|  |  |
| --- | --- |
| **Radiocommunication Study Groups** |  |
|  |  |
|  |  |
| Source: Document 5A/TEMP/261 | **Annex 8 to****Document 5A/636-E** |
| **10 November 2014** |
| **English only** |
| Annex 8 to Working Party 5A Chairman’s Report |
| WORKING DOCUMENT TOWARDS A PRELIMINARYDRAFT NEW REPORT ITU-R M.[RLAN Mitigation]  |
| Possible additional mitigation techniques to facilitate sharingbetween RLAN systems and incumbent services |

***[Editor’s Note****: Document 5A/636 Annex 9 “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 Annex 9 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 so that RLANs would protect incumbent services, including use of geo-location databases, dedicated radar signal detectors, and enhancements to DFS.

# 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. 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.

## 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.

## 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 protecting EESS (active) operations*.]

RLANs have used a geolocation database to share frequency bands with both fixed broadcast stations and with nomadic wireless PMSE microphones including Electronic Newsgathering (ENG) stations, through the registration of wireless microphones in a geolocation database for protection from unlicensed RLAN devices at a specific geographic location for a specific time period. Industry is currently investigating the ability of RLANs to protect incumbent EESS (active) operations from interference via such a geolocation approach.

## 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, database security requires additional study. The expectation 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.

### 3.2.1 Database Security

### 3.2.2 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 changes to ensure that mitigation techniques cannot be disabled, or devices reprogrammed to operate outside parameters for which the RLAN device was certified.

## 4.3 Determine availability of data

## 4.4 Satellite Data and Connection security

### 4.4.1 Satellite Data

### 4.4.2 Satellite Connection Security

## 4.5 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 radar incumbents may need to have enhanced Dynamic Frequency Selection (DFS) capabilities. One administration has recently required that manufacturers of RLAN devices sharing spectrum in the 5 GHz radar frequency ranges take measures to ensure that DFS cannot be disabled.

Additional issues regarding DFS are being studied, including:

Potential use for all radar types (Ground/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).

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