|  |  |
| --- | --- |
| **Radiocommunication Study Groups** |  |
|  |  |
|  |  |
| Source: Document 5A/TEMP/262 | **Annex 9 toDocument 5A/636-E** |
| **10 November 2014** |
| **English only** |
| Annex 9 to Working Party 5A Chairman’s Report |
| compilation of technical information on TECHNIQUES that could be used in RLAN deployments to facilitate sharing |
|  |

This document contains technical information describing various techniques that could be applied when developing and deploying RLAN systems, in particular in the frequency bands in the 5 GHz frequency range. The document focusses on the feasibility of implementing these techniques in RLANs/RLAN deployments as this is the area of expertise of WP 5A. It does not address the effectiveness of these techniques as mitigation techniques with respect to EESS(active) and radar systems for the ongoing sharing studies within JTG 4-5-6-7, as such a discussion needs to be held in JTG 4-5-6-7 itself with experts from all involved systems present. If WP 5A would, at a later stage, start work on assessing these techniques as mitigation techniques to facilitate sharing with EESS (active) and radiodetermination, this would have to be done in cooperation with WP 7C and WP 5B respectively.

**Attachments:** Attachment 1: Use of all techniques in combination

 Attachment 2: Changes to DFS including Lower Detection Threshold

 Attachment 3: Collaborative Detection

 Attachment 4: Alternate Channelization

 Attachment 5: Reduce Transmit Power

 Attachment 6: Exclusion Zones in conjunction with Geo-location databases

 Attachment 7: Geo-location database

 Attachment 8: Dedicated sensors

Attachment 1

Use of all techniques in combination

The incumbent services which operate in the 5 GHz range have different characteristics which may result in the need for different mitigation techniques. Although one particular technique may not necessarily address all incumbent systems, several techniques could be used in conjunction to mitigate interference.

On the other hand, the consistency between the specific requirements/operational conditions of various techniques used in conjunction has to be verified. In addition, the feasibility of their implementation by RLAN devices will also need to be addressed, as appropriate.

These RLAN mitigation techniques can be viewed as a collection of “tools in a toolbox” to enable flexibility for regulators to adopt appropriate mitigation techniques to facilitate sharing between RLAN and incumbent systems.

An advantage of lowering the e.i.r.p./PSD is that devices with lower transmit powers could potentially avoid the need for other mitigation techniques.

Comments:

– Use of mixed models (some systems operating at higher power and/or geolocation database, while others utilize lower power and/or antenna/e.i.r.p. elevation angle mask) needs to be studied to determine if such mixed use can be allowed without harmful interference into incumbent services.

– Mixed model use may require changes to DFS threshold, e.i.r.p. power, antenna/e.i.r.p. elevation angle mask, etc.

– Further, the reported access point (AP) location should be accurate [to within 3 meters and be demonstrated to validate the AP location every ten seconds] to address indoor/outdoor sharing issues.

Attachment 2

Changes to DFS including lower detection threshold

## Technical description

Dynamic Frequency Selection (DFS) is a well-established mitigation technique that has been implemented in RLAN networks to protect radar systems. In this mitigation technique, RLANs check for radar operation on a channel before and during use by RLANs. If a radar is detected, RLAN operations quickly move to a different channel. Only devices capable of detecting radars are permitted to initiate RLAN networks on a DFS channel: these master devices (e.g. Access Points) then control which channels the clients operate on.

## Key points regarding mitigation technique

Recommendation ITU-R M.1652, developed in 2003, “provides the requirements of dynamic frequency selection (DFS) as a mitigation technique to be implemented in wireless access systems (WAS) including radio local area networks (RLANs) for the purpose of facilitating sharing with the radiodetermination service in the 5 GHz band.”

*Key Steps in implementing this technique, shown schematically in Figure 1 below:*

1) Channel availability check (CAC): Prior to starting operation on a channel, a master RLAN device checks for radar operation on the channel. The master RLAN device starts operation of a network on that channel only if there is no activity by a primary system.

2) In-service Monitoring (ISM): Once a RLAN starts operation on an available channel, master RLAN equipment continue to monitor the RLAN operating channel for radar waveforms in case a radar system turns on after the RLAN operation in the channel has started. This continuous monitoring mode is known as in-service monitoring (ISM).

3) Channel Move Time: Once a radar signal above the detection threshold is detected on the operating channel, the master RLAN equipment broadcasts commands to cease all transmission on the channel. The broadcast is repeated a number of times to assure reception by all member devices. RLAN operation is then moved to a different available channel (identified via a channel availability check).

4) Non-occupancy period: Once a radar is detected on the operating channel and RLAN operation moves to another channel, the RLAN is unable to resume operations on the original operating channel for the non-occupancy period.

Detailed information regarding the DFS process is available in Recommendation ITU-R M.1652 Annex 2 “Radar detection and example of associated DFS procedures”.

Figure 1

DFS Process Overview



Annex 1 of Recommendation ITU-R M.1652 specifies the detection, operational and response requirements for DFS. A summary of these parameters is available in Table 1 below.

TABLE 1

|  |  |
| --- | --- |
| Parameter | Value |
| DFS detection threshold | –62 dBm for devices with a maximum e.i.r.p. of < 200 mW and–64 dBm for devices with a maximum e.i.r.p. of 200 mW to 1 W averaged over 1 μs |
| Channel availability check time | 60 s |
| Non-occupancy period | 30 min |
| Channel move time | ≤ 10 s |

Recommendation ITU-R M.1652 also provides the following guidance regarding channel move time:

Channel move time is defined as the period of 10 s needed by a WAS to cease all transmissions on the operating channel upon detection of an interfering signal above the DFS detection threshold. Transmissions during this period will consist of normal traffic for typically less than 100 ms and a maximum of 200 ms after detection of the radar signal. In addition, intermittent management and control signals can be sent during the remaining time to facilitate vacating the operating channel. The aggregate time of the intermittent management and control signals are typically less than 20 ms.

“Master” devices

Master RLAN devices (e.g. Access Points) are the only devices which can initiate an RLAN network on DFS channels. All other RLAN devices cannot transmit without receiving an enabling signal from a Master device. Therefore, mitigation technique capabilities do not need to be implemented in each RLAN device worldwide. For example, the radar detection capability in DFS is done by “Master” RLAN devices, which then provides instructions (e.g. permission to transmit, clear channel immediately, etc.) to all associated client devices. If a client device loses connection to the “Master” (e.g. access point), it may not use active scanning to associate itself again to this or to another access point.

The minimum and maximum radar pulse widths are not specified in ITU-R M.1652. The current minimum pulse widths tested are 1us for US and 0.5 us for ETSI. The maximum pulse widths are 100 us for chirping and 20 us for normal pulses.

## Proposed changes to current DFS

The following possible changes to DFS as currently specified could help protect new radars.

1) Detection of lower pulse widths. For example, some radars operating in the 5 GHz range have pulse widths as small as 100 ns.

2) Detection of a new set of pulse repetition frequencies as well as possibly different burst structure and staggering pattern. Some radars have rapidly changing inter-pulse periods with different pulse width and different number of pulses per transmitted burst. As such, changes to the test waveforms would need to be done.

3) Lower DFS detection threshold to assist with protection for radars with lower output power.

4) Detection of new frequency-hopping radars that might have different characteristics.

5) Changes to channel move and channel closing time.

6) Clients would have to go silent in this band if they don’t hear from the master devices for a predefined time (e.g. 500 ms).

7) Modification to Annex 4 of Recommendation ITU-R M.1652 (e.g. jitter the start time of the first radar pulse).

## Potential impact

For some ground tracking radars where the interference occurs only during the first few samples, improving the response time of RLANs to radar waveform detection events by decreasing the channel closing time and channel move time would help reduce the interference.

Protection of new airborne radars can be challenging due to lower output power which can make the detection difficult. However, lowering the DFS detection threshold could assist in protection for these airborne radars.

DFS could also be used to protect EESS systems as these systems have similar waveform features to the radar systems. DFS, at lower detection thresholds levels (change 3 above), reduced channel move and channel closing times (change 5 above), and clients going silent (change 6 above), could be capable of detecting and reducing interference to EESS systems.

## Feasibility of implementing from RLAN perspective

DFS has been utilized to protect some scanning, chirping, and frequency hopping radars. The original DFS parameters were established in 2003 and has been implemented in equipment for years. Due to improvements in technology as well as expertise gained through the implementation of DFS, modifying DFS may be feasible. However, the extent to which these DFS parameters would need to be modified to protect incumbent services is not currently known. In addition, it is not known whether it would be feasible to implement the modifications needed to protect incumbent services.

Industry is currently investigating what detection parameters (including threshold, channel moving time, lower pulse width, number of pulses, probability of detection, …) would be possible with reasonable costs and practical false alarm rate (ref. Report ITU-R M.2034).

## Comments

## For terrestrial radars

Improvements to DFS specifications and the feasibility of DFS for incumbent radar systems have not been demonstrated. The following considerations and issues are still pending:

– Consideration of meteorological radars.

– Consideration of frequency hopping (FH) radars.

– Consideration of bi-static radars, in particular since the transmitter and receiver are in different locations.

– Consideration and analysis of suitable test signals (example test signals attached in Appendix 1 for FH radars and Annex 3 of Report ITU-R M.2115 for meteorological radars).

– How much could the DFS parameters be modified to ensure both an appropriate protection to terrestrial radars and to minimize the false radar detections for the RLAN network?

– Furthermore, studies are required to determine if RLAN can implement detection of smaller pulse width radar systems down to 0.1 microseconds.

– APs needs to take into account and demonstrate they can properly detect current radar pulses that are less than one microsecond, wide-band, continuous-wave, and frequency hopping systems.

– DFS design should be flexible enough to detect future radar pulses that are less than one microsecond, wide-band, continuous-wave, and frequency hopping systems.

## For EESS

The following list contains additional comments, concerns, and questions that need additional study and investigation regarding implementation of DFS:

– [WP 7C has stated (see Doc. [5A/526](http://www.itu.int/md/R12-WP5A-C-0526/en)) that the DFS as a concept cannot work for mitigating the RLAN interference to EESS (active) in general and SAR in particular, irrespective of its capability to detect lower signal levels. The problem is linked to the fact that a channel switch driven by DFS would only happen after the RLAN device has been illuminated by the SAR signal and therefore too late to avoid having the RLAN signal interfering with the SAR reflected signal. At that moment the SAR will be already illuminating a different area on Earth (noting the orbital speed of around
7 km/s).]

– One study (Doc. [4-5-6-7/479](http://www.itu.int/md/R12-JTG4567-C-0479/en)) indicated that the threshold of DFS should be reduced to about –100 dBm within the RLAN channel, i.e. well below the noise floor
(e.g. – 86 dBm for a 160 MHz channel). If this level is required, DFS would have to have a significantly large dynamic range, and would increase the cost of DFS implementation in RLAN devices. In addition, at such a low threshold level, DFS would react to any out of band emissions produced by other electrical apparatus and/or by background noise.

appendix 1 (to Attachment 2)

Example of test signals to protect frequency hopping radars

[Radars that operate in the 5 GHz band can hop across the 5 250-5 850 MHz band. The frequencies will be selected by using a random without replacement algorithm until all frequencies have been used. After the use of all frequencies, the pattern is reset and a new random is generated.

The proposed test signals in the table below are presented to improve DFS specifications

Frequency Hopping DFS test signals

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Frequency hopping radar type**(Note7) | **Pulse Width (µsec)** | **Pulse Repetition Interval (pri) (µsec)** | **# Number of pulses per frequency hop** | **Burst length (ms)**(Note 8) | **Trial length (ms)** | **Pulse modulation**(Note 9) | **Minimum detection probability with 30% channel load**(Note 10) |
| 1 | 1 | 200 (=5 kHz) | 4 | 0.8 | 480 | none | Pd>80% |
| 1 | 20 | 333 (=3 kHz) | 3 | 1 | 600 | none | Pd>80% |
| 1 | 30 | 500 (=2 kHz) | 2 | 1 | 600 | none | Pd>80% |
| 2 | 3 | 333 (=3 kHz) | 1 to 9 | # | 120 | chirp | Pd>80% |
| 2 | 10 | 500 (=2 kHz) | 1 to 9 | # | 120 | chirp | Pd>80% |
| 2 | 15 | 1000 (=1 kHz) | 1 to 9 | # | 120 | chirp | Pd>80% |
| Note 7: Radar Type 1 : Up to 600 possible frequencies (step 1 MHz) within the range 5250-5850 MHz,  Radar Type 2: Up to 120 possible frequencies (step 5 MHz) within the range 5250-5850 MHz (Note 11), A frequency is selected randomly from a group of 600 (or 120 for radar Type 2) integer frequencies ranging from 5 250-5 850 MHz, using a ‘use without re-use’ scheme. Frequency test signal changes after each burst.Note 8: A burst is randomly composed of 1 to 9 pulses (n), then burst length (or hop length) = n x pri.Note 9 : Modulation used is defined in Note 2, Table D.4 (in reference of ETSI EN301893)Note 10: The proposal includes that a minimum of 30 trials per set be run with a minimum probability of detection calculated by  . For ChS=10 MHz, Pd>70%; for ChS = 2 0MHz, Pd>80%.Note 11: Although these frequency hopping radar test signals hop over the entire range from 5 250-5 850 MHz, detection of these signals is only required when operating within the 5 350-5 470 MHz and the 5 725 to 5 850 MHz |

]

Attachment 3

Collaborative detection

## Technical description

In Collaborative Detection, the Access Points in the metropolitan area collaborate to detect and avoid the radar. The Access Points detect radar with standard Dynamic Frequency Selection (DFS) techniques and share this information via a database manager, which would then notify other Access Points in the metropolitan area. The other Access Points in the metropolitan area would terminate operation or change channels upon being informed of a radar event.

## Key points regarding mitigation technique

As illustrated in *Figure 2* and *Figure 3* below, the collaborative mitigation technique only relies upon DFS detection and distribution of the radar detection event via a database manager. No information regarding the location of the radar is required a priori in the database.

*Key Steps in implementing this technique*

1) All RLANs with DFS master capability (e.g. Access Points) perform radar detection, as per DFS rules specified for the band.

2) When an Access Point detects a radar, it informs its associated client devices to either terminate operation or switch channels. This step also follows DFS rules specified for the band.

3) Upon radar detection, the Access Point also reports this event to the database manager.

4) The database manager collects reports of radar detection and determines when a valid radar event has occurred. A valid radar event is then reported to other Access Points in the metropolitan area.

5) Upon receipt of a radar event from the database manager, the Access Point informs its associated client devices to either terminate operation or switch channels.

*Bi-static radars/ Hidden node*

Bi-static radar receivers, in which the radar transmitter and radar receiver are spatially separated as illustrated below, operate in the 5 GHz frequency range.

Figure 1

Bi-static radar

baseline

Tx

Rx

reflected energy

RLANs could be located near the radar receiver and cause interference, but too far from the radar transmitter for the Dynamic Frequency Selection (DFS) to be activated in the RLAN. The distance between transmitter and receiver (baseline) is typically in the range of 30-50 km. Therefore, both the transmitter and the receiver would be located in a common general metropolitan area.

These steps are illustrated in the figure below to mitigate interference to bi-static radar. In this scenario, RLAN devices near the bi-static radar transmitter will detect and cease operation based on existing DFS rules. Information regarding the radar event is also reported to the database manager. With the database manager reporting the radar event to all the other APs , the RLAN devices potentially interfering with the bi-static radar receiver would be notified and would terminate operation or switch channels.

This approach would similarly address other types of “hidden node” problems.

Figure 2

Collaborative mitigation technique for bi-static radar



*Airborne radars*

In the case of airborne radar systems, the potential of interference from RLANs is due to low radar transmit power and sensitive radar receiver. With low radar transmit power, DFS detection is challenging, and fewer RLANs turn off. With collaborative mitigation as shown in Figure 3, the APs that detect the airborne radar report the detection to the database. The database manager propagates this information throughout the metropolitan area. So even in the situation in which fewer APs detect the airborne radar, the interference to the airborne radar could be reduced.

Figure 3

Collaborative mitigation technique for airborne radar



## Potential impact

This technique could be used to mitigate interference to airborne radar systems, bi-static radar, or other RLAN/radar “hidden node” deployment scenarios. In this proposed mitigation technique, the detection is dynamic so it will also address mobile radars.

## Feasibility of implementing from RLAN perspective

DFS is already implemented in RLAN devices. Geo-location databases and RLAN device access to such databases are addressed in separate contributions and are therefore not repeated in this contribution. Investigations are currently being undertaken to address the communication timescale necessary between the database and RLAN device and the implication on the relative cost for deployment.

## Comments

– Does not address EESS.

– Who is going to determine the size of the metropolitan area in which all equipments are to be switched-off? To cover all possibilities a very large number of RLANs may be unnecessarily turned off.

– See applicable comments for the geo-location database.

– If RLAN are not able to distinguish a signal from a bi-static or airborne radar from a signal from another radar type, this approach could quickly lead to the unavailability of the corresponding spectrum in a certain area.

– APs needs to be able to meet any requirements (e.g. DFS) to operate in the band.

– The interactions between the APs and database needs to be clearly articulated and dependencies between the sensing network and database fully explained, include a plan for when communication and/or sensing failure occurs between the, AP, and database as well as self-diagnostics to access proper functions.

– There is a need for all APs to determine their own location irrespective of indoor/outdoor conditions in order to ensure that the appropriate mitigation measures and limits are applied.

– Further, the reported AP location should be accurate [to within 3 meters and be demonstrated to validate the AP location every ten seconds].

Attachment 4

Alternate channelization

## Technical description

The alternate channelization scheme proposes to reduce the interference in two ways: (a) shift the 160 MHz channel to occupy only half of the 5350-5470 MHz band and (b) disallow 20 MHz/40 MHz devices that do not use any other mitigation technique from transmitting in this band.

## Key points regarding mitigation technique

It is important to note that this mitigation technique is proposed for only for RLAN devices which do not use other interference mitigation techniques. Devices which can reliably detect the presence of incumbents using other mitigation technique(s) can follow the baseline channelization scheme shown in Figure 1 below. For example, a 20 MHz device which can reliably detect the presence of incumbent services using other mitigation technique(s) can transmit in the band.

The baseline channelization scheme for IEEE 802.11 devices is shown below.

Figure 1

Baseline Channelization Scheme



Two points to note here are: (i) 20 MHz and 40 MHz devices, which have a higher power spectral density than the wider bandwidth devices, are present in the entire band. (ii) the band of operation for 160 MHz channel devices overlaps completely with 5 350-5 470 MHz.

*Alternate channelization Scheme A:*

An alternate channelization (scheme A) is shown below. When compared to the baseline channelization, the 20 MHz/40 MHz devices do not transmit and the 160 MHz devices overlap with only half of the band of interest.

Figure 2

Alternate Channelization Scheme A



*Alternate channelization Scheme B:*

Alternate Channelization Scheme B (shown below) incorporates the changes proposed in Scheme A plus 80 MHz devices would not transmit in one of the 2 channels. When compared to the baseline channelization, the 20 MHz/40 MHz devices do not transmit, the 80 MHz devices only transmit in one channel, and the 160 MHz devices overlap with only half of the band of interest.

Figure 3

Alternate Channelization Scheme B



## Reduced allocation of the 5 350-5470 MHz band to RLANs

Only the upper half of the 5 350-5 470 MHz bands would be utilized by the RLAN as depicted above. It should be noted that the figure above shows a combination with an additional mitigation to only the use of 80 MHz and 160 MHz channels which is an additional. This option with use of lower bandwidth channels could also be considered.

## Potential impact

The wider bandwidth channels facilitate higher data speeds for RLAN devices. In the alternate channelization schemes shown above, there are still three non-overlapping 160 MHz channels for use by RLAN devices.

When compared to the baseline channelization, the interference in the alternate channelization schemes may be lower because the 20 MHz/40 MHz devices would not transmit and the 160 MHz devices would overlap with only half of the 5 350-5 470 MHz band. The proposal for the reduced allocation shown above would lower the aggregate interference seen at the incumbent receiver compared to the baseline channelization scheme. An initial study on EESS protection (Document 5A/621) suggests that the possible gain range is **1.8 dB** to **4.9 dB**. Further investigations are required to determine the impact of the alternate channelization schemes or the reduced allocation to the incumbent services.

## Feasibility of implementing from RLAN perspective

Current RLAN devices have flexible channel and band selectivity to address the existing variation in available channels and bands in regulatory domains around the world. RLAN equipment can implement alternate channelization schemes today. The regulatory table in the IEEE 802.11 standard would have to be updated to include the new band with this channelisation scheme. However, no changes to the IEEE 802.11ac specification would be required to support these channelization schemes

## Comments

– Reducing the number of RLAN channels may increase the density of RLAN devices per channel as the expected deployment density of RLAN is a relatively fixed value. This would require new studies to determine impact to incumbent services, potential impact to DFS thresholds, and potential impact to required power levels.

– Is it expected that this technique will be implemented for RLAN devices only or also other mobile devices expected to operate under the proposed allocation?

– Any regulations of this technique will have to ensure that no smaller channels would be allowed.

– Studies conducted so far primarily used the baseline channelization scheme. The alternate channelization schemes shown above do not allow 20 MHz or 40 MHz RLAN operations in the 5 350-5 470 MHz band. It is unclear whether they would result in an increase of the number of wideband RLAN devices in the band 5 350 5 470 MHz. For example, it can be assumed that there will be added pressure in the remaining 5 GHz band to accommodate the displaced 20 MHz and 40 MHz operations, which could make it more challenging for wider channel RLAN operations to find clear channels outside of 5 350-5 470 MHz. This, in turn, could make the 5 350-5 470 MHz band a naturally favoured band for wideband (80 MHz and 160 MHz) operations given that the band is pre-cleared of narrow band (20 MHz and 40 MHz) operations, thereby increasing the number of expected wideband devices/operations in this portion of the 5 GHz band. It is unclear what the net effect would be with respect to the level of interference from RLAN devices into EESS (active) given these alternate channelization schemes.

Attachment 5

Reduce transmit power

## Technical description

A further technique to reduce the interference into incumbent services is to constrain the transmit power of the RLANs by either restricting the Effective Isotropic Radiated Power (e.i.r.p.) or by bounding the Power Spectral Density (PSD) more stringently.

## Key points regarding mitigation technique

There is a substantial difference in emissions between RLANs designed for higher-powered use and those designed for lower-powered use.

For example, Resolution **229 (Rev.WRC-12)** limits operation in the 5 150-5 250 MHz and 5 250‑5 350 MHz bands to a maximum mean e.i.r.p. of 200 mW and a maximum mean e.i.r.p. density of 10 mW/MHz in any 1 MHz band. This mitigation technique was utilized to help enable RLAN sharing with satellite, radar and EESS in those bands.

Lowering the e.i.r.p. only affects the operation of devices that have “high enough” power. Devices that already transmit with powers below the lower threshold are unaffected. For example, lowering the e.i.r.p. by 3 dB would not provide a full 3 dB reduction in interference.

## Device design

It is important to note that RLAN device design is driven by a complex set of factors. For example, battery life considerations trade off against higher-power devices. As a result, most smartphones, tablets and laptops incorporate RLANs at a maximum e.i.r.p. of 25 mW.

Furthermore, current RLAN devices are being designed with regulatory restrictions and constraints programmed directly into hardware such that it is not accessible and it cannot be changed by the end user. Such an approach would also ensure that the RLAN device operates at lower transmit power (or cease operation) if other mitigation techniques are not incorporated.

## Potential impact

Reducing the transmit power lowers the aggregate interference and could assist with mitigating interference.

An advantage of lowering the e.i.r.p. /PSD is that devices with lower transmit powers could potentially avoid the need for other mitigation techniques.

## Feasibility of implementing from RLAN perspective

RLAN devices already include technology to adjust their transmit power level over a wide range. This is part due to variation in maximum e.i.r.p. levels for different bands in different regulatory domains and as a power saving feature to extend platform battery life. There would be no impact to hardware implementation cost or complexity to address lower e.i.r.p./PSD in the proposed new band. However, lowering the e.i.r.p. /PSD should be considered only after other mitigation techniques have been explored and exhausted.

Comments

– This technique is self-evident.

– What is the impact on RLAN systems when operating at such reduced power levels including consideration of the impact on large channels and frequency reuse.

– Reducing the e.i.r.p. presents the possibility to improve the frequency reuse.

– Changes in power distribution levels requires new studies.

Attachment 6

Exclusion zones in conjunction with geo-location databases

## Technical description

Another technique to reduce the interference into incumbent services is to apply exclusion zones.

## Key points regarding mitigation technique

The exclusion zone mitigation technique has been applied for well-known services, operating sites and test ranges. For example, radio astronomy service observation sites are protected by geographic exclusion zones, which are often stated in the form of a rectangle or a circle centered on the coordinates of the observation site. The exclusion zone mitigation has also been applied near border areas to prevent interference in neighboring countries.

## Potential impact

Going forward, exclusion zones could be implemented in geo-location databases to protect radio operations that have varying time and location characteristics (see Attachment 7)**.**

## Feasibility of implementing from RLAN perspective

This proposed mitigation technique would be used in conjunction with geo-location databases.
Geo-location databases are addressed in Attachment 7.

## Comments

– Does not address EESS, mobile radars and radars with undisclosed location.

– which service is it aimed to address?

Attachment 7

Geo-location database

## [Technical description

ETSI has developed EN 301 598 the harmonized standard for white space devices (WSDs) operating in the UHF TV band (470-790 MHz). This harmonized standard is the key element in the regulation of WSDs in Europe. Appendix 2 explains the framework under which ETSI compliant WSDs will operate, and provides an overview of the requirements in the EN. In this document the framework under which compliant White Space devices will operate in the UHF TV band (470‑790 MHz) is used as an example of how similar requirements may be implemented in the 5 GHz RLAN devices.

[*Editor’s Note: This document does not address the scope of how the database is provided with the information on the incumbent services or how the appropriate operational requirements for White Space Devices are calculated*]

[*Editor’s Note: This document does not describe the implementation of the geo-location database concept for the 5 GHz RLAN case*]

## Comments

There are several technical/operational and regulatory issues which WP5A has not considered yet:

## General principles

– It does not seems conceivable that individual RLAN can be equipped with orbital propagation software and therefore there will be a centralized system in charge of informing all the billions of expected RLAN in the world when they will have to switch channel according to the orbital analysis.

– In case one believe that such orbit avoidance can be made within the individual RLANs, these questions about collecting and distributing the dynamic information about all satellites remain.

– Over any area and to maintain their operation, all RLAN operating in the 5 350‑5 470 MHz band will undertake a channel change at the same time. Over urban/suburban area, this will represent several hundred thousand equipment.

– Considering the RLAN protocol, and assuming that all these RLAN have already a list of available channels (i.e. having performed all DFS requirements), this will create huge perturbation of the use of the channels outside the 5 350-5 470 MHz band in which these numerous RLAN will try to access a new channel.

– This can only be ensured if all AP and terminals are duly connected to the internet

– Does it mean that the spectrum will be assigned to specific operators?

## Data base principles

– There is no organization that has a database of the EESS active sensors operated. The reference to the NORAD database or other satellites database is not correct, since these databases don’t carry any information about the presence of a given sensor on-board a satellite neither have a correspondence with the name used in the ITU filings.

– Even the ITU SNS (Space Networks Systems) database does not include all necessary orbital and RF characteristics of EESS (active) systems that would be required for that purpose.

– How the orbital information will be collected and how is the dynamicity of this information managed? It is to be noted that orbit adjustments are often performed on the satellites and this information would therefore be rather dynamic and not static at each satellite launch. Also, information about new satellites will have to be considered.

– The orbital characteristics are different among different types of EESS (active) sensors (SAR, altimeters, scatterometers, ...).

– The knowledge of the current orbital position of the various EESS (active) satellites is not sufficient to determine the territory illuminated by the corresponding sensors at a given moment. Indeed, the EESS(active) sensors have very different imaging geometry, not only among the various sensors (SAR, altimeters, scatterometers), but also within the same sensor type (left- or right-looking SAR, forward-looking or circular scanning scatterometers, variable altimeter measurements geometry with multiple beams, etc.).

– Some of the EESS satellites have dual use (civil and military) and information on their precise orbital position will not be disclosed to an external organization. It is unlikely that such detailed information will be made available by all EESS (active) sensors operators.

– considering the number of existing/planned satellites (several tens), it should be understood that this would imply many events each day when the 5 350-5 470 MHz band will be blocked for a given RLAN, wherever it is located. Since these blockages would be quite long, this could represent aggregate period of more than 50% of the time without availability of the channels covering the band 5 350-5 470 MHz band.

– Is it compatible with the RLAN operational requirements, considering that this would bring back extension main argument for extending the current RLAN allocation at 5 GHz ?

– Due to the global nature of EESS (active) missions/systems, such a database would require international overview and will have to be developed and maintained by a suitable international organisation taking responsibility for it.

– Which international organization would be in charge of collecting the orbital information, maintain this database, propagate all the orbits and provide the actual ephemeris of all the satellites?

– Who will pay for this task?

– Will this organization be legally/economically responsible for loss of data linked to mistakes in the generation of the information?

– How will national administrations ensure that the mechanism is working and it is actually implemented and active on all RLAN on their territory?

– In the determination of the up-to-date location of EESS satellites, it is not clear how and where would such information be provided and maintained. Although NORAD TLE data have been made publically available in its website, the data was never made available for the purpose of having tens of millions of RLANs worldwide continually downloading the data to determine mitigation strategies. Doing so could add additional burden, cost and security risk to the NORAD website. It is also uncertain as to how orbital information of all active remote sensing satellites can be made available in a timely and efficient way to the numerous RLANs so that all such RLANs are not all trying to retrieve the same information from one server. Can this function be handled by a separate entity, if so, how would it be provided and maintained?

– With regard to the protection of radar systems, it has to be noted that part of these equipment are used for military purpose and the information related to the characteristics of these equipment are unknown as well as their geographical location. In addition, some of these radars are tactical. In this situation, it is inappropriate to rely on some information on the location of such radars.

– The communications between the access points and the database needs to be able to adjust for fast moving operations, especially aeronautical systems. Additionally, a backup plan for access point and database communication failure should be presented in order to ensure protection of the incumbents.

– To be considered as a mitigation technique, there is a need for all APs to determine their own location irrespective of indoor/outdoor conditions in order to ensure that the appropriate mitigation measures and limits are applied.

– Further, the reported AP location should be accurate within 3 meters and be demonstrated to validate the AP location every ten seconds.

## Terminal principles

– Which means are going to be used to ensure precise location of each RLAN location? in particular in indoor environment?

– In the determination of the up-to-date location of an RLAN device, it is not clear how to make sure that users do not tamper with the system to use a band that they should not use in a certain region.

– In addition, some administrations may have regulatory provisions in place that could prevent the disclosure of the exact location of an RLAN.

– What about other types of Mobile applications (Peer-to-Peer, Video surveillance, …)

– How often do the terminals scan the database? It is not possible for all terminals to be listening at the same time. Thus, it is impossible for the RLAN terminals to cease all transmission on the channel at once. Does the scanning time provide enough time for all terminals to cease operation and not cause interference to EESS?

– In addition, taking into account that a number of user terminals are battery dependant, a frequent scan of the database has an impact on the power consumption. It appears essential to assess to which extent this operation degrade the battery autonomy of the terminal.

## Application principles

– It remains uncertain on the issue of how does one ensure that despite the result of the calculation performed showing the need to avoid interference to EESS that the RLAN is not “spoofed” to circumvent any mitigation strategy that should be employed from being employed.

– In the determination of potential interference from an RLAN device to EESS, would the calculation (to determine location orbital information) and mitigation strategies be performed using a single accredited software program on a single remote server or off-line at the location of the RLAN? It is not clear how does one ensure that the calculations done off-line will not be tampered with by users.

– The calculation of the times during which the RLAN could transmit could either be done at a centralized location where an appropriate software program would use the RLAN location information to make a determination of when it is able to transmit and to provide the RLAN with a validation code thereby removing a normally inhibited transmission in the band.

– The issue of malicious use may be more manageable in scenarios where access to the channels overlapping EESS operations (5 350-5 470 MHz) are more controlled.

– If the spectrum is not assigned to specific operators, but available to the general public (including operators and private users), it may be difficult to ensure the integrity of the service by dealing with malicious uses in a timely manner.

– Facing such a constraining situation where the service will be repeatedly disrupted (due to switch-off), one can believe that users could wish to overcome the situation by any means (as is currently done for DFS in number of cases).

– Any interference will represent a dead-end for EESS (active).

– Considering the interference mechanisms from RLAN to EESS (active) (aggregate interference), it is more than likely that EESS operators will detect possible interference only once RLAN deployment will be already high and mature.

– Building upon the experience of interference to meteorological radars for which it takes long time to Administrations to find single RLAN sources (for long time interference) and for which Administrations are not able to locate sources for short-term interference, it appears that administrations will not be able to handle future potential interference in urban/suburban areas.

Conclusion: A number of issues and challenges need to be addressed before the geolocation database be considered as a viable RFI mitigation technique for the RLAN/EESS (active) sharing scenario.]

Appendix 2 (to attachment 7)

Framework under which ETSI compliant WSDs will operate,
and overview of the requirements in the EN

**1 Background**

The European regulatory regime for the use of wireless devices was designed with the aim of removing the need for national type approval of devices. In this regime, manufacturers are required to self-declare conformance to the “essential requirements” of the R&TTE Directive via a number of possible routes. The primary route is through compliance with a Harmonised Standard developed by European Standards Organizations. Harmonised Standards that address the requirements of Article 3.2 of the Directive (effective use of the spectrum to avoid harmful interference) are normally produced at ETSI. These typically include RF requirements, such as transmitter power and unwanted emissions.

Once the ETSI Standard has completed the approval process and is cited in the Official Journal, equipment manufacturers could use it to show compliance with the requirements of the Radio and Telecommunications Terminal Equipment Directive. Devices compliant with the requirements of the Directive can be put into the European market – although actual use will be subject to the authorisation regimes of each member states.

In practice, citation in the OJ means that manufacturers have a well-defined set of technical requirements that TV WS equipment needs to comply with. This facilitates the development process and greatly reduces the risk that different member states come up with different requirements.

EN 301 598 differs from past ETSI harmonized standards, in the sense that it targets the interactions between a WSD and a white space database (WSDB) in addition to the usual specification of RF limits. This is because the European framework for access to TV white spaces stipulates that the limits on the radiated frequency and power of a WSD shall not be fixed, but dynamically calculated by a WSDB on the basis of the WSD’s location, technical characteristics and requirements for protection of the incumbent users. The novel features of this standard set the foundations for future standards for cognitive and WSDs dynamically sharing spectrum with incumbents in other bands.

**2 Framework for operation in the TV White Spaces**

EN 301 598 is based on a framework for access to TVWSs which involves the following four entities:

1. White space databases WSDB − WSDBs provide devices the parameters for the radio transmissions, so that devices do not cause undue interference to the primary users.
2. WSDB regulatory listing − This identifies the WSDBs that are authorized by a national regulatory authority (NRA) to provide service in the relevant jurisdiction.
3. Master WSDs − These are geolocated devices capable of communicating with a WSDB and of accessing the regulatory list.
4. Slave WSDs − These are devices that do not communicate directly with a WSDB, but instead operate under the control of a master WSD.

WSDBs and master devices exchange information to determine the parameters of the radio transmissions, EN 301 598 specifies three datasets for this:

**– Device parameters** are the parameters that WSDs will communicate to a WSDB in order to provide the WSDB with relevant information about the device. These parameters include the technical characteristics of the device and its location.

**– Operational parameters** are generated by a WSDB and communicated to WSDs.
They specify the radio resources (frequencies and powers) and other instructions which WSDs must comply with. There are two types of operational parameters:

– Specific operational parameters. The WSDB derives these for a particular WSD, on the basis of the WSD’s specific device parameters.

– Generic operational parameters. The WSDB derives these for all slave WSDs operating in the coverage area of a master WSD. These are derived from the characteristics of the master WSD, and assumed default (cautious) slave device parameters.

**– Channel usage parameters**– These are reported back by a WSD to a WSDB to inform of the *actual* radio resources that it will use.

The framework assumes a typical sequence of events in the interactions between the four entities. This is described below and illustrated in Figure X.

1) **Database identification**. The master WSD must obtain the list of the WSDBs approved to operate in the regulatory domain. The list is hosted by the relevant NRA (as is the case of the UK) or by a trusted party, and accessible over the internet. The master WSD selects a WSDB from the list for its operations.

2) **Specific operational parameters for a master WSD**. The master WSD communicates its device parameters – which include its location – to the chosen WSDB. The WSDB will generate the operational parameters on the basis of the information provided by the master WSD, and the information that it holds about the primary users. The operational parameters will include a range of channels and powers. The master device must select which of those it will use, and report its choice to the WSDB by means of the channel usage parameters. The device can then start transmissions.

3) **Generic operational parameters for slave WSDs.** These parameters identify the resources that any slave WSD in the coverage area of master WSD can use. The master WSD will make a request for these parameters to the WSDB, which will use the information about the master WSD to calculate the master’s coverage area. The WSDB will then calculate the generic operational parameters by assuming a) that slaves may be at any location within the master’s coverage area, and b) default conservative values for the DPs of the slaves. At this stage the WSDB does not know anything about the slave WSDs that could be using these parameters. The WSDB will then send the generic operational parameters to the master WSD, and the master WSD will broadcast them to its coverage area.

4) **Association of a slave WSD with a serving master WSD.** When switched on, a slave WSD will listen for a master’s broadcasts. It will then use the channels and powers identified in the generic operational parameters to associate with the master WSD. This means that it will communicate its unique device identifier, or the full set of its device parameters. The slave WSD may now continue to use the radio resources identified in the generic operational parameters for data transmissions, or alternatively it may request specific operational parameters.

5) **Specific operational parameters for a slave WSD.** The radio resources allowed by the generic operational parameters will be limited because they are based on conservative assumption. A slave WSD whose device parameters are better than these assumptions, in particular a device that can accurately locate itself, may provide its parameters to the WSDB to gain access to more resources. For this, a process similar to obtaining specific operational parameters for a master WSD will be followed.

Figure X

Framework for operation in the TV whites spaces and typical sequence of operation



**3 Device requirements in EN 301 598**

EN 301 598 includes several requirements. It first defines that devices can be of two types – A and B, next specifies a number of RF requirements which are not unlike those of traditional harmonised standards, and finally includes a several non-RF requirements to deal with the fact that the radio parameters are communicated by a database. This section summarises of these requirements, with an emphasis on the elements that differ from previous ETSI ENs.

## 3.1 Device types

EN 301 598 defines two types of WSDs:

* A Type A WSD is a device that is intended for fixed use only. This type of equipment can have integral, dedicated or external antennas.
* A Type B WSD is a device that is not intended for fixed use and which has an integral antenna or a dedicated antenna.

The key differentiator between the two classes is the type of antenna that the device supports. In this context, an integral antenna is designed as a fixed part of the equipment and that cannot be disconnected. An external antenna is removable antenna which is designed for use with a broad range of radio equipment, i.e. it has not be designed for use with a specific product. And a dedicated antenna is removable antenna supplied and assessed with the equipment, designed as an indispensable part of the equipment.

The classification also corresponds to the applications that have so far have been identified. Professional installations, such as a base station serving rural broadband customers, will most likely be type A devices. Type-B WSDs correspond to mobile/portable equipment such as handsets, dongles, or access points which do not require installation and can be mass market. EN 301 598 requires these devices to have non-detachable antennas, to mitigate the risk of the end user tampering with the antenna.

## 3.2 RF requirements

As with past standards, the RF requirements in EN 301 598 address the prevention of harmful interference by ensuring that the wanted radiated power, and the unwanted radiated power (inside and outside the band) do not exceed specific limits.

The specifications of limits outside the UHF TV band are relatively straightforward, and are defined in the same manner as existing HSs, and include limits on transmitter/receiver spurious emissions and transmitter inter-modulation. On the other hand, the limits inside the UHF TV band are more complex. This is fundamentally because a WSD may operate in a single DTT channel, or simultaneously in a group of contiguous DTT channels, or in multiple non-contiguous DTT channels, or a mixture of contiguous and non-contiguous DTT channels. The key RF requirements are the following

### 3.2.1 Nominal channel

A Nominal Channel is defined as one or more contiguous DTT channels that are used by a WSD for its wanted transmissions. Its lower and upper edge frequencies must coincide with the European harmonized DTT channel raster. The EN requirements are:

– The Nominal Channel Bandwidth used by a WSD shall not exceed the Maximum Nominal Channel Bandwidth specified by the WSDB.

– The Total Nominal Channel Bandwidth, which is the sum of the bandwidth in all Nominal Channels, shall not exceed the Maximum Total Nominal Channel Bandwidth specified by the WSDB.

### 3.2.2 In-block power and power spectral density

The WSDB will communicate the WSD two power limits for each DTT channels where operation is possible:

*– P*0(dBm / 100 kHz) Maximum in-block RF e.i.r.p. spectral density for each DTT channel edge frequency pair.

*– P*1 (dBm) Maximum in-block RF e.i.r.p. for each DTT channel edge frequency pair.

The requirement of EN 301 598 is that the device must not exceed the levels communicated by the WSDB. In particular, The RF power spectral density in any 100 kHz bandwidth within a DTT channel shall not exceed the level P0 specified by the WSDB for that channel.

### 3.2.3 Unwanted emissions inside the band

The out-of-block e.i.r.p. spectral density, POOB, of a WSD shall satisfy the following requirement:

POOB (dBm / (100 kHz)) ≤ max{ PIB (dBm / (8 MHz)) - ACLR (dB), - 84 (dBm / (100 kHz)) }

where PIB is the in-block e.i.r.p. spectral density over 8 MHz, and ACLR is the adjacent channel leakage ratio outlined in the Table I below for different device emission classes. Each out-of-block e.i.r.p. spectral density is examined in relation to PIB in the nearest (in frequency) DTT channel used by the WSD.

The device class is part of the device parameters communicated to the WSDB, which will use the information in calculating operation parameters. Class 1 devices have the most stringent emission mask and will benefit from increased TVWS availability.

Table X

ACLR for different device emission classes

|  |  |
| --- | --- |
| **Where POOB falls within the nth adjacent DTT channel (based on 8 MHz wide channels)** | **ACLR (dB)** |
| **Class 1** | **Class 2** | **Class 3** | **Class 4** | **Class 5** |
| n = ±1 | 74 | 74 | 64 | 54 | 43 |
| n = ±2 | 79 | 74 | 74 | 64 | 53 |
| n ≥ +3 or n ≤ -3 | 84 | 74 | 84 | 74 | 64 |

The absolute threshold of –84 dBm/(100 kHz) is to take into account the difficulty in maintaining a high leakage ratio at very low in-block e.i.r.p.s.

## 3.3 Data communication requirements

The objective of EN 301 598 is that the WSDs only communicate with approved WSDBs, and then provide the necessary device parameters to the WSDB and operate in accordance with the information received from the database.

The EN defines the contents of the operational parameters, the device parameters and the channel usage parameters, but their detailed specification (such as the format and size of the data) is left to the protocols that devices and WSDBs will use to communicate (such as IETF PAWS).

### 3.3.1 Database identification

Database identification is the process by which a master WSD consults the list of WSDBs that have been approved by the relevant NRA for the provision of services at the geographical location of the master WSD.

At start up, and before initiating any transmissions, a master WSD must locate and consult the list. EN 301 598 further specifies that the master WSD must not transmit if it cannot consult the list, and that it must not request parameters from a WSDB that is not on the list. In addition, the master WSD must re-consult the list with a frequency that is specified in the list itself, and that would normally be in the order of one or several days.

The internet address for the lists for the various regulatory domains is provided in ETSI TR 103 231.

### 3.3.2 Data exchange and compliance with parameters

The dynamic nature of frequency and power allocations to WSDs led ETSI to specify precise requirements for the exchange of parameters between WSDBs and WSDs and subsequent compliance with OPs. However, EN 301 598 is not prescriptive about the sequence, or about the name and format of the parameters. Instead, the requirements are about what parameters a device is allowed to use, and what parameters it must communicate to other entities.

These requirements can be summarised as follows:

– A WSD shall only transmit in accordance with operational parameters that it has received from a WSDB.

– A master or a slave WSD that require specific operational parameters from a WSDB must report their device parameters to the WSDB. A slave WSD that intends to use the generic operational parameters broadcasted by a master must report its unique device identifier (although it may report the rest of the device parameters if it wishes to).

– A master WSD must communicate its channel usage parameters to the WSDB prior to transmission, and slave device must do the same to the serving master WSD.

– A master WSD must relay the parameters between the WSDB and slave WSDs that it serves.

### 3.3.3 Master and slave WSD update

NRAs have stated that it should be possible to switch off a device within a short time for interference management purposes. For this, EN 301 598 requires a master WSD to support an update function, through which a WSDB can inform that the OPs of the master WSD and its served slave WSDs are no longer valid.

In addition, there are requirements to automatically stop transmissions when the connection between the master WSD and the WSDB is lost, and where the slave WSD stops receiving the signal of the serving master WSD.

### 3.4 Other requirements

Accurate location of devices is an important element of operation under the framework. Also, special attention must be given to avoid the end user tampering with the elements of the device that are used in determining the operational parameters. The EN 301 598 includes specific requirements in these areas.

### 3.4.1 Geolocation requirements

A key element in the operation of WSDs is the ability of the WSDB to provide OPs on the basis of the location of the WSD. Not all WSDs are required to geolocate, though. The broad location of slave WSDs can be derived from an estimate the coverage area of the serving master WSD, and hence slave WSDs are not required to have this capability. On the other hand, the location of the master WSDs must be known by the WSDB in order to calculate operational parameters for it and generic operational parameters for the slave devices that it serves. Therefore, EN 301 598 requires master WSDs to have this capability.

In addition, WSDs which geolocate must check its location at least every 60 seconds and renew the parameters if they move away from the location originally reported to the WSDB.

### 3.4.2 User access restrictions and security measures

An important concern from the perspective of interference to incumbent primary services is the risk of users tampering with the WSDs. If a WSD user is capable of bypassing the process of receiving parameters from a WSDB, or is capable of inputting bogus device parameters into the WSD, then serious interference could result. For this reason, EN 301 598 contains strict requirements to avoid the users gaining access to the configuration of the WSD, and to ensure that communications with a WSDB are secured and authenticated.

Attachment 8

Dedicated sensors

[Technical description

TBD (e.g. based on Document [4-5-6-7/369](http://www.itu.int/md/R12-JTG4567-C-0369/en))

Comments

There are several technical/operational and regulatory issues which WP5A has not considered yet:

– With reference to what is said on DFS, even assuming that, differently from the RLAN, these devices will have the sufficient sensitivity to detect the SAR signal, the specific EESS (active) problem remains, in particular for SARs. Indeed, there is still the need to switch channel before the SAR signal illuminates the RLAN and not at the moment it is illuminated.

– SAR systems present different operating modes which are not performing measurements over a continuous strip, but can jump from one area to another, hence presenting holes within the SAR visibility area. Therefore a remote local sensor may not sense the SAR because it is not transmitting when over the sensor area; but the SAR may then become active over the area where the RLANs are located and receive interference from them.

– Furthermore, if the SAR (or other EESS active sensor) illumination moves from open water onto land masses, there will be no possibility to protect measurements made on the coastal areas since it is unlikely that “RLAN sensors” could be deployed on open water. Similar problems would exist for EESS active sensors moving from mountain areas or, in general, areas where these remote RLAN sensors cannot be placed.

– Another concern is to know how the alarm from the sensor network would be relayed to all RLAN in the region. Considering a typical 7 km/sec speed of the satellites, the size of the region where all the RLAN would have to switch channels would be quite large, since it would have to allow time for the sensor to communicate its detection to a control centre, time to the control centre to distribute the information to all the AP in the region, and time for the AP and terminals to switch channels.

– This can only be ensured if all AP and terminals are duly connected to the internet

– Overall, if all technical issues are solved, such a network of interconnected sensors would be very complex and expensive. Who is going to pay for the world-wide deployment of such a sophisticated network?

– Who is going to take the responsibility to operate it?

– how will administrations check the actual use of this system?

– Due to the global nature of EESS (active) missions/systems, such a sensors network would require international cooperation and oversight, introducing further complexities (e.g., responsibilities, interactions, development, etc.).

– To be considered a feasible interference mitigation technique, Dedicated Listening Devices (DLDs) needs to take into account and demonstrate they can properly detect and protect current and future radar pulses that are less than one microsecond, wide-band, continuous-wave, and frequency hopping systems. Further, it should be able to inform the access point of the bandwidth for proper channel selection.

– The interactions between the DLDs, APs and database needs to be clearly articulated and dependencies between the sensing network and database fully explained, include a plan for when communication and/or sensing failure occurs between the DLD, AP, and database as well as self-diagnostics to access proper functions.]