|  |  |  |  |
| --- | --- | --- | --- |
|  | **Radiocommunication Study Groups** | |  |
| **INTERNATIONAL TELECOMMUNICATION UNION** | |  | |
|  | |  | |
| Source: Document 5A/TEMP/109 | | **Annex 23 to Document 5A/298-E** | |
| **21 November 2016** | |
| **English only** | |
| Annex 23 to Working Party 5A Chairman’s Report | | | |
| WORKING DOCUMENT TOWARDS A PRELIMINARY DRAFT NEW  REPORT ITU-R M.[RLAN Mitigation] | | | |
| Study of proposed additional mitigation techniques to facilitate sharing between RLAN systems and incumbent services | | | |

***[Editor’s Note****: Document* [*5A/114*](http://www.itu.int/md/R15-WP5A-C-0114/en)[*Annex 23*](https://www.itu.int/md/dologin_md.asp?lang=en&id=R15-WP5A-C-0114!N23!MSW-E) *“Compilation of technical information on techniques that could be used in RLAN deployments to facilitate sharing” provides details and initial comments with regard to various proposed additional mitigation techniques, Administration should consider that Annex as a resource when providing input to this working document. Additionally, text is needed for the introduction explaining why focus is given on the three additional mitigation techniques contained in the current draft.]*

# 1 Introduction

Under Resolution **229 (WRC-12)**, RLANs can operate in the 5 250-5 350 MHz and 5 470‑5 725 MHz frequency ranges on a co-primary basis with radar systems. Prior to operation, RLANs in those frequency ranges must use specific regulatory provisions and DFS to enable the RLAN networks to protect the incumbent radiolocation systems. The mobile systems must also vacate RLAN channels when new radiolocation systems come into operation on any portion of those channels[[1]](#footnote-1).

Although the techniques specified in Resolution **229 (WRC-12)** enable effective sharing in these frequency ranges, additional mitigation techniques or modifications to DFS may be needed to facilitate sharing in other frequency ranges to ensure protection of co-primary users, including aeronautical radiolocation systems, ground-based and maritime radars, and EESS (active). Research is underway to investigate the possibility to mitigate interference to incumbents in the 5 350‑5 470 MHz band in a practical manner so that RLANs would protect incumbent services.

*[Editor’s Note: please specify what mitigation techniques (described in the report) applies to what band/service]*

# 2 Dedicated Radar Signal Detectors

Dedicated Radar Signal Detectors (DRSDs) are independent detectors that will interact with RLAN access points (APs) to enable authorized use of the APs over a specific geographical area to allow detection of specific radar, for which DFS alone is not a sufficient mitigation technique. The DRSDs detect radar emissions and this information when received by APs allows the latter to dictate to any connected AP devices that use is not allowed while the radar signal is present.

Industry is researching the use of DRSDs. Among the issues being studied are coverage area, connection security, channel authorization methodology (including architecture and interdependencies), detection threshold and required response time. Achievable response time is also being studied, noting that latency of the control network between DRSDs and APs is a factor in achievable minimum channel move times.

## 2.1 DRSD Coverage area

A DRSD could be used to facilitate detection of radar emissions from a distance if mounted outside. For example, DRSDs could be placed on towers or rooftops. Industry is studying the area over which a DRSD could detect a radar signal, and whether that area is sufficient to protect radar operations.

*[Editor’s Note: It is not clear at this time whether DRSD could detect all type of current radars. Question is also raised, how it could be implemented when a new or modified radar with differing technical characteristics and/or scanning pattern is introduced, and whether DRSDs can detect and protect current and future radar pulses that are less than one microsecond, wideband, continuous-wave, and frequency hopping. Both, of which, may result in the DRSD not sensing the radar because it is not transmitting when over the sensor area; but the radar may then become active over the area where the RLANs are located and receive interference from the RLANs]*

## 2.2 Radar data and connection security

DRSD siting and network topologies are also parts of the required studies. For example, each DRSD network could consist of one or more DRSDs capable of providing low latency notifications to access points (APs) in their areas of coverage. DRSDs could be location-aware high sensitivity receivers and could be installed at locations with unobstructed views of the sky and surrounding terrain. The presence of radar emissions could be communicated to the APs over secure methods that ensure against corruption or unauthorized modification of the data. Periodic encrypted contact verification signals between the DRSD network and the APs [required periodicity TBD] could be designed to ensure that RLAN devices timely receive notifications and that their transmissions do not exceed the radar protection level specified.

*[Editor’s Note: Further work is required to define the secure lines between DRSD and APs, such as the maintenance and management of the secure lines (including a mechanism to handle new APs)]*

## 2.3 Channel authorization methodology

RLAN devices would follow instructions from the DRSD network regarding authorized channels when a DRSD detects radar in use: for example, the device might be required to move to a different channel, refrain from initiating on a channel where the radar is operating, or avoid a channel for a specified period.

## 2.4 Response time

As noted above, DRSD-connected RLAN devices would have to ensure that their transmissions comply with procedures established for protection of the incumbent services. Maximum response latencies and minimum delays prior to resumption of transmission following the most recent detection of an incumbent services’ transmission would be specified for each class of incumbent system.

# 3 Database

*[****Editor’s note****: Database use is currently only being examined as a mitigation mechanism, for purposes of this Working Document, as a means for determining if protecting EESS (active) operations is possible]*

RLANs have used a terrestrial geolocation database to share frequency bands with both fixed broadcast stations and with nomadic wireless PMSE microphones including Electronic Newsgathering (ENG) stations, through the voluntary registration of wireless microphones in a geolocation database for protection from unlicensed RLAN devices at a specific geographic location for a specific time period. A terrestrial-based geolocation database keeps track of the location of licensed terrestrial stations (including wireless microphone devices that are registered on a voluntary basis) and their corresponding spectrum and service areas.

Industry is currently investigating the ability of RLANs to protect incumbent EESS (active) operations from interference via such a geolocation approach. (see compilation for more detailed proposals and the associated comments and challenges that are unresolved).

Current terrestrial geolocation databases are based on all the necessary information on the incumbent service being available on a national basis. In the case of EESS, detail information on the satellite system (e.g., beam location, scanning direction, and velocity of the satellite) would be required to determine the service area coverage that changes dynamically. And this information will not be available on a national basis and would need to be collected on an international basis.

## 3.1 Database Security and Integrity

[Industry has experience in devising geolocation databases to enable opportunistic use of vacant broadcast television spectrum with respect to PMSE and ENG as discussed above. For potential sharing in the 5 350-5 470 MHz band, in addition to the database security that requires additional study, the dynamic nature of EESS satellites should be carefully taken into consideration. One approach expressed theoretically to date is that the database would rely only on sensing and publicly-available information and would only provide authorization tickets to APs connected to the database.]

*[Editor’s Note: These text need to be reviewed in order to provide an explanation of the needs of database security and integrity but not solutions]*

### 3.1.1 Database security

### 3.1.2 Database integrity

# 4 Device Security and Integrity (DSRD or database components)

Device manufacturers can be required to include security features in RLANs to prevent unauthorized software and hardware changes to ensure that mitigation techniques cannot be disabled, or devices reprogrammed to operate outside parameters for which the RLAN device was certified.

*[Editor’s Note: These text need to be reviewed in order to provide an explanation of the needs of device security and integrity but not solutions]*

These features include: x, y, z *[Editor’s note: manufacturers to list example actions that have been taken to ensure the devices are tamper free]*

## 4.1 Determine availability of data

## 4.2 EESS Data and Connection security

### 4.2.1 Satellite data

### 4.2.2 Satellite Connection Security

## 4.3 RLAN channel authorization methodology

# 5 Update of RLAN devices

# 6 Dynamic Frequency Selection (Access point or DRSD)

RLAN devices seeking to share in other frequency bands with radio determination incumbents may need to have enhanced Dynamic Frequency Selection (DFS) capabilities.

*[Editor’s Note: Some administration require manufacturers of RLAN devices sharing spectrum in the 5 GHz radar frequency ranges take measures to ensure that DFS cannot be disabled. As noted in Section 4 of this Report, prevention of device tampering by consumers requires Administration attention.]*Because DFS parameters need to be matched to the characteristics of the different type of radars to be protected, the required parameters are different for the different radar types.

## 6.1 DFS for Meteorological Radars

*[Editor’s Note: The current version of the 1652 is rev 1 (2011). It need to be verified, whether rev. 1 covers current radar characteristics]*

Table 1 provides the DFS requirements for the band 5 350 to 5 470 MHz to protect meteorological radars. These parameters have been proven to allow WAS to avoid interfering with the meteorological radars in the band 5 600 to 5 650 MHz.

Table 1

|  |  |
| --- | --- |
| Parameter | Values for the frequency band 5 350 – 5 470 MHz |
| Minimum pulse width (see detailed test signals in Report ITU-R M.2115) | 0.5 μs |
| PRF (see detailed test signals in Report ITU-R M.2115) | Fixed, Staggered and Interleaved |
| Channel Availability Check (CAC) time | 10 minutes |
| Off-Channel CAC (Note 1) | Yes |
| CAC and Off-Channel CAC detection probability (Note 2) | 99.99% |
| In-service monitoring detection probability | 60% |
| CAC for slave devices with power above 200 mW (after initial detection by In-service) | Yes |
| Detection Threshold | -62 +10 -EIRP Spectral Density (dBm/MHz) + G (dBi), however the DFS threshold level shall not be lower than -64 dBm assuming a 0 dBi receive antenna gain |
| Channel Move time | 10s |
| Channel closing time | 1s |
| Non-occupancy period | 30 minutes |
| Possibility to exclude 5 600‑5 650 MHz band from the channel plan or to exclude these channels from the list of usable channels | Yes |
| Requirement that none of the DFS related settings are accessible to the end‑user | Yes |

**6.2 Other Issues**Additional issues regarding DFS are being studied, including:

1) Potential use for all radar types (Ground (including meteorological radars)/Maritime/EESS/Aeronautical)

i) Threshold required:

A Adjustment to DFS threshold value

B Probability of coincidence

C Value with and without timing changes

D Detection of 0.1 µsec to 1 µsec pulse width signals.

ii) Channel off time Expiration (for dedicated detectors):

A Define expiration methodology

B Define expiration time period.

iii) Channel Move time:

A Define total time (i.e., channel detection, channel closing, etc.).

B Define Channel Move Spacing (to ensure RLAN channel moves are sufficient to ensure no adjacent channel interference to incumbents).

2) Robustness and effectiveness of DFS

1. Recommendation [ITU-R M.1652](http://www.itu.int/rec/R-REC-M.1652/en). [↑](#footnote-ref-1)