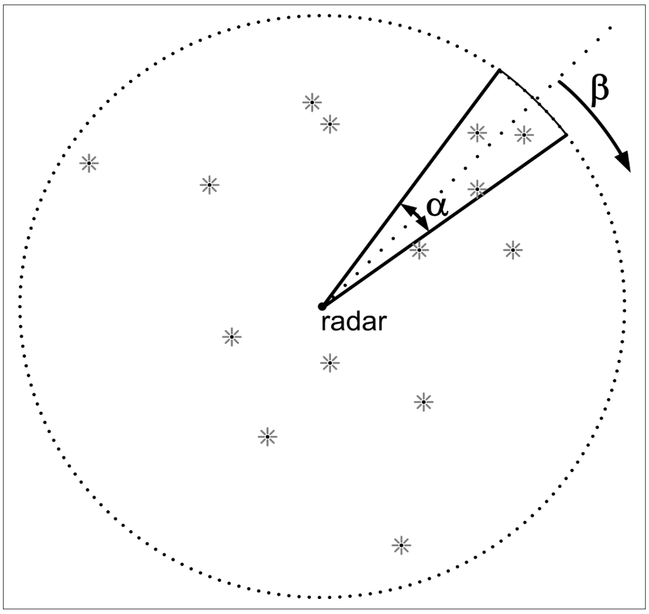


Figure 9. Radar scanning and RLAN devices
The radar rotates with α beam width and β rotation speed.

The time interval between two consecutive pulses can be divided into two periods (see Fig. 8). The first one is between the transmission of a pulse and the theoretical limit when its echo is received by the radar. This measurement time ($T_{measure}$ [s]) is calculated from maximum range of the radar (R [m]) and signal propagation speed ('speed of light') (c [m/s]):

$$T_{measure} = \frac{2 \cdot R}{c} \quad [s] \; (4)$$

The second period is the idle time between the end of observation and the next pulse, called Time of Inter-Measurement Gap (IMG) (T_{IMG} [s]):

$$T_{IMG} = T_{PR} - T_{measure} = \frac{1}{PRF} - \frac{2 \cdot R}{c} \quad [s] \; (5)$$

The pulse length is negligible compared to other durations; therefore it is omitted in this formula. Using these parameters the utilization of the radar and the channel is:

$$U_{measure} = \frac{T_{measure}}{T_{PR}} = \frac{2 \cdot R \cdot PRF}{c} \quad (6)$$

The number of pulses (N_{P_CT}) and InterMeasurement Gaps in 'Contacted Time' (N_{IMG_CT}) is defined as:

$$N_{P\_CT} = N_{IMG\_CT} = \frac{T_{cont}}{T_{PR}} = T_{cont} \cdot PRF \quad (7)$$

4.1.2 Modeling RLAN traffic

Not only radar operation, but also RLAN traffic should be described in order to be able analyze and model the proposed solution.

We analyze two scenarios for modeling RLAN traffic, in 'Scenario I' without and in 'Scenario II' with acknowledgements (ACK).

Scenario I: RLAN traffic without ACKs

In 'Scenario I' RLAN traffic consists of data frames only without any acknowledgement (ACK), therefore RLAN transmission contains frames and idle times. In general distributions of frame size and arrival times are unknown. We use this deterministic traffic pattern for modeling, because this is the worst case: all of the frames use the maximum time duration (with maximum size) (T_{frame} [s]) and minimum interframe time (IFT) ($T_{interframe}$ [s]) consequently this case gives the most occupied channel *(Figure 10)*.

Frame time (T_{frame} [s]) consists of two parts: fixed duration for frame initialization (T_{frame_init} [s]) and the other part depending on frame size (S_{frame} [bit]) and bit rate of transmission (BR_{frame} [bit/s]):

$$T_{frame} = T_{frame\_init} + \frac{S_{frame}}{BR_{frame}} \quad [s] \; (8)$$

Channel utilization (U_{frame}) can be calculated with these parameters:

$$U_{frame} = \frac{T_{frame}}{T_{frame} + T_{int\,erframe}} \quad (9)$$

Scenario II: RLAN traffic with ACKs

Unlike the previous scenario, RLANs mostly use acknowledgements (ACKs) for reliable transmissions. After sending the data frame (T_{frame}) RLAN devices wait (T_{ACK_delay}) for the ACK (T_{ACK}). Similarly to the 'RLAN traffic without ACKs' model, this one simulates the worst case in deterministic way. The frame and ACK transmission periods can be grouped together (called 'Extended Frame'), supposing that the further channel allocation technique can not interrupt this frame-ACK communications *(Figure 11)*.

This grouping increases the channel utilization according to the worst case estimation. This allows a more simple way of modeling RLAN traffic with ACK, too.

Duration of frames and ACKs (T_{ACK} [s]) are calculated the same way as before:

$$T_{ACK} = T_{ACK\_init} + \frac{S_{ACK}}{BR_{ACK}} \quad [s] \; (10)$$

And the 'Extended Frame' time ($T_{extended\_frame}$ [s]) using 'ACK Delay Time' (T_{ACK_delay} [s]) as mentioned above:

$$T_{extended\_frame} = T_{frame} + T_{ACK\_delay} + T_{ACK} \quad (11)$$

Maximum usage of channel ($U_{extended\_frame}$) can be defined in this scenario, too.

$$U_{extended\_frame} = \frac{T_{extended\_frame}}{T_{extended\_frame} + T_{int\,erframe}} \quad (12)$$

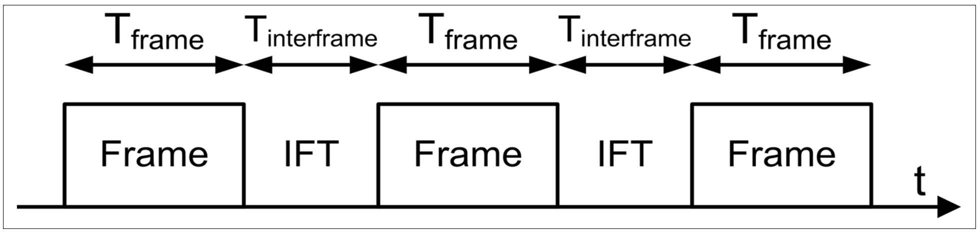


Figure 10.
Traffic scheme and timing for RLANs without ACKs

Frames with the same length (T_{frame}) and idle period (IFT) ($T_{interframe}$) alternates in our RLAN transmission model.

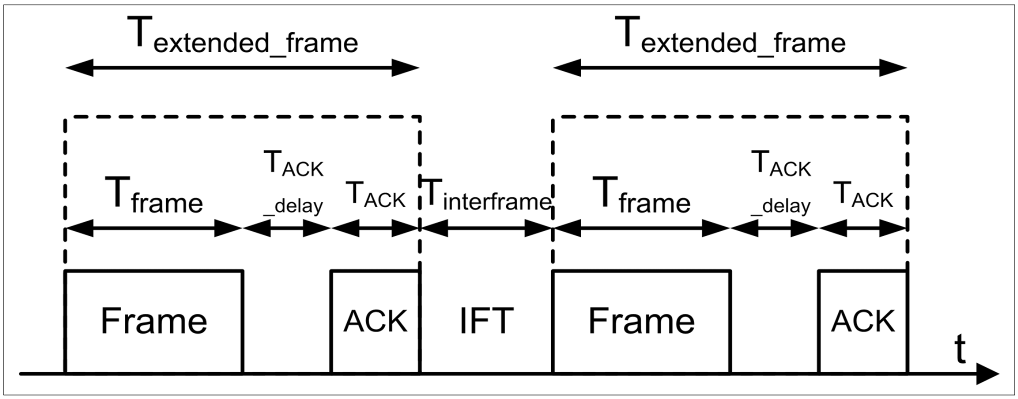


*Figure 11.
Traffic scheme and timing for RLAN with ACKs*

In acknowledged RLAN transmissions frames and acknowledgements (ACKs) and idle time between them (ACK delay) should be combined into 'Extended Frame'.

This is higher than U_{frame}, because 'Extended Frames' are larger than original frames but 'InterFrame Time' is equal.

4.2 Modeling channel allocation

The overview of the channel allocation technique was given in Subsection 3.1. To achieve our goal (minimizing the traffic of the RLANs during radar scan) we use Channel Allocation Frames (CAFs) (e.g. CTS) in general. RLAN traffic can be blocked for a specific duration by each CAF. But this event occurs only in the case when an RLAN device receives a CAF successfully. CAF can be successful if and only if the beginning of the CAF is in an interframe time (IFT) of the RLAN traffic. However, detecting IFT on the radar side and using detection-based adaptive transmission of CAFs can be difficult and it is unnecessary. When the radar receives signals of more than one RLAN simultaneously, it can detect fewer and shorter idle periods, due to overlapping RLAN traffics. However, CAFs can be transmitted successfully not only in these periods, because each RLAN has its own IFTs, when the allocation can occur. It can be difficult to separate traffic of RLANs, and derive when and which one has its IFT.

We decided that our proposed solution uses a simple deterministic RLAN-traffic-independent CAF transmission without using any detection and without a complex adaptive mechanism, according to the difficulty above. The rate of successful allocation can be maximized by the maximum rate of CAF frequency. This results in a deterministic structure of channel allocation transmission with using short CAFs (T_{CAF} [s]) and as short as possible idle time ('InterCAF Time') (T_{ICAF} [s]) between them *(Figure 12)*. Duration of CAF can be calculated the same way as duration of data frames with the parameters: fixed time for initialization (T_{CAF_init} [s]), size of CAF (S_{CAF} [bit]) and transmission bit rate (BR_{CAF} [bit/s]):

$$T_{CAF} = T_{CAF\_init} + \frac{S_{CAF}}{BR_{CAF}} \qquad \text{[s] (13)}$$

This channel allocation operation is used only in InterMeasurement Gaps of radar, as discussed in Subsection 3.3.

4.3 Analysis of proposed solution

As mentioned above, CAF can block RLAN traffic, when an RLAN device detects it. It can occur when the whole CAF is received from its beginning without overlapping with RLAN frames. RLANs using CSMA (Carrier Sense Multiple Access) do not transmit frames after beginning of any frame including CAF is detected. Therefore this successful reception of a CAF becomes a successful channel allocation, too. Applying RLAN traffic and channel allocation models described in Subsection 4.1 and 4.2, the number of successful CAFs during an interframe time (IFT), N_{CAF_IFT} can be estimated:

$$N_{CAF\_IFT} = \frac{T_{\text{int erframe}}}{T_{CAF} + T_{ICAF}} \qquad (14)$$

In this case we supposed that CAFs and RLAN frames are not synchronized, and one's periodicity is not exactly a multiple of other's in our deterministic model. This condition guarantees the variety of relative positions of CAFs and RLAN frames.

We supposed that CAF traffic does not affect RLAN traffic, only when successfully receiving a CAF. If this

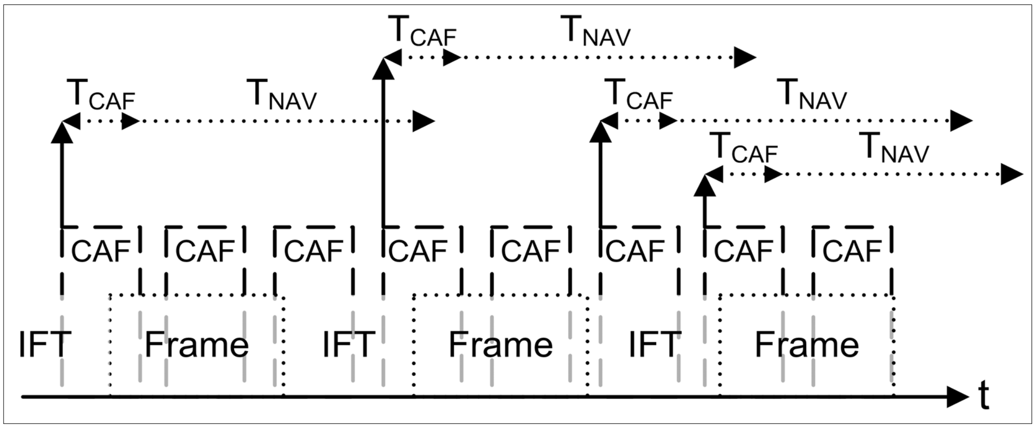


*Figure 12.
Scheme and timing for channel allocation frames (CAFs) and RLAN traffic*

Channel Allocation Frames (CAFs) are sent periodically and in parallel with RLAN traffic. CAFs can be detected by RLAN devices in their idle time (InterFrame Time). Receiving CAFs successfully mute RLAN devices for a time specified by CAF.

assumption is incorrect, then CAFs can cause longer idle periods and RLAN frame retransmissions (due to frame-CAF collision) in RLAN traffic, too. However, in this case utilization of the RLAN channel can not exceed the worst case limit, as described in *Scenario I* and *II.*

The interframe frequency (number of IFT in one second) (F_{IFT} [1/s]) can be calculated as

$$F_{IFT} = \frac{1}{T_{frame} + T_{interframe}} \qquad [1/s] \quad (15)$$

T_{frame} can be replaced with $T_{extended\_frame}$ as necessary.

Using both values (N_{CAF_IFT} and F_{IFT}), the average frequency of successful CAFs in IFT (F_{CAF_IFT} [1/s]) can be estimated, too:

$$\begin{aligned} F_{CAF\_IFT} &= N_{CAF\_IFT} \cdot F_{IFT} = \\ &= \frac{T_{interframe}}{T_{CAF} + T_{ICAF}} \cdot \frac{1}{T_{frame} + T_{interframe}} = \\ &= \frac{1}{T_{CAF} + T_{ICAF}} \cdot \frac{T_{interframe}}{T_{frame} + T_{interframe}} = \frac{1 - U_{frame}}{T_{CAF} + T_{ICAF}} \end{aligned} \qquad (16)$$

This result demonstrates our previous two worst case assumptions: efficiency can be increased by minimizing both RLAN traffic utilization and CAF cycle duration. This formula (16) can be used not only in the case of deterministic, but also in the case of random RLAN traffic, only the utilization of the channel should be known.

The above result is modified by usable time slot, so the more relevant value is the frequency of successful CAFs in IFTs in 'InterMeasurement Gaps' (IMG) ($F_{CAF\_IFT\_IMG}$ [1/s]):

$$\begin{aligned} F_{CAF\_IFT\_IMG} &= F_{CAF\_IFT} \cdot \frac{T_{IMG}}{T_{PR}} = \\ &= F_{CAF\_IFT} \cdot (1 - U_{measure}) = \\ &= \frac{(1 - U_{frame}) \cdot (1 - U_{measure})}{T_{CAF} + T_{ICAF}} \end{aligned} \qquad [1/s] \quad (17)$$

Accordingly, the average number of successful channel allocations during each IMG is:

$$N_{CAF\_IFT\_IMG} = F_{CAF\_IFT} \cdot T_{IMG} = \frac{(1 - U_{frame}) \cdot T_{IMG}}{T_{CAF} + T_{ICAF}} \qquad (18)$$

Another useful measure can be the number of successful channel allocations during a radar scan (T_{cont}) ($N_{CAF\_IFT\_IMG\_Tcont}$):

$$\begin{aligned} N_{CAF\_IFT\_IMG\_Tcont} &= F_{CAF\_IFT\_IMG} \cdot T_{cont} = \\ &= \frac{(1 - U_{frame}) \cdot (1 - U_{measure})}{T_{CAF} + T_{ICAF}} \cdot \frac{\alpha}{\beta} \end{aligned} \qquad (19)$$

Each successful channel allocation protects the radar from RLAN traffic for duration (T_{CAF_NAV}), that is the sum of the time value (NAV – Network Allocation Vector) contained in CAF (T_{NAV}) and the time of CAF itself (T_{CAF}), see Figure 12:

$$T_{CAF\_NAV} = T_{CAF} + T_{NAV} \qquad [s] \quad (20)$$

With this value the minimum number of successful channel allocations in each scan period (T_{cont}) ($N_{CA\_Tcont\_min}$) can be estimated:

$$N_{CA\_Tcont\_min} = \left\lceil \frac{T_{cont}}{T_{CAF\_NAV}} \right\rceil = \left\lceil \frac{1}{T_{CAF} + T_{NAV}} \cdot \frac{\alpha}{\beta} \right\rceil \qquad (21)$$

One of the most important values that can describe the efficiency of the proposed solution (ρ) is the ratio of occurred effective channel allocations ($N_{CAF\_IFT\_IMG\_Tcont}$) and the number of needed ($N_{CA\_Tcont\_min}$).

$$\begin{aligned} \rho &= \frac{N_{CAF\_IFT\_IMG\_Tcont}}{N_{CA\_Tcont\_min}} = \frac{F_{CAF\_IFT\_IMG} \cdot T_{cont}}{\left\lceil \frac{T_{cont}}{T_{CAF\_NAV}} \right\rceil} = \\ &= \frac{\frac{(1 - U_{frame}) \cdot (1 - U_{measure})}{T_{CAF} + T_{ICAF}} \cdot \frac{\alpha}{\beta}}{\left\lceil \frac{1}{T_{CAF} + T_{NAV}} \cdot \frac{\alpha}{\beta} \right\rceil} \approx \\ &\approx \frac{T_{CAF} + T_{NAV}}{T_{CAF} + T_{ICAF}} \cdot (1 - U_{frame}) \cdot (1 - U_{measure}) \end{aligned} \qquad (22)$$

The approximation can be applied in case of $T_{cont} >> T_{CAF\_NAV}$. This formula clearly shows which parameters can affect the efficiency of channel allocation dominantly. This efficiency (ρ) can reach or exceed 1, if

$$\begin{aligned} & 1 < \frac{T_{CAF} + T_{NAV}}{T_{CAF} + T_{ICAF}} \Leftrightarrow \\ & \Leftrightarrow T_{CAF} + T_{NAV} > T_{CAF} + T_{ICAF} \Leftrightarrow \\ & \Leftrightarrow T_{NAV} > T_{ICAF} \end{aligned} \qquad (23)$$

Table 1. Practical parameters and constants

Parameter	Value	Comment
RPM	2	From radars specification (0-6)
β	12°/s	From radars specification (0-36°/s)
α	1°	Average radar beam width (3 dB)
PRF	400 1/s	Generally used from radar specification (250-1300)
R	240 km	Radar range: 0-240 km
c	$3 \cdot 10^8$ m/s	Speed of light
$T_{frame\ init}$	20 μs	IEEE 802.11a: preamble (16 μs) + PLCP (4 μs)
S_{frame}	1516 bytes	Supposing Ethernet traffic (64-1516 bytes – see below)
BR_{frame}	6 Mbps	IEEE 802.11a: 6-54 Mbps
$T_{interframe}$	34 μs	IEEE 802.11a: DIFS + backoff (with 1 time slot (worst case))
$T_{ACK\ init}$	20 μs	IEEE 802.11a: preamble (16 μs) + PLCP (4 μs)
S_{ACK}	14 bytes	IEEE 802.11a
BR_{ACK}	6 Mbps	IEEE 802.11a: 6-54 Mbps
$T_{ACK\ delay}$	16 μs	IEEE 802.11a: SIFS
$T_{CAF\ init}$	20 μs	IEEE 802.11a: CTS preamble (16 μs) + PLCP (4 μs)
S_{CAF}	14 bytes	IEEE 802.11a: CTS
BR_{CAF}	6 Mbps	IEEE 802.11a: CTS: 6-54 Mbps 6 Mbps for worst case and for best receiving conditions
T_{ICAF}	16 μs	We can specify it freely, but for easier implementation and compatibility we set to SIFS.
T_{NAV}	32267 μs	IEEE 802.11: CTS 15 bit value: 0-32267 in μs

4.4 Evaluation in practice

In practice most of the parameters are defined in standards and specifications. In our solution the values of the RLAN traffic parameters come from IEEE 802.11, 802.11a (including RTS/CTS introduced in Subsection 3.2) [4] and weather radar parameters as defined its specifications and using general settings [3,14,18]. For practical evaluation of this allocation technique, the worst case or default values of parameters are given in *Table 1*.

Using these values in practice (Table 1) the parameters of our model can be calculated, see *Table 2*.

Parameter	Value	Parameter	Value
T_{PR}	2500 μs	U_{frame}	86.73 %
$T_{measure}$	1600 μs	$U_{extended\_frame}$	89.06 %
T_{IMG}	900 μs	F_{IFT}	3218 Hz
T_{cont}	83.33 ms	F_{CAF_IFT}	2001 Hz
$U_{measure}$	64 %	$F_{CAF\_IFT\_IMG}$	720 Hz
T_{frame}	222.1 μs	$N_{CAF\_IFT\_IMG}$	1.8
$T_{interframe}$	34 μs	T_{CAF_NAV}	32.3 ms
$T_{ACK}= T_{CAF}$	38.67 μs	$N_{CA\_Tcont\_min}$	3
$T_{extended\_frame}$	332.8 μs	ρ	20.01

Table 2. Calculated parameters

The results of worst case calculations and estimations can be seen in Table 2. We find that since the radar is in idle state in 36% of its time, there is a 900 μs IMG for channel allocation. During an IMG, 1.8 successful channel allocations occur in average, but only 3 are needed during a 83.33 ms 'Contacted Time'. With these worst case parameters the proposed solution allocates channels at least 20 times more often than needed.

These results can be much better if the estimation is based on real parameter values, not on the worst case. For example, using a real distribution of frame sizes gives some improvement. Supposing that the frame size distribution is similar to as it was in 2000 in world wide networks, estimation can be much better. Based on an earlier publication [20], similarly to [19] and [21], the cumulative density function (CDF) of the IP packet size can be obtained. From this CDF the smoothed probability density function (PDF) (or histogram) can be derived, as shown in *Figure 13*.

We suppose these traffic characteristics describe not only Ethernet and backbone traffic, but they are valid for WLAN environment, too. This assumption can be used, because much of traffic is IP and passed through in Ethernet network, which shapes the traffic characteristic to a similar one.

We can find three modes in the histogram of packet size distribution (see Fig. 13). Only 14% of the traffic has the maximal size, 19% is around 570 bytes and almost 33% has the minimal size with 40 bytes. Due to the payload encapsulation and framing every packet gets 16-20 bytes additional overhead. Using these statistics and information, the average frame size can be around 500 bytes. In this case, the efficiency (ρ) of the solution exceeds 35, which means that CAF occur in the average 35 times more often than needed.

We can also analyze the relationship between the efficiency and RLAN bit rate, frame size and using ACKs. This comparison is shown in *Figure 15*.

The *Figure 14* shows that 20 is the lowest efficiency, but under some conditions even 115 can be reached.

4.5 Applicability

We can see that the solution is more efficient than needed under every circumstance. It can protect meteorological radars against

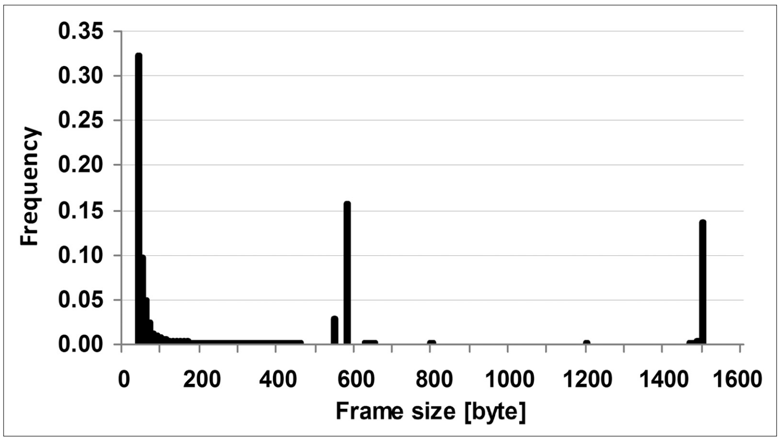


Figure 13.
Frequency of Frame Size

Smoothed probability density function (PDF) (histogram) of frame size in bytes in typical networks (based on [20])

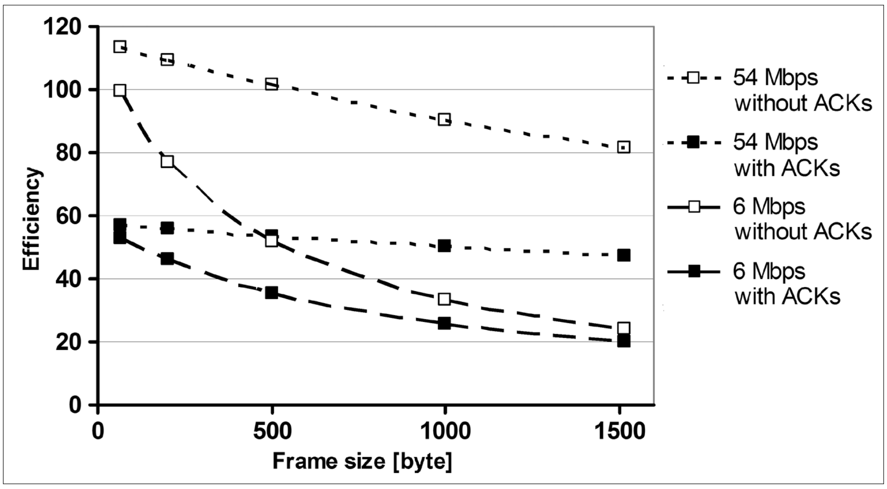


Figure 14.
The efficiency of proposed channel allocation technique

This diagram shows the efficiency connected to RLAN traffic at different frame size at 6 and 54 Mbps with or without ACKs.

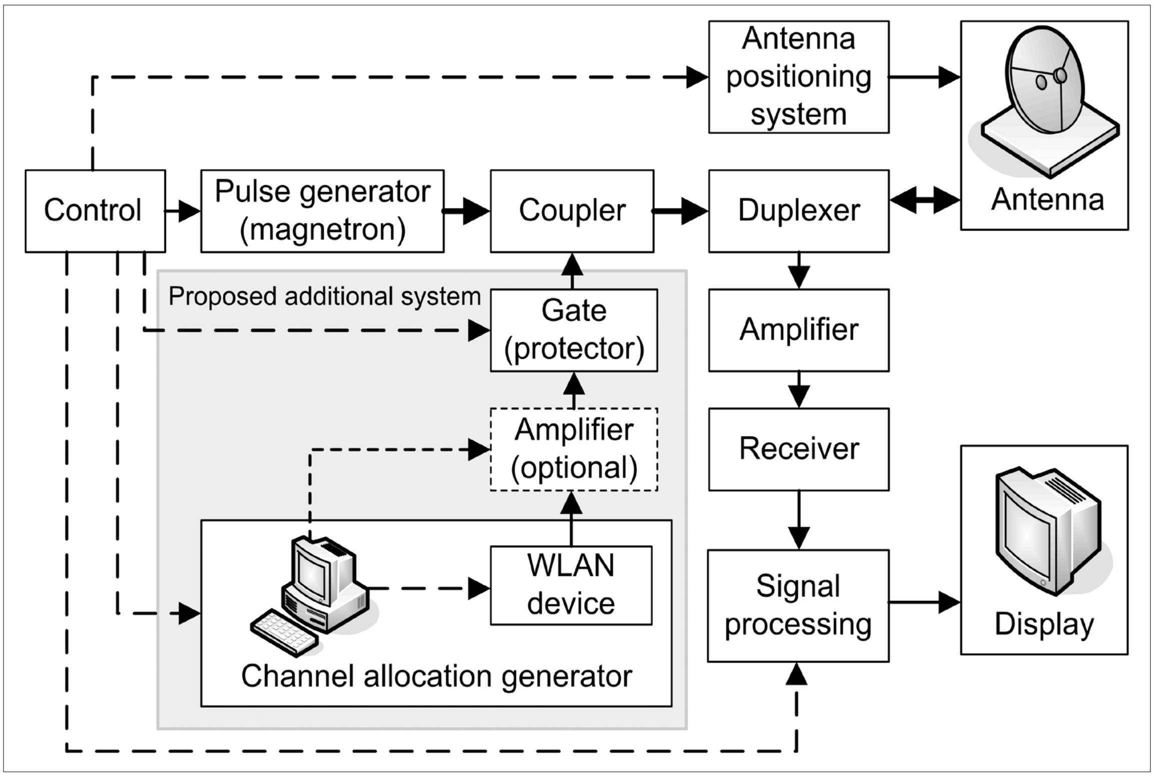


Figure 15. Radar block diagram with the proposed solution

RLAN interference using simple RTS/CTS mechanism. Thus, the implementation of this technique is not too difficult. A simple computer can send CTS frames continuously through a WLAN adapter, synchronized to radar measurement cycle. For higher efficiency we can apply an optional power amplifier. The signal can be transmitted directly into the waveguide of the radar through a coupler, which exits in most of the radars for testing and calibrating purposes. We can also use a controlled gate before the coupler to protect the amplifier against the high power radar pulses (see Fig. 15).

The proposed technique can be used as a standard-compliant solution, because it uses an ordinary WLAN device and a frame type that is specified in the standards. This can not conflict with the radar; moreover it allows undisturbed radar operation.

5. Conclusions

In this paper we have addressed the problem of interference between meteorological radars and RLAN devices. We have evaluated the current solution – DFS – and its limitation. We have proposed some new solutions, and detailed the most viable one: channel allocation based on RTS/CTS. We have given models for radar operations and RLAN traffic. We have shown that using the proposed technique the interference can be eliminated in a very efficient way, due to the mandatory and embedded functionality of RTS/CTS and parameters from standards.

We will try to test this solution in practice soon. We expect this method to be implemented all over the world and will solve the problem of 5 GHz interference.

Acknowledgement

This work has been supported by
Hungarian National Communications Authority (NHH),
Hungarian Meteorological Service (OMSZ)
and High-Speed Networks Laboratory,
Budapest University of Technology and Economics.

Authors

ZOLTÁN HORVÁTH received his M.Sc. degree in Computer Science in 2006 from the Budapest University of Technology and Economics (BME), where he currently pursues his Ph.D. studies at the Department of Telecommunications and gives Computer Networks courses. He has participated in many R&D projects related to planning, testing and building local and metropolitan area networks including WiMAX and community network technologies. He also worked as an advisor for the Hungarian National Communications Authority in applying ETSI regulations, testing devices, EMC measurements and interference examination cooperating with the Hungarian Meteorological Service. He is member of IEEE and Secretary for Project Management Division in Scientific Association for Infocommunications (Hungary).

DÁVID VARGA received his M.Sc degree in Electrical Engineering at Budapest University of Technology and Economics (BME) in 2007. Formerly he took part in building a WiMAX network for testing purposes. He developed a protocol enhancement to the 802.11 WLANs that enables direct communication between wireless stations in infrastructure mode. He worked as an advisor for the Hungarian National Communications Authority cooperating with the Hungarian Meteorological Service in applying ETSI regulations, device testing, EMC measurements and interference examination. Currently he is working on a WLAN based indoor positioning system.

References

[1] Horváth, Z., Lukovszki, Cs., Varga, D., Micskei, T., "Interference on Meteorological Radar and Wi-Fi in 5 GHz band" (in Hungarian), Híradástechnika, Vol. LXIV., No. 5., July 2009.

[2] Horváth, Z., Micskei, T., Varga, D., Lukovszki, Cs., "Interference on Meteorological Radar and WiFi in 5 GHz band", http://www.hit.bme.hu/~hotvathz/publication/radar_wifi_interference_summary_2008.pdf

[3] Horváth, Z., Micskei, T., Seller, R., Varga D., Lukovszki, Cs., "Analyzing WiFi DFS efficiency and opportunities stopping radar interference" (in Hungarian), Hungarian National Communications Authority (NHH), December 2007.

[4] "IEEE Std 802.11-2007, (Revision of IEEE Std 802.11-1999), Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", 2007.

[5] "ETSI EN 301 893 V1.2.3: Broadband Radio Access Networks (BRAN); 5 GHz high performance RLAN; Harmonized EN covering essential requirements of article 3.2 of the R&TTE Directive".

[6] "ETSI EN 301 893 V1.3.1: Broadband Radio Access Networks (BRAN); 5 GHz high performance RLAN; Harmonized EN covering essential requirements of article 3.2 of the R&TTE Directive".

[7] "ETSI EN 301 893 V1.4.1: Broadband Radio Access Networks (BRAN); 5 GHz high performance RLAN; Harmonized EN covering essential requirements of article 3.2 of the R&TTE Directive".

[8] "ETSI EN 301 893 V1.5.1: Broadband Radio Access Networks (BRAN); 5 GHz high performance RLAN; Harmonized EN covering essential requirements of article 3.2 of the R&TTE Directive".

[9] ITU-R Radio Communication Study Groups, "Studies on the effect of wireless access systems including RLANs on terrestrial meteorological radars operating in the band 5600-5650 MHz (documents 8A/103?E and 8B/65?E)", International Telecommunication Union (ITU), Geneva, Switzerland, 30 August 2004.

[10] Brandao, A. L., Sydor, J., Brett, W., Scott, J., Joe, P., Hung, D., "5 GHz RLAN interference on active meteorological radars", Vehicular Technology Conference (VTC'05), 30 May–1 June 2005, Vol.2, pp.1328–1332.

[11] European Telecommunications Standards Institute, "DFS Update: European Weather Radars – Details & Overview", BRAN#52, Sophia-Antipolis, 8-11 October 2007. http://www.ieee802.org/18/Meeting_documents/2007_Sept/BRAN52d014_European_Weather_Radar_SIgnals_-_Details__Overview.pdf

[12] Wi-Fi Alliance, Spectrum & Regulatory Committee, "Spectrum Sharing in the 5 GHz Band – DFS Best Practices", 10 October 2007. http://www.ieee802.org/18/Meeting_documents/2007_Nov/WFA-DFS-Best%20Practices.pdf

[13] ITU – Radiocommunication Study Groups, "Theoretical analysis and testing results pertaining to the determination of relevant interference protection criteria of ground-based meteorological radars", Draft new REPORT ITU-R M.2136, Working Party 5B, 3 December 2008.

[14] ITU – Radiocommunication Study Groups, "Technical and operational aspects of ground-based meteorological radars", Draft new RECOMMENDATION ITU-R M.[MET-RAD], Working Party 5B, 3 November 2008.

[15] EUMETNET, "Recommendation on C-Band Meteorological radars design to ensure global and long-term coexistence with 5 GHz RLAN", 35th EUMETNET Council, Reading, UK, 4 December 2008.

[16] Collier, C.G., "Applications of Weather Radar Systems: A guide to uses of radar data in meteorology and hydrology", John Wiley and Sons, New York, 1989.

[17] Hungarian National Communications Authority (NHH), "Broadband Data Transmission with Wireless Access Devices", 2nd Ed., Budapest, 1 October 2006. http://www.nhh.hu/dokumentum.php?cid=11887

[18] Hungarian Meteorological Service (OMSZ), Weather Radar Images, Budapest, 2007-2009, http://www.met.hu

[19] Claffy, K.C., Miller, G., Thompson, K., "The Nature of the Beast: Recent Traffic Measurements from an Internet Backbone", The 8th Annual Conference of the Internet Society (INET'98), Geneva, Switzerland, 1-24 July 1998. http://www.pdos.lcs.mit.edu/decouto/papers/claffy98.pdf

[20] McCreary, Sean and Claffy, K.C., "Trends in Wide Area IP Traffic Patterns: A View from Ames Internet Exchange", Cooperative Association for Internet Data Analysis (CAIDA), San Diego Supercomputer Center, University of California, San Diego, ITC Specialist Seminar, 2000. http://www.caida.org/publications/papers/2000/AIX0005/AIX0005.pdf

[21] Fraleigh, C., Moon, S., Lyles, B., Cotton, C., Khan, M., Moll, D., Rockell, R., Seely, T., Diot, S.C., "Packet-level traffic measurements from the Sprint IP backbone", IEEE Network, Vol.17, No.6, Nov-Dec. 2003, pp.6–16.