Advanced Dynamic spectrum
5G mobile networks Employing
Licensed shared access

Advanced Dynamic spectrum 5G mobile networks Employing Licensed shared access

Grant Agreement for: Collaborative project
Project acronym: ADEL
Grant Agreement number: 619647

Advanced Dynamic spectrum 5G mobile networks Employing Licensed shared access

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no. 619647.

Project Deliverable D4.3: Spectrum Sharing Policy Reinforcement

Contractual Date of Delivery:	01/06/2016
Actual Date of Delivery:	15/06/2016
Editors:	Konstantinos Voulgaris
Authors:	Konstantinos Voulgaris, Georgios Papageorgiou, Konstantinos Ntougias, Nicola Marchetti, Muhammad Majid Butt, António Jorge Morgado, Álvaro Gomez
Work package title:	WP4 – Licensed Shared Access resource allocation techniques
Work package leader:	Athens Information Technology
Contributing partners:	AIT, TCD, PTIN, UEDIN
Nature	O[1]
Dissemination level	CO[2]
Version	V2.0

[1] Nature of the Deliverable:
R = Report, P = Prototype, D = Demonstrator, O = Other
[2] Dissemination level codes:
PU = Public
PP = Restricted to other programme participants (including Commission Services)
RE = Restricted to a group specified by the consortium (including the Commission Services)
CO = Confidential, only for the members of the consortium (including the Commission Services)

Total Number of Pages:	
File:	

Abstract: This deliverable presents the problem of enforcing Licensed Shared Access policies under the ADEL architecture. We tackle this issue in three ways: first, we safeguard security and integrity in accessing the ADEL controlling nodes; then we develop a novel method to detect misbehaving nodes; and, finally we present novel resource allocation protocols that account for the behaviour of the LSA users.

Keywords: LSA, Shared Access, Policy Enforcement, Misbehaviour, Resource Allocation

Document Revision history

Version	Date	Send to	Summary of main changes	Approved by
V0.1	16/10/15	ALL	Initial version with inputs from all contributing partners	
V0.2	25/01/16	ALL	Initial version with inputs from all contributing partners	
V0.3	26/05/16	ALL	Complete input for Section 7	
V0.4	27/05/16	ALL	Complete input for Sections 8, 9	
V1.0	30/05/16	ALL	Final version	
V2.0	14/06/16	ALL	QA completed	

Copyright

© Copyright 2014 – 2017, the ADEL Consortium

Consisting of:

Coordinator: Dr. Tharm Ratnarajah, University of Edinburgh (United Kingdom) - UEDIN

Participants:

Athens Information Technology (Greece) – AIT

Thales Communications and Security (France) - TCS

Technical University Darmstadt (Germany) - TUDA

Intel Mobile Communications GmbH (Germany) - IMC

EURECOM (France) - EUR

Trinity College Dublin (Ireland) - TCD

Portugal Telecom Inovacão SA (Portugal) – PTIN

This document may not be copied, reproduced, or modified in whole or in part for any purpose without written permission from the ADEL Consortium. In addition to such written permission to copy, reproduce, or modify this document in whole or part, an acknowledgement of the authors of the document and all applicable portions of the copyright notice must be clearly referenced.

This document reflects only the authors' view. The European Community is not liable for any use that may be made of the information contained herein.

All rights reserved.

Executive Summary

This is the deliverable *D4.3 Spectrum Sharing Policy Reinforcement*, developed under FP7 project ADEL (ICT- 619647). This work was carried out as part of WP4: Licensed Shared Access resource allocation techniques. This deliverable relies on the work defined within task T4.3 as detailed in the Description of Work.

1 Table of Contents

2 List of Figures and Tables

2.1 List of Figures

2.2 List of Tables

3 Abbreviations

5G Fifth generation
AWGN Additive White Gaussian Noise
BF Beamforming
CR Cognitive Radio
C-RAN Cloud-Radio Access Network
CSI Channel State Information
CSIR Channel State Information at the Receiver
CSIT Channel State Information at the Transmitter
ED Energy Detection
i.i.d. Independent and identically distributed
LSA Licensed Shared Access
MAC Medium Access Control
MF Matched Filter
MIMO Multiple-Input-Multiple-Output
MISO Multiple-Input-Single-Output
MNO Mobile Network Operator
OOB Out-of-Band
QoS Quality-of-Service
RAN Radio Access Network
SDMA Spatial Division Multiple Access
SIMO Single-Input-Multiple-Output
SINR Signal-to-Interference-plus-Noise Ratio
SNR Signal-to-Noise Ratio
SS Spectrum Sensing
VMNO Virtual Mobile Network Operator
ZF Zero Forcing

4 Purpose and Scope

In the traditional CR literature, the issue of how to detect and identify secondary users who are violating the spectrum access rules and policies and discourage them by appropriate incentives and penalties has received considerable attention. However, the proposed solutions are either inadequate to address all issues and misbehaving scenarios, or too complicated and hard to implement. By imposing stricter access rights to secondary users the LSA paradigm has the potential to simplify spectrum access policy reinforcement. This Task has developed practical algorithms to detect misbehaving wireless nodes that violate LSA spectrum access policies and appropriate penalty / incentive schemes that reinforce secondary user compliance. Such compliance checking and reinforcing is not as simple as in the case of traditional spectrum allocation rules and may require distinguishing between occasional / unintentional (due to spectrum sensing errors) and persistent / intentional violations of policies.

5 Reference Documents

[Pap2008] Papamanthou, Charalampos, Franco P. Preparata, and Roberto Tamassia. "Algorithms for location estimation based on RSSI sampling." Algorithmic Aspects of Wireless Sensor Networks. Springer Berlin Heidelberg, 2008. 72-86.

[Peng2006] Peng, Rong, and Mihail L. Sichitiu. "Angle of arrival localization for wireless sensor networks." Sensor and Ad Hoc Communications and Networks, 2006. SECON'06. 2006 3rd Annual IEEE Communications Society on. Vol. 1. IEEE, 2006.

[Beck2009] A. Beck and M. Teboulle, "A Fast Iterative Shrinkage-Thresholding Algorithm for Linear Inverse Problems," *SIAM Journal on Imaging Sciences*, vol. 2, no. 1, pp. 183--202, Jan. 2009.

[Boyd2010] S. Boyd, N. Parikh, E. Chu, B. Peleato, and J. Eckstein, "Distributed Optimization and Statistical Learning via the Alternating Direction Method of Multipliers," *Foundations and Trends in Machine Learning*, vol. 3, no. 1, 2010.

[Kim2007] S.-J. Kim, K. Koh, M. Lustig, S. Boyd, and D. Gorinevsky, "An Interior-Point Method for Large-Scale ℓ_1-Regularized Least Squares," *IEEE Journal of Selected Topics in Signal Processing*, vol. 1, no. 4, pp. 606--617, Dec. 2007.

[Tibshirani1996] R. Tibshirani, "Regression shrinkage and selection via the lasso: a retrospective,"*Journal of the Royal Statistical Society: Series B (Statistical Methodology)*, vol. 58, no. 1, pp. 267--288, Jun. 1996.

[Osbourne2000] M. Osbourne, B. Presnell, and B. Turlach, "A new approach to variable selection in least squares problems," IMA *J. Anal.* 20, 3 (2000), 389-402.

[Facchinei2015] F. Facchinei, G. Scutari and S. Sagratella, "Parallel Selective Algorithms for Nonconvex Big Data Optimization," *IEEE Transactions on Signal Processing*, vol. 63, no. 7, pp. 1874-1889, Nov. 2015.

[ADEL D5.2] Project Deliverable D5.2: Centralised and Distributed Sensing Techniques.

[Yang2016] Yang Yang, and Marius Pesavento, "A Unified Successive Pseudo-Convex Approximation Framework," arxiv.org, 2016.

[Yang2014] Yang Yang, and Marius Pesavento, "An Online Parallel Algorithm for Spectrum Sensing in Cognitive Radio Networks," *Asilomar Conference on Signals, Systems and Computers, 2014 48th*, IEEE, 2014.

[Fan2001] Fan J. and Li R (2001), "Variable Selection via Nonconcave Penalized Likelihood and Its Oracle Properties," *Journal of the American Statistical Association*, 96, 1348-1360.

[Zou2006] Zou, Hui, "The adaptive lasso and its oracle properties," *Journal of the American statistical association* 101.476 (2006): 1418-1429.

[Zou2008] Zou, Hui, and Runze Li. "One-step sparse estimates in nonconcave penalized likelihood models." *Annals of statistics* 36.4 (2008): 1509.

[Johnson2015] Johnson, Brent A., et al. "Model selection and inference for censored lifetime medical expenditures." Biometrics (2015).

[Ark2010] Stamatios Arkoulis, Giannis F. Marias, Pantelis A. Frangoudis, Jens Oberender, Alexandru Popescu, Markus Fiedler, Hermann de Meer and George C. Polyzos, "*Misbehavior Scenarios in Cognitive Radio Networks*", in Future Internet 2010, 2(3), 212-237; doi:10.3390/fi2030212

[Park2014] Jung-Min Park, Jeffrey H Reed, A A Beex, T Charles Clancy, Vireshwar Kumar, Behnam Bahrak, "*Security and enforcement in spectrum sharing*", Proceedings of the IEEE, 2014, vol. 102, n. 3

[Ofcom] Ofcom, "*Baldock radio monitoring station*", available at: http://stakeholders.ofcom.org.uk/binaries/enforcement/spectrum-enforcement/baldock.pdf

6 Publications

M. Majid Butt, Carlo Galiotto and Nicola Marchetti, "Fair and Regulated Spectrum Allocation in Licensed Shared Access Networks", accepted in IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), 2016.

V. Frascolla, A. Morgado, A. Gomez, M. M. Butt, N. Marchetti, K. Voulgaris, C. B. Papadias, “Dynamic Licensed Shared Access – A new architecture and spectrum allocation techniques,” accepted in IEEE Vehicular Technology Converence (VTC) Fall 2016.

G. Papageorgiou, K. Voulgaris, C. B. Papadias, “Sparse Modeling Methods for Misbehaviour Detection in LSA Networks,” submitted to IEEE Global Wireless Summit (GWS) 2016.

7 Spectrum Sharing Policy Enforcement

Under task 4.3, ADEL intends to propose mechanisms to detect policy violation, either intentional or unintentional, and devise penalties and/or incentives schemes to promote conformance to the sharing rules.

7.1 Introduction

To achieve the task's goals, is important to identify the types of threats that might occur in the LSA system. One of the approaches, which was followed by AIT, consists in identifying the threats according to the logical entity being attacked. Other approach, followed by PTIN, is to list the threats according to the logical entity originating them.

In the ADEL approach, the logical entities of the LSA system are the LSA Band Manager, LSA Repository, Radio Environment Map (REM) and Spectrum Sensing Reasoning, which may be deployed by private companies, to which are added the LSA Authentication Server and the LSA Sharing Agreement Databases, which are mandatorily deployed by the national regulatory authority (NRA). For security reasons, whenever possible, these logical entities should be linked with each other preferably through wired connections.

This LSA system is going to be used to coordinate the access of the several LSA licensees to the LSA band, so they can share the band without causing interference to each other and to the Incumbents. To improve the LSA system reliability and responsiveness, several spectrum sensing networks were added, which operate under the coordination of the spectrum sensing reasoning logical entity.

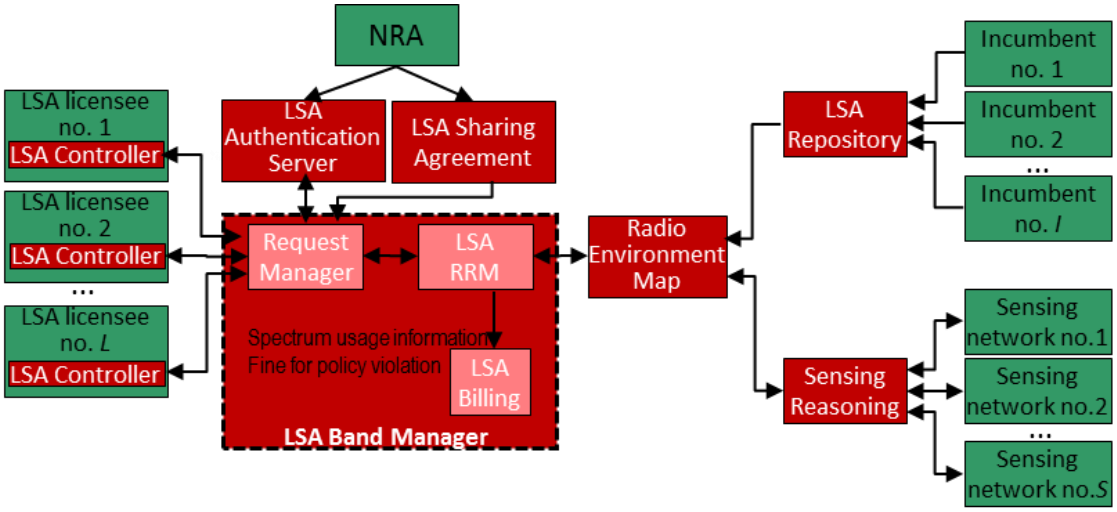


Figure 1: LSA system as proposed by ADEL

In all these modules, there is the risk of steal of ID's, unauthorized access, data adulteration, service degradation and unpredicted module shutdown. To minimize these risks, we propose to link the network modules using a virtual private network (VPN), and

to run NRA-certified software in all of these modules. In the next table we list the type of threats that all the modules may face, and which are not LSA-specific.

Table 1: Non-LSA violations that may be originated by any module

Non-LSA threat	Solution
External adulteration of the policies and ID's stored in the NRA servers	Only NRA has write permission
Steal of IDs (message interception, ID exposal to unauthorized users)	Encryption
Unauthorized use of stolen valid IDs (IDs of Incumbent, Licensee, Controller, Repository, Map, Sensing Reasoning modules).	Change security keys periodically
Use of invalid IDs	Authentication
Service degradation (intentional message flooding of any module just to degrade operation)	Identify IP address. Shutdown network interface. Inform authorities.
A module goes down	Use redundancy

In the next sections the LSA-specific threats originating in the Licensee, Incumbent and Sensor Networks are going to be described. We assume NRA is not a source of violations.

7.2 Policy conformance in the LSA licensees

To ensure the LSA licensee is aware of the spectrum sharing policies, and their follow-up updates, we propose a mechanism whereby LSA licensees must periodically reconnect to the LSA Band Manager during the period they have spectrum allocated to them. The objective is three-fold:

- LSA Band Manager knows it can order to that licensee to stop using the frequencies, as soon as it might be needed.
- If the connectivity between the LSA licensee and the LSA Band Manager is broken, the LSA licensee software (which must be previously certified by NRA) knows it should stop using those frequencies as soon as possible.
- LSA licensees might provide their location updates, if needed.

Therefore, if anyone detects (through sensing, propagation calculations, complaints, NRA monitoring) the LSA licensee is causing unexpected troubles, the LSA Band will send to the respective LSA licensee an order to stop using that spectrum. Certified LSA licensee's software must respect such type of orders.

In the next table we identify the violations that may be caused by the LSA licensee, how to detect and to correct them.

Table 2: Policy violations caused by the LSA licensees

LSA licensee LSA-threat	Detection method	Correction method
Spectrum request from unknown LSA licensee (ID is not in authentication server)	Contact authentication server	Ignore request
LSA licensee not authorized to request spectrum in that band/time/area	Compare with policies	Refuse request
LSA licensee request placed with insufficient antecedence	Compare with policies	Refuse request
LSA licensee requests spectrum with excessive quality (e.g. C/N, C/I,…above pre-defined level) that avoids other Licensees to share it.	Compare with policies	Refuse request
LSA licensee provide inaccurate hardware details (spectrum usage not coherent with TX characteristics: location, power, antenna height or orientation)	Complaint; NRA monitoring; Use sensing	Command to cease transmission
LSA licensee is using a radio technology that is causing interference (e.g. spectral contents outside authorized transmission mask)	Complaint; NRA monitoring; Use sensing;	Command to cease transmission.
LSA licensee requests spectrum with no intention to use part/all of it	Complaint; NRA monitoring; Use sensing;	Change assignment
LSA licensee uses spectrum not assigned to him ever/anymore.	Complaint; NRA monitoring; Use sensing;	Command to cease transmission.
LSA licensee using LSA spectrum failed the periodic contact to the LSA Band Manager	LSA Licensee software detection	LSA Licensee software ceases transmission automatically
LSA licensee does not respect command to cease transmission (i.e. licensee did not stop emissions after a pre-defined time interval)	LSA Band Manager complaint; NRA monitoring; Use Sensing,	Mark in the REM that spectrum as unusable; Reissue command to cease transmission; Notify NRA.

7.3 Policy conformance in the LSA incumbent

There should be no mandatory policy conformance mechanisms for the incumbent: it should behave properly, as if it was not sharing the band, not causing harmful out-of-band interference. If anyone detects (through sensing, propagation calculations, complaints, NRA monitoring) the Incumbent is abusing in the utilization of the spectrum, they inform the NRA, that then acts as in any other non-LSA system.

In alternative, upon agreement, the incumbent, especially those that are moving like PMSE cameras, may accept to follow the same 'connectivity check' procedure as the LSA licensee, in order to be able to send location updates to, and accept 'reconfiguration command' from, the LSA Band Manager. This solution implies installing NRA-certified software in the incumbent, to make sure it will perform periodic contacts with the band manager when it is using the spectrum, and stops using the spectrum if this connectivity is broken.

The incumbent spectrum sharing violations are similar to the ones listed for the LSA licensees, as shown in the table below (differences between the LSA licensee violations and the Incumbent violations are indicated in blue).

Table 3: Policy violations caused by the Incumbents (in blue are the differences relative to the Licensee situation)

Incumbent LSA-threat	Detection method	Correction method
Incumbent accesses spectrum without sending a notification to the LSA repository	LSA licensee complaint; NRA monitoring; Spectrum sensing;	NRA and/or Band Manager informs the incumbent it has to notify the LSA repository
Spectrum access notification sent from unknown incumbent	Contact authentication server	Ignore notification
Incumbent is not authorized to use spectrum in that band/time/area	Compare with policies	Refuse notification
Incumbent notification has unsufficient details	Compare with policies	Refuse notification;
Incumbent notification placed with insufficient antecedence	Compare with policies	Refuse notification
Incumbent notifies it wants to access spectrum with excessive quality (e.g. C/N, C/I,…above pre-defined level) that avoids Licensees to share it.	Compare with policies	Refuse notification

Incumbent LSA-threat	Detection method	Correction method
Incumbent provides inaccurate hardware details (spectrum usage not coherent with TX characteristics: location, power, antenna height or orientation)	Complaint; NRA monitoring; Use sensing	Command to reconfigure transmission (optional); Notify NRA
Incumbent is using a radio technology that is causing interference (e.g. spectral contents outside authorized transmission mask)	Complaint; NRA monitoring; Use sensing;	Command to reconfigure transmission (optional); Notify NRA
Incumbent licensee notifies it is going to access spectrum, but does not use part/all of it	Complaint; NRA monitoring; Use sensing;	Change assignment
Incumbent uses spectrum not assigned to him ever/anymore.	Complaint; NRA monitoring; Use sensing;	Command to reconfigure transmission (optional); Notify NRA
Incumbent using LSA spectrum failed the periodic contact to the LSA Band Manager (optional)	Incumbent software detection	Incumbent software ceases transmission Automatically
Incumbent does not respect command to reconfigure transmission (i.e. incumbent did not reconfigure emissions after a pre-defined time interval) (optional)	LSA Band Manager complaint; NRA monitoring; Use Sensing,	Mark in the REM that spectrum as unusable; Reissue command to reconfigure transmission; Notify NRA.

The difference is that the LSA Band Manager, which behaves as the policy enforcement module, has to collect information from the REM and the repository to inspect if the incumbent is requesting access to the correct part of the spectrum.

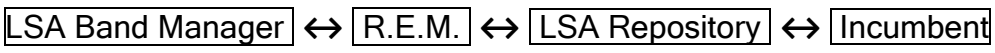


Figure 2: Links connecting the LSA band Manager to the Incumbent

7.4 Policy conformance in the sensing networks

In ADEL, each the sensing networks may be composed by up three hierarchical groups of modules, which are, from bottom to upper level: sensors, concentrators and aggregators. As may be more than one such sensing network attached to the LSA system, the several networks are coordinated by a single spectrum sensing reasoning module, which also behaves as interface with the LSA system.

To ensure the sensing networks are not causing spectrum sharing violations by intentionally or unintentionally providing wrong measurements, we propose a mechanism whereby the sensing networks are periodically instructed to measure a reference/pilot signal, transmitted from known locations at variable carrier frequencies. These measurements will be used both for calibration of sensors and fault detection purposes.

In addition, the measurements provided by the spectrum sensors should pass a set of sanity checks before being used to compute a final result, which could be, e.g. comparing the experimental values with the theoretical bounds, or comparing measurements from nearby sensors to detect abnormalities.

At the same time, the spectrum sensing reasoning module should collect, for each sensing network, reliability/performance metrics along the time to use as weights for future measurements.

In the case of violations caused by the sensing networks the policy enforcement module, i.e. the LSA Band Manager, has indirect knowledge of these violations as it is not directly connected to the sensing networks.

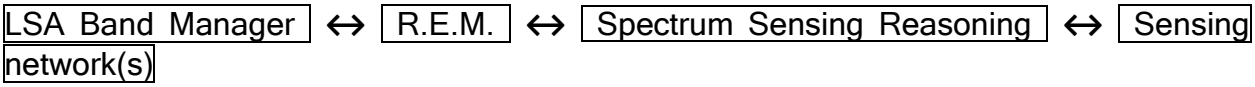


Figure 3: Links connecting the LSA band Manager to the sensing networks

As a result, it may take longer to react to this type of policy violations. This is highly undesirable because ADEL relies on spectrum sensing to react quickly to changes in the radio environment. To solve this problem, without having to change the system architecture, the LSA Band manager should delegate in the Reasoning module to run violation checks every T_1 seconds, and then the LSA Band Manager will check the Spectrum Sensing Reasoning module every T_2 seconds, with $T_2 >> T_1$.

8 Misbehavior Detection for Spectrum Sharing Policy Reinforcement

Consider a CR network composed of a known number N_I of Incumbent Users (IUs) and N_L Licensee Users (LUs). The IU network is composed of transmitters and receivers, which are also used as sensors. All users are located in a square geographical area A that is divided into smaller square cells (grid $M \times M$). It is also assumed that the grid is fine, so that each IU cannot be located in more than one of these cells. However, a LU can be found in a cell where the IU is either present or absent. Furthermore, it is assumed that: a) the number of the LUs is much smaller than the size of the grid (this can be always accomplished with a finer segmentation of the grid) and b) the environment is static, in the sense that the channels between each cell do not change significantly over time (a small sampling period). In principal, the locations of the LU transmitters are unknown; however, if we assume that are known and fixed the identity of the LUs could be uniquely identified. The goal of the IU's sensing network is the detection of all LU transmissions in the geographical area that is under the control of the IU according to the licensed shared access (LSA) agreed policy. If unauthorised licensee user transmissions are detected a penalty is imposed on the misbehaving licensees. An unauthorised transmission is a transmission that violates the agreed spectrum sharing rules in the temporal, spatial, or spectral domains.

The task of detecting unauthorised transmissions reflects to the ability of a method to successfully locate the source(s) of transmissions, and therefore identify the LUs that violate the agreement policy. Thereafter, the band-manager or regulator, which has gained knowledge of the band occupancy based on the detection process penalises the users that misbehave. Thus, the detection is characterized by: a) locating the LU that violates the agreement policy and b) estimating the severity of the violation (e.g., transmitting power) for each LU over a specific period and at a specific band over the geographical area A. Basic sensing techniques have previously been used for detection of transmission source location, based on Angle of arrival information or RSSI estimation [Peng2006, Pap2008]. However, these solutions are prone to errors due to channel propagation effects, such as the attenuation of transmission signals due to pathloss. As a result, these methods can lead to increased probability of false alarm, the probability to erroneously detect a LU as transmitting, which would lead to unfair penalisation of Licensee users. Thus, in order to establish a robust misbehaviour detection procedure, prior knowledge of the channel is required. As a matter of fact, the channels could be estimated/learnt periodically, since we have assumed a relatively static environment. In the following, we consider that the channels are known over a specific sampling time period T_s.

Let the channel gain from the location of the k-th LU to an IU receiver/sensor n be $\boldsymbol{g}_{n,k} = \boldsymbol{g}_n \in \mathbb{C}^{M^2}$ and $\boldsymbol{r}_{n,k}$ is the respective pathloss attenuation vector with values equal to d^{-a}, where d is the distance between the source and the receiver and a corresponds

to a propagation constant; a typical choice for its selection in an urban environment is between 2.5 and 3.7 (here we let $a = 3$). Hence, the channel between the k-th LU and the n-th IU sensor is considered as $\mathbf{h}_n = \boldsymbol{r}_{n,k} \circ \boldsymbol{g}_{n,k}$, where the symbol "$\circ$" denotes the Hadamard product between the vectors. Moreover, it is assumed that:

- The channel gains $\boldsymbol{g}_n$ are i.i.d. random variables with a bounded positive definite covariance matrix (thus $\mathbf{h}_n$ is also a random variable).

Let the transmitted signal sample from the k-th LU be $\mathrm{x}_k(t) \in \mathbb{C}, t = 1,\ldots,T_s$. Since the number of the LUs is much smaller than the number of all possible locations over the area A ($N_L \ll M^2$), the transmitted signal from all LUs is modelled as a *sparse* vector denoted by $\mathbf{x}_*(t)$. We assume that within the sampling time period T_s the number, of LU transmitters, N_L, and thus the support S of the sparse vector $\mathbf{x}_*(t)$ remains unchanged.

The signal sample received at each IU n-th sensor is assumed of the linear form:

$$\mathrm{y}_n(t) = \mathbf{h}_n^{\mathrm{T}}\mathbf{x}_*(t) + \mathrm{v}_n(t),\ n = 1,\ldots,N_I, \tag{1}$$

where $\mathrm{v}_n(t)$ are assumed i.i.d. random variables with zero mean and bounded variance, uncorrelated with $\boldsymbol{g}_n$.

Equation (1) can be written in a more compact form as

$$\mathbf{y}(t) = \mathbf{H}\mathbf{x}_*(t) + \mathbf{v}(t), \tag{2}$$

where $\mathbf{y}(t) = [\mathrm{y}_1(t),\ldots,\mathrm{y}_{N_I}(t)]^{\mathrm{T}}$, $\mathbf{H}^{\mathrm{T}} = [\mathbf{h}_1\ \mathbf{h}_2 \ldots \mathbf{h}_{N_I}]$ and $\mathbf{v}(t) = [\mathrm{v}_1(t),\ldots,\mathrm{v}_{N_I}(t)]^{\mathrm{T}}$.

In order to successfully perform the detection of LU transmissions and fairly penalise / reward the respective LUs, our goal is to recover both the support of the sparse vector $\mathbf{x}_*$ (which denotes the location of the transmitters), but also estimate its values over the fixed sampling time period T_S (which denote the transmitted signals of the identified transmitters). In addition, in order to correctly identify the activity of a LU (non-transmitting- $\mathcal{H}_0$ or transmitting- $\mathcal{H}_1$), a standard energy detector (other detectors are also applicable) is used on the estimated/received signal $\hat{\mathbf{x}}(t)$:

$$E_k = \frac{1}{T_s}\sum_{t=1}^{T} |\,\hat{\mathrm{x}}_k(t)\,|^2 \ \begin{matrix}\mathcal{H}_1\\ \geq \\ \leq \\ \mathcal{H}_0\end{matrix}\ \tau_{ed}(k) \tag{3}$$

where $\tau_{ed}(k)$ is a model defined threshold which depends on the agreed power transmission levels for each LU. In the simplest scenario, where no transmissions are authorized by the IU $\tau_{ed}(k)$ is set at the noise level for all LUs. If the estimated signal is not sparse then we have an increased probability of false alarm, resulting to an unfair penalisation of the LU. Furthermore, a poor estimation of the signal could also lead to

the erroneous classification of the activity of a LU. Since the Least-Squares method produces a non-sparse solution, we resort to sparse optimisation methods.

Sparsity-aware learning and related optimisation techniques have been at the forefront of the research in signal processing, encompassing a wide range of topics, such as compressed sensing, de-noising and signal approximation techniques. There are two major paths, towards modelling sparse vectors/signals. The first one, focuses on minimising the ℓ_0 (pseudo)-norm of a vector which equals the number of non-zero coordinates of a vector (this is a non-convex function). Thus, the resulting minimisation task is the following:

$$\min_{\mathbf{x}(t)} \| \mathbf{x}(t) \|_0 \text{ s. t. } \left\| \mathbf{y}(t) - \mathbf{H}\mathbf{x}(t) \right\|_2 \leq \varepsilon, t = 1,2,..., \quad (4)$$

However, the cost function in (4) is non-convex; moreover, the optimisation task is known to be NP-hard (combinatorial). As an alternative path, a preferable and nowadays standard technique is to minimize the ℓ_1-norm of the unknown sparse vector, which is the closest convex relaxation to the ℓ_0 -norm and also generates sparse representatrions. Instead of using a formulation similar to (4), its unconstrained formulation is often considered, which is known as the Least Absolute Shrinkage and Selection Operator (LASSO) [Tibshirani1996, Kim2007, Beck2009, Boyd2010], i.e.,

$$\min_{\mathbf{x}(t)} \left\{ \frac{1}{2} \left\| \mathbf{y}(t) - \mathbf{H}\mathbf{x}(t) \right\|_2^2 + \lambda \left\| \mathbf{x}(t) \right\|_1 \right\}, t = 1,2,..., \quad (5)$$

where $\lambda > 0$ is a regularisation constant that controls the sparsity level of the vector $\mathbf{x}(t)$.

The optimization task in (5) is solvable with a variety of methods; however, among the most popular are the Alternating Direction Method of Multipliers (ADMM), the Homotopy method [Osbourne2000], the FISTA [Beck2009] or the FLEXA [Facchinei2015]. Although the cost function that is minimised is convex the non-differentiable term (ℓ_1-norm) is the reason for slow convergence for the majority of the aforementioned methods. More recently, a state-of-the-art line search method has been proposed for non-differentiable optimization problems within the ADEL project [ADEL D5.2]. The so-called Soft-Thresholding with simplified Exact Line search Algorithm (STELA), which also handles a more general class of minimization tasks, offers good approximation properties, whilst offering computational advantages against its competitors in terms of cost. This is very important in many Cognitive Radio (CR) environments, since transmission operations are extremely fast, imposing time constraints for successful detections. Since the STELA method is applicable for the LASSO task Yang et. al managed to successfully apply the method as an alternative to solve (5) [Yang2014, Yang2016].

However, the optimization task in (5) does not satisfy the “oracle properties” as shown by Fan and Li [Fan2001]. To this end, Zou proposed the Adaptive LASSO task [Zou2006], which assigns weights to different coefficients:

$$\hat{\mathbf{x}}(t) := \arg\min_{\mathbf{x}(t)} \left\{ \frac{1}{2} \left\| \mathbf{y}(t) - \mathbf{H}\mathbf{x}(t) \right\|_2^2 + \lambda \left\| \mathbf{W}\mathbf{x}(t) \right\|_1 \right\}, \quad (6)$$

where $\mathbf{W}$ is a diagonal matrix with weights

$$\mathrm{w}_{jj} = \frac{1}{\left|\hat{\mathrm{x}}_j^{(LS)}(t)\right|^{\gamma}},\ j = 1,\ldots,\mathrm{M}^2 \tag{7}$$

where $\hat{\mathbf{x}}^{(LS)}(t)$ is the Least-Squares solution and $\gamma > 0$. Although the task in (6) enjoys better statistical properties (oracle), it still suffers from slow convergence if solved with a standard technique such as the ADMM algorithm.

Another approach is to use the log-penalised estimator term in (5), i.e.,

$$\min_{\mathbf{x}(t)} \left\{ \frac{1}{2}\left\|\mathbf{y}(t) - \mathbf{H}\mathbf{x}(t)\right\|_2^2 + \lambda \sum_{j=1}^{\mathrm{M}^2} \log\left(\left|\mathrm{x}_j(t)\right| + \varepsilon\right) \right\},\ t = 1,2,\ldots, \tag{8}$$

And by taking a first-order Taylor-series approximation of the logarithm penalty about the current value, we obtain the over-approximation of (8),

$$\hat{\mathbf{x}}^{(i)}(t) := \arg\min_{\mathbf{x}(t)} \left\{ \frac{1}{2}\left\|\mathbf{y}(t) - \mathbf{H}\mathbf{x}(t)\right\|_2^2 + \lambda \sum_{j=1}^{\mathrm{M}^2} \mathrm{w}_{jj}^{(i-1)} \left|\mathrm{x}_j(t)\right| \right\},\ t = 1,2,\ldots,\ i = 1,\ldots, \tag{9}$$

$$\mathbf{w}_{jj}^{(i-1)} = \frac{1}{\left|\hat{\boldsymbol{x}}_j^{(i-1)}(t)\right| + \boldsymbol{\varepsilon}},\ \hat{\boldsymbol{x}}_j^{(0)}(t) = \mathbf{0}, \tag{10}$$

which is also known as the Iteratively Reweighted LASSO (IRWL). The linear approximation in (9), which is also proposed in [Johnson2015], is analogous to the one proposed in [Zou2008], except that the authors there did not make use of the perturbation $\boldsymbol{\varepsilon}$ in (10) and they argued strongly in favour of a on-step approximation (see equation (6)). In order to solve the task in (9) efficiently and with minimal computational cost, we propose the STELA method for the IRWL task, which is straightforwardly applicable with a fixe weight matrix $\mathbf{W}$.

However, we propose a novel version in which the weights are also updated within the STELA iterations with the current estimates. Instead of solving a Weighted LASSO task at every i-th step and updating the weights after the i-th's step solution, we update the weights with each current solution obtained from the successive line search intermediate step of the STELA method. The gain is that the method accelerates in convergence speed, while attaining sparse properties and a very good approximation error. The algorithm is summarised in the following steps, initialising at $\mathbf{x}^{(0)} = \mathbf{0}, w_{jj}^{(0)} = 1$:

For $\tau = 0,1,\ldots$, do:

1. $\mathbf{r}(\mathbf{x}^{(\tau)}) = \mathbf{d}(\mathbf{H}^{\mathrm{T}}\mathbf{H}) \circ \mathbf{x}^{(\tau)} - \mathbf{H}^{\mathrm{T}}(\mathbf{H}\mathbf{x}^{(\tau)} - \mathbf{y}),$

2. $\mathbb{B}_j \mathbf{x}^{(\tau)} = (\mathrm{d}_j(\mathbf{H}^{\mathrm{T}}\mathbf{H}) + \mathrm{c})^{-1} \mathcal{S}_{\lambda \mathrm{w}_{jj}^{(\tau)}}(\mathrm{r}_j(\mathbf{x}^{(\tau)}) + \mathrm{c}x_j^{(\tau)}),\ j = 1,\ldots,\mathrm{M}^2$

3. $\gamma^{(\tau)} = \left[-\dfrac{(\mathbf{H}\mathbf{x}^{(\tau)} - \mathbf{y})^{\mathrm{T}}\mathbf{H}(\mathbb{B}\mathbf{x}^{(\tau)} - \mathbf{x}^{(\tau)}) + \lambda\left(\| \mathbf{W}^{(\tau)}\mathbb{B}\mathbf{x}^{(\tau)} \|_1 - \| \mathbf{W}^{(\tau)}\mathbf{x}^{(\tau)} \|_1\right)}{\left(\mathbf{H}(\mathbb{B}\mathbf{x}^{(\tau)} - \mathbf{x})\right)^{\mathrm{T}}\mathbf{H}(\mathbb{B}\mathbf{x}^{(\tau)} - \mathbf{x})} \right]_0^1$

4. $\mathbf{x}^{(\tau+1)} = \mathbf{x}^{(\tau)} + \gamma^{(\tau)}(\mathbb{B}\mathbf{x}^{(\tau)} - \mathbf{x}^{(\tau)})$

5. $\mathbf{w}_{jj}^{(\tau+1)} = \frac{1}{\left| x_j^{(\tau+1)} \right| + 1}, j = 1, \ldots, M^2$

End

Figure 4: Minimisation algorithm

In the algorithm of Figure 4 $\mathbf{d}(\mathbf{H}^{\mathrm{T}}\mathbf{H})$ is the diagonal of the matrix $\mathbf{H}^{\mathrm{T}}\mathbf{H}$, c is a small positive constant, $\mathcal{S}_{\mathrm{a}}(b) := [\mathrm{b} - \mathrm{a}]^{+} - [-\mathrm{b} - \mathrm{a}]^{+}$ is the soft-thresholding operator and $[s]_0^1 := \min(\max(s,0),1)$ denotes the projection of s onto $[0,1]$.

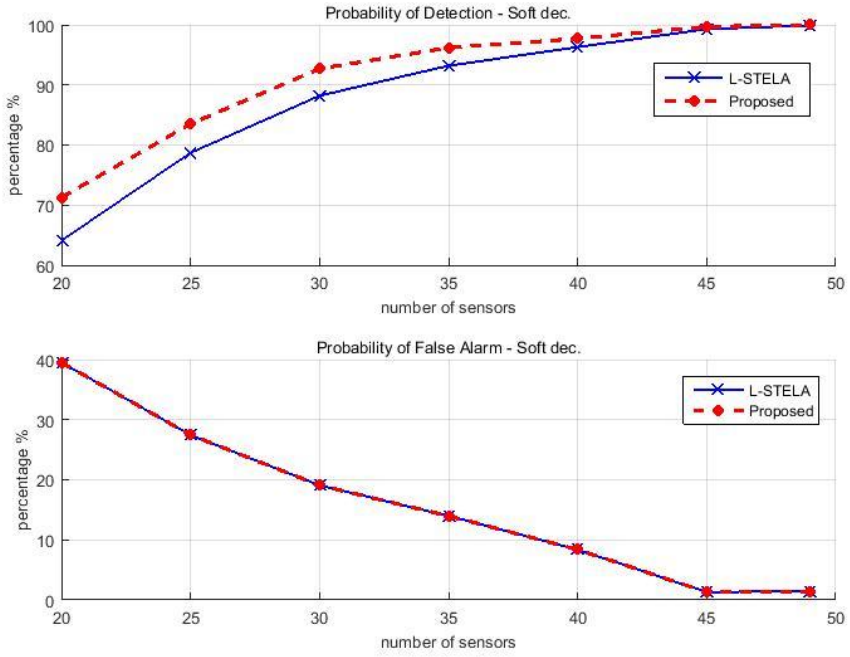
Next, we present the results of the application of the LASSO STELA (L-STELA) and the proposed one to the misbehavior detection task. Finally, various simulation results demonstrate the performance of each method and highlight the advantages of the later method over its predecessor.

8.1 Scenario A: LUs uniformly distributed over the entire grid

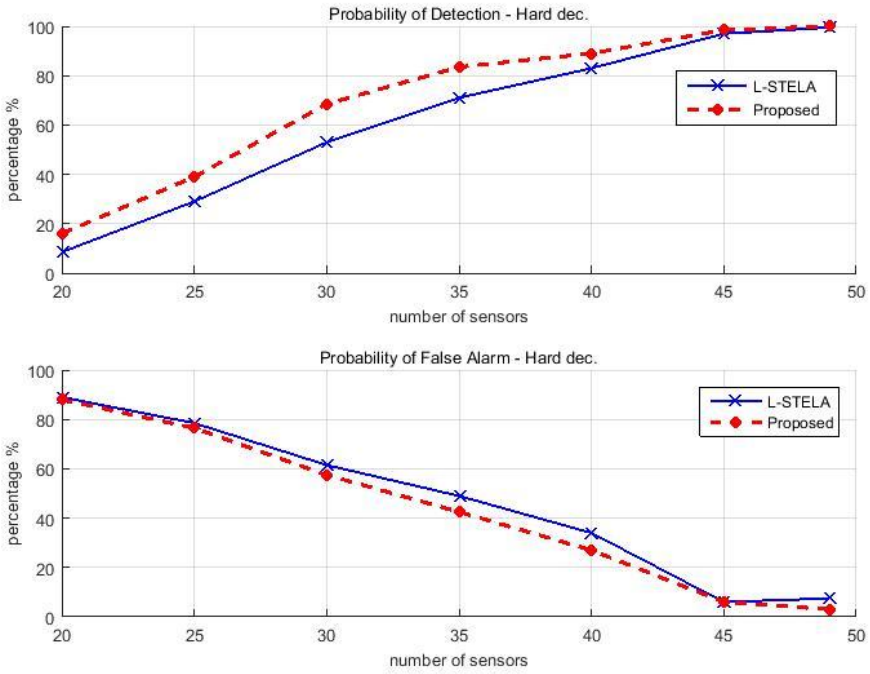
In the first scenario we consider the topology of a 7x7 grid, where 5 LUs (corresponding to 10% of the possible locations) are distributed uniformly at random over the entire grid. Each one of the LU transmits with a fixed power (energy) selected uniformly at random over the interval [60,100]. The vector corresponding to the channel estimates is chosen $\boldsymbol{g}_n \in \mathcal{CN}(0, \mathbf{I})$ and $\mathrm{v}_n(t)$ follows the standard complex Gaussian distribution at an average SNR of 20dB. The distances from each grid to the next are computed according to the Euclidian distance for $d = 1$ between two subsequent cells (on the same row or column) and 0.8 for transmission within the cell. The number of IUs varies between 20 and 49 users chosen at random over the grid, while we have measured the probability of detection and the probability of false alarm in two different ways. By taking a *soft decision* rule, where the detection is measured for each location found with respect to the total number of the true locations and the false alarm by computing the percentage of extra locations which are incorrectly classified as misbehaving LUs. The second decision rule offers a *hard decision*, and the probability of detection is measured on whether all the correct LU transmitter locations have been identified. In the case of the *hard decision*, the probability of false alarm is computed as the percentage for which the system has identified extra (thus incorrectly) locations of a possible transmitting LU. For

all of the experiments the sampling window is chosen at $T_s = 30$ and the results are averaged over 200 independent Monte Carlo runs.

The respective results are depicted in Figure 5. In particular, in (a) is shown the soft decision rule, where we conclude that for each number of IU sensors over the grid and equal probabilities of false alarm, the proposed method attains a higher probability of detection. Of course, the difference between the detection probabilities achieved by the



(a)



(b)

Figure 5: Probabilities of detection and false alarm while varying the number of IU sensors over the grid. (a) using the soft and (b) using the hard decision criterion for the scenario A.

algorithms reduces as the number of sensors increases. In Figure 5 (b) the hard thresholding rule is less forgiving as it imposes stricter criteria for both the detection as well as the false alarm. It is readily seen that although both methods manage well, the proposed method attains both a higher probability of detection and also a lower probability of false alarm.

Moreover, in Figure 6 the relative error between the transmitted energy and the estimated one is shown, where the performance towards estimation is evaluated. As it can be seen the proposed method manages to decrease the estimation error from 10%-30% for certain numbers of IU sensors.

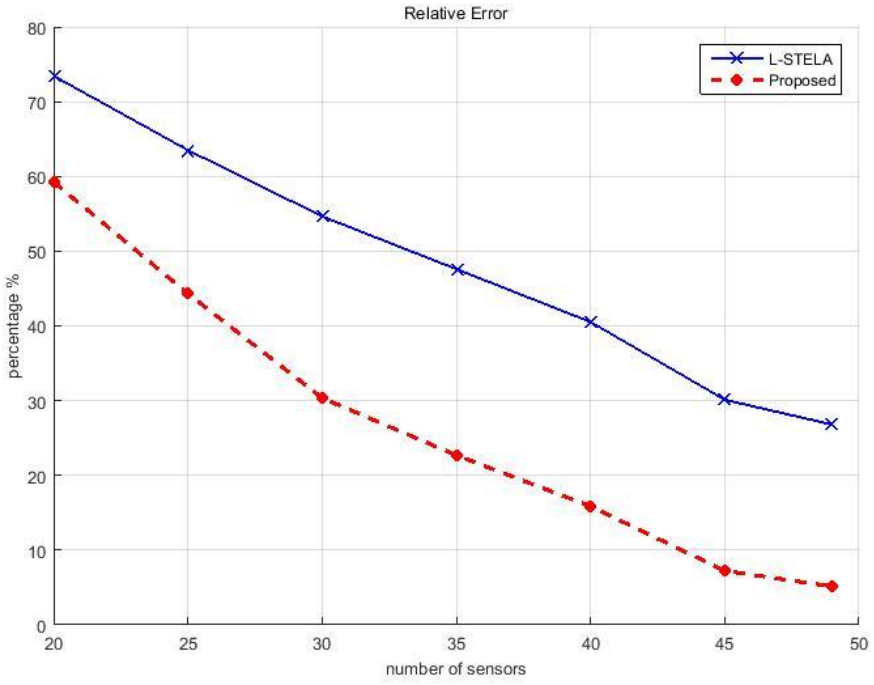
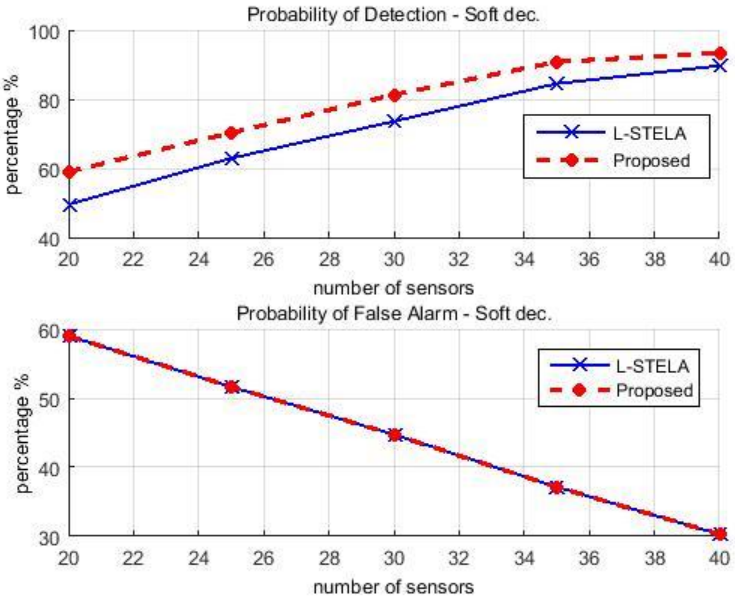


Figure 6: The relative error between the transmitted and the estimated energy while varying the number of sensors over the entire grid.

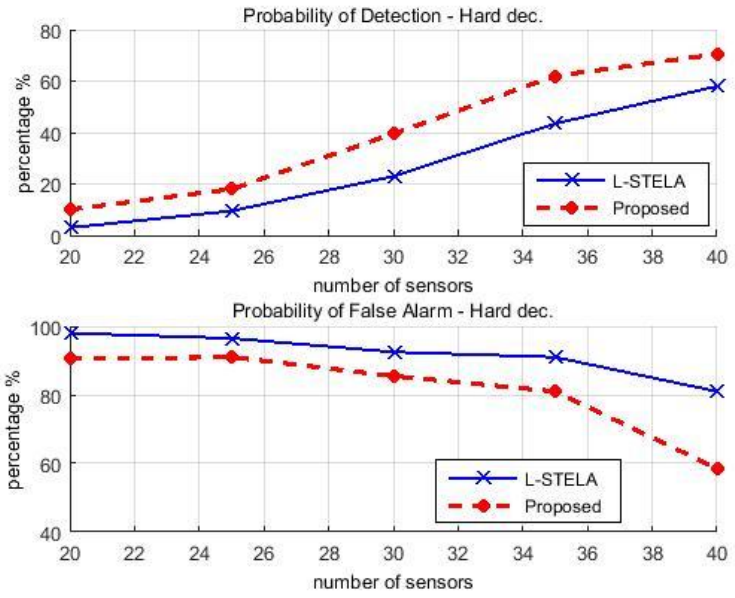
8.2 Scenario B: LUs uniformly distributed in cells where the IU is absent

The second scenario differentiates from the first only in the placement of the 5 LUs, which are only distributed (uniformly at random) in the cells that the IU is absent. Here, we have varied the number of IU sensors between 20 and 40.

In Figure 7 (a), where the soft decision rule is applied, the results are similar to Figure's 1 (a) with the only notable difference being the lower probability of detection and higher probability of false alarm. However, such a result is totally expected, since the sensor is far from the transmission source, thus the task of successful detection is now harder. Also in Figure 7 (b), we observe that the differences for the two methods are even broader. This is also a fact verified by the results in Figure 8, where the relative error of the estimation process is computed for each one number of sensors in the grid.



(a)



(b)

Figure 7: Probabilities of detection and false alarm while varying the number of IU sensors over the grid. (a) using the soft and (b) using the hard decision criterion for the scenario B.

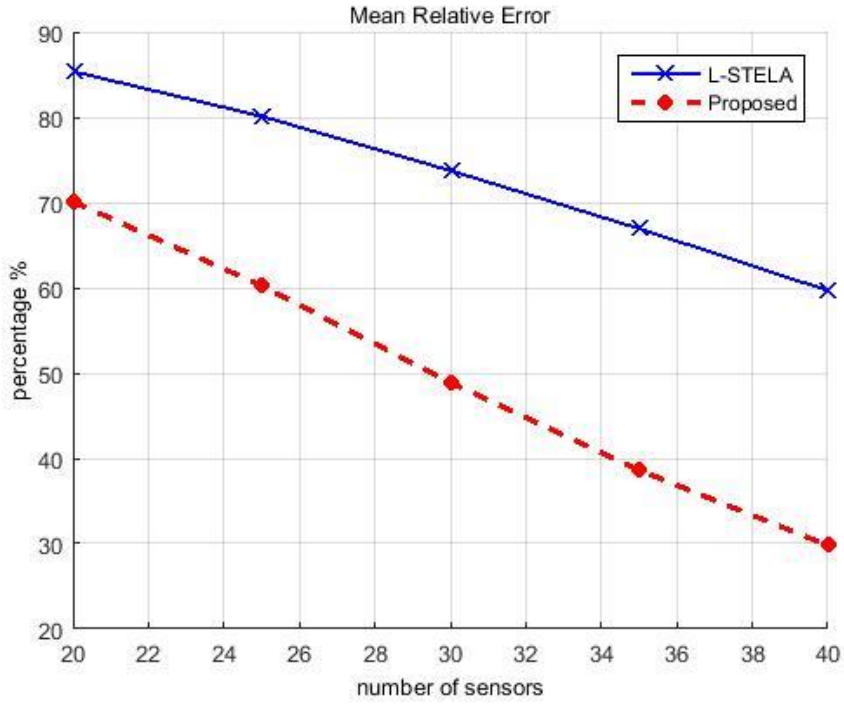
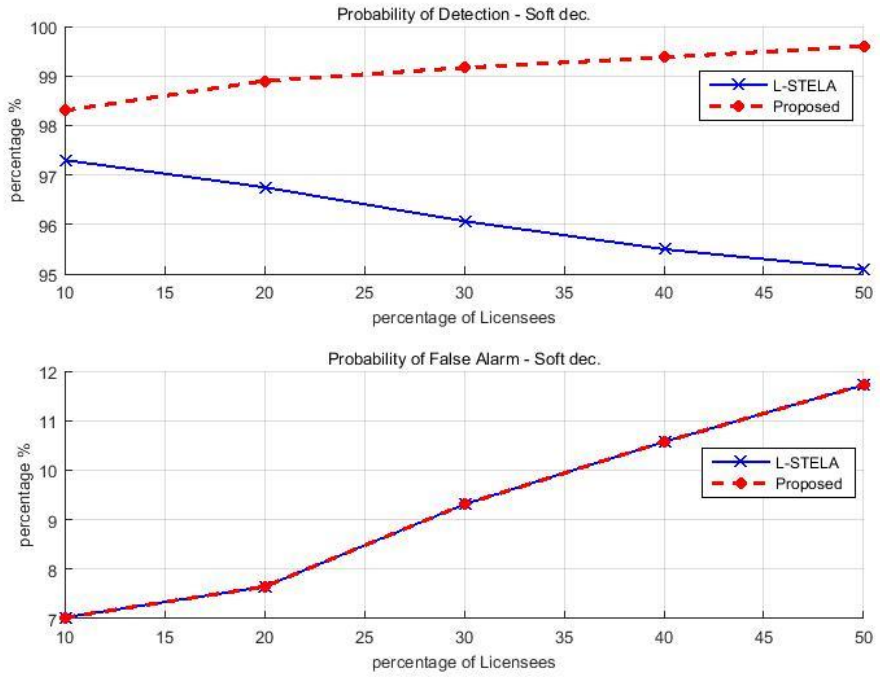


Figure 8: The relative error between the transmitted and the estimated energy while varying the number of sensors over the free cell of the grid.

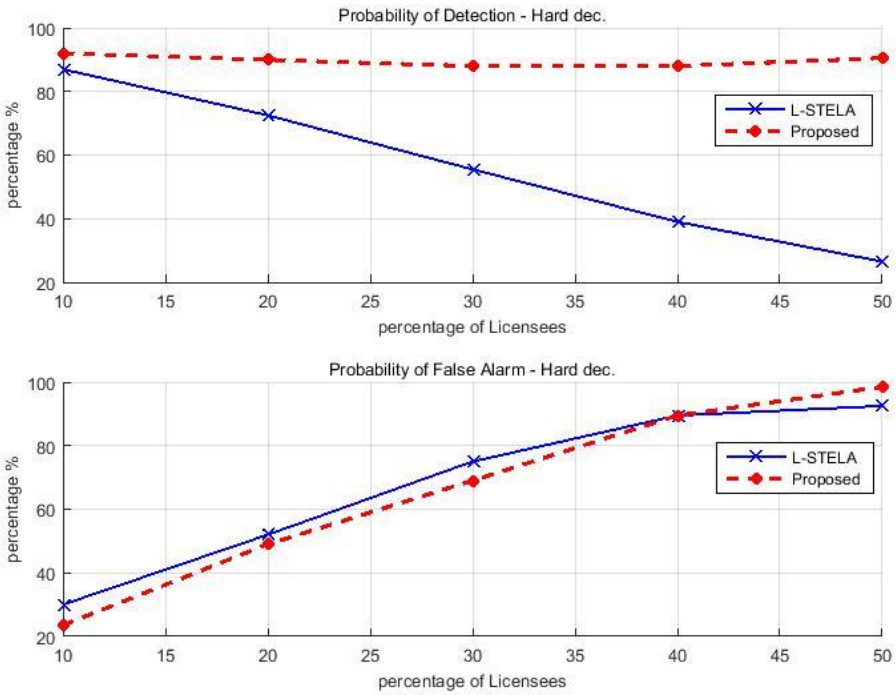
8.3 Evaluation of the method for an increasing number of LUs

The final experiment follows the setup of the first experiment and demonstrates the performance of each method for a fixed number of IU sensors ($N_I = 40$), while varying the number of LUs between 10% and 50% of the size of the grid in random locations (uniformly).

In Figure 9 the probabilities of detection and false alarm are shown. Here, it can be readily seen that the probability of detection is decreasing, while the probability of false alarm increases for an increasing number of LUs. However, one can notice that the proposed method seems preferable for the localisation task. Finally, the gains towards estimation for the proposed algorithm are much more clear, as it is demonstrated in Figure 10.


Probability of Detection - Soft dec.
percentage %
percentage of Licensees
L-STELA
Proposed
Probability of False Alarm - Soft dec.
percentage %
percentage of Licensees
L-STELA
Proposed

(a)


Probability of Detection - Hard dec.
percentage %
percentage of Licensees
L-STELA
Proposed
Probability of False Alarm - Hard dec.
percentage %
percentage of Licensees
L-STELA
Proposed

(b)

Figure 9: Probabilities of detection and false alarm while varying the number of LUs. (a) using the soft and (b) using the hard decision criterion.

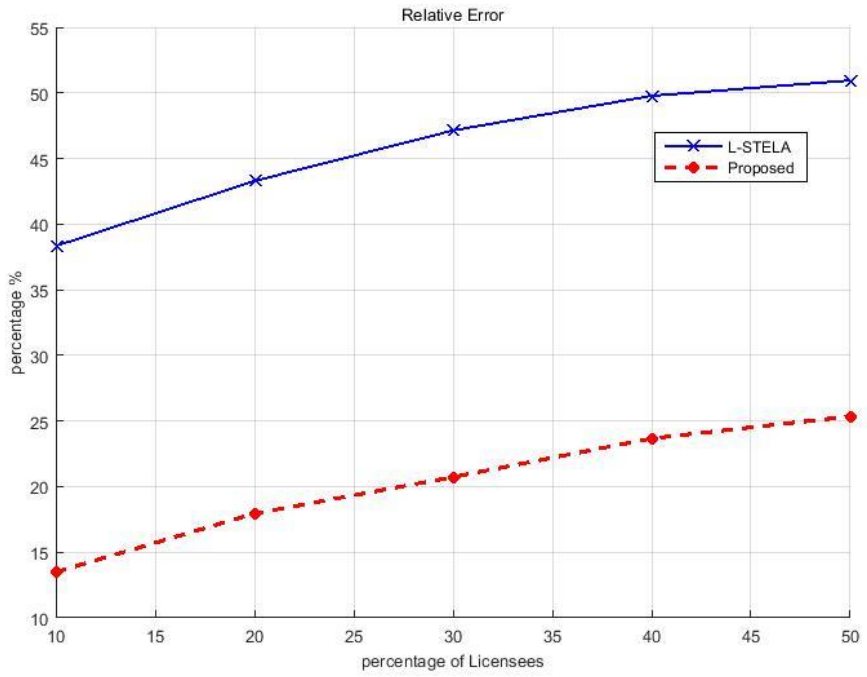


Figure 10: The relative error between the transmitted and the estimated energy while varying the number of LUs.

8.4 Conclusions

In this section we presented an analytical formulation, by exploiting sparse optimization techniques. We have shown that we can detect an arbitrary number of transmitters within a predefined area (grid). This method extends the collaborative sensing methodology developed in ADEL's D5.2 to significantly improve the accuracy and the speed of detection, as well as to reduce the probability of false alarm. Using our model, the Band Manager can identify the Licensee Operators who use shared resources and confirm whether they comply with the LSA rules. The results demonstrate the importance of the number of sensing nodes to correctly detect the transmitters. This raises the issue of incentivising Licensee operators to act as sensing nodes, thus aiding in the detection of misbehaviour.

9 Punishment and Incentives for Policy Enforcement

In this section we propose algorithms to punish misbehaviour, by limiting access to the shared resources for misbehaving nodes, but also to incentivise both the well-behaving of LSA users and the cooperation between users to improve the overall operation of the LSA community.

9.1 Introduction

In Licensed Shared Access (LSA) an incumbent operator gives access to other Licensee operators to use its spectrum under the rules of the "LSA agreement". The ADEL architecture, identifies the LSA Band Manager as the central function that allocates the available resources to the LSA licensees (see Figure 1 for reference).

The smooth operation of spectrum sharing requires the involved parties to develop trust between them that the rules of the LSA agreement are honoured, giving incentives to the incumbent to continue sharing its allocated spectrum without worrying that its fundamental business may be affected.

However, absent any control and monitoring, the selfish LSA agreement parties may have incentives to misbehave and violate the rules of the LSA agreement to maximise their own utility function. In the ADEL architecture both the Incumbent and the Licensee Operators can act as both active spectrum users and as passive sensing nodes. In addition, the ADEL architecture allows a special category of players who are only sensing. These nodes can be part of the Incumbent's infrastructure, belong to the NRA, or be independent players who provide the sensing service to the LSA community for some reward. The Band Manager is responsible to collect and process the information from the sensor nodes that allows it to detect misbehaviour. It then has to create the right mixture of penalties and rewards to promote collaboration between the parties and adhering to the LSA rules.

9.1.1 LSA party misbehaviour

While the ADEL system specifies protocols that aim to maximise the system-wide utility (e.g., high aggregate resources utilisation, and fairness), selfish operators try to maximize their own utility, usually impeding the utility of other LSA operators, or the incumbent, and therefore the complete ecosystem's social welfare.

Node misbehaviour under the cognitive radio concept has been considered in the literature. A comprehensive summary of possible attacks to a cognitive radio system is provided in [Ark2010] The authors review the different steps in requesting and granting spectrum access in a hypothetical cognitive radio system and identify actions which malicious or selfish nodes could take to disturb and/or improve their own utility against that of the cognitive radio community. The majority of the identified attacks relate to obstructing the communication between the spectrum licensees and the auctioneer, or

bypassing authentication systems to present false credentials to the controlling entity which opens the way to malicious manipulation of the decision making centre. Similarly, [Park2014] reviews the threats present in "Sensing-Driven" and "Database-Driven" Spectrum Sharing architectures. Emphasis is given on attacks that aim to compromise the privacy of either the Primary User or the Secondary User, or the access to the shared database. The authors then present possible *ex ante* (preventive) and *ex post* (punitive) measures to enforce compliance with the shared access agreements. The preventive measures focus on protecting the devices' software and hardware layers from tampering with, while the punitive measures aim to identify the misbehaving users and punish them with either (i) exclusion from shared access, or (ii) by imposing financial penalties.

9.1.2 Definition of misbehaviour

It is important to first understand what constitutes misbehaviour under the LSA paradigm. The shared resources span across four dimensions;

- The **time period** during which an allocation is scheduled;
- The **spectrum** that will be used by the licensee;
- The maximum **power** that the licensee is allowed to transmit at; and,
- The **geographic area** that the licensee will serve during the allocation period.

Abusing the use of any of the above resources constitutes misbehaviour and in the rest of our analysis we do not distinguish explicitly between the different types of resources. A malicious party would try to benefit by abusing the use of its allocated resources, either by exceeding the allowed use, or by requesting unnecessary resources to hamper competition.

It should be noted that failure to comply with the LSA agreement rules is not always intentional. Hardware and software failures may lead to misbehaviour without any underlying intention from the Licensee to benefit beyond what is offered through the LSA agreement. While unintentional misbehaviour raises concern and needs to be identified and treated, the magnitude of the applied punishment may be different to that applied for intentional misbehaviour. At the same time, it is likely that unintentional misbehaviour would arise more sporadically and would be corrected as soon as the misbehaving player is notified.

9.1.3 Types of node or LSA party misbehaviour

9.1.3.1 Exceeding allowed use

An LSA party may choose to use its allocated resources beyond the level agreed. This applies to all the dimensions of spectrum allocation, described above. So, the LSA party may decide to not release the spectrum at the agreed time, it may use (or interfere with) more spectrum than allocated, it may use higher transmission power than allowed, or it may use the spectrum in a different geographic region than what it is expected to. As mentioned above, exceeding the allowed use limits is not always due to intentional misbehaviour, but could be due to system errors. For example, using more spectrum

than agreed may be due to inadequate band-pass filters at the transmitter, or intermodulation due to structural damage. Similarly, if the Licensee is using the allocated resources in the wrong geographical area, it may be due to errors in its geolocation database.

9.1.3.2 Misusing the allocated resources

A malicious operator may reserve resources it does not need in order to constrain the ability of other operators to compete. While this type of misbehaviour does not lead to interference, it is still malicious and intentional as it is against the spirit of LSA and spectrum sharing and reduces the overall utility of the spectrum sharing community. The problem can become more aggravated in areas where the available resources are scarce while there are many Licensees contending for the same resources.

9.1.4 Detection of misbehaviour

The first step in dealing with non-compliance with the LSA agreement rules is to successfully detect it.

9.1.4.1 Spectrum monitoring performed by National Regulatory Authorities (NRAs)

Traditionally, NRAs are responsible for monitoring the radiowaves and enforcing spectrum licensing and policies. For this reason, NRAs deploy spectrum sensing infrastructure at national and regional levels. For example, the UK Telecoms Regulator (Ofcom) describes in [Ofcom] the spectrum sensing facilities it has deployed in the UK. These allow Ofcom to detect transmissions in the 9kHz to 3GHz range across the country and identify the source's location. However, the detection process can be long. It involves the use of a number of Unattended Monitoring Systems (for frequencies above 20MHz), primarily deployed in areas where spectrum usage is high, such as town and city centres, which measure spectrum usage and report it to Ofcom's headquarters daily, as well as a network of Remote Monitoring and Direction Finding Systems (RMDF) which provide monitoring and direction finding capabilities. The RMDF system is used for investigating interference complaints. If the location of the interferer cannot be identified, transportable monitoring systems can be deployed, or field monitoring vans can be sent to the area where interference is reported. It is obvious that this is largely a manual procedure which can be both time consuming and costly and therefore not always appropriate for the requirements of LSA enforcement.

9.1.4.2 Distributed sensing from LSA players

The ADEL architecture (Figure 1) defines the presence of sensing networks. These can be parts of the Incumbent's or the Licensee operators' networks, or can be separate entities that offer spectrum sensing as a service. It is therefore expected that sensing-capable devices will be deployed in areas with LSA activity. More importantly, it is expected that the density of sensing devices will be higher in areas of increased interest

from Licensee operators. By collecting sensing information from the LSA sensing networks and provided that the location of the Licensee who is granted access to the shared spectrum is known, the LSA Controller can identify the location of the interferer, and from this its identity.

In Section 8 we proposed an efficient and effective algorithm that allows the Band Manager to identify the location (and therefore the identity) of transmitting LSA users, as well as estimate their transmission power. By periodically collecting sensing information across all the shared bands, and by comparing the identities of the active transmitters against its resource allocation database the Band Manager can identify misbehaviour in the time, spectrum, and power domains.

9.2 Fairplay-driven Resource Allocation for LSA

In order to incentivise compliance with the spectrum sharing rules we propose the use of a ranking system to monitor the behaviour of the LSA parties. Each LSA party's score is maintained in the database and is used to decide which LO should be allocated the available resources, as well as the temporal duration of the allocation. The ranking system must have the following qualities:

- Punish misbehaviour;
- reward compliance with the LSA agreements;
- promote collaborative detection of misbehaving parties;
- promote the efficient use of shared resources; and,
- forgive parties that, while they have misbehaved in the past, have demonstrated change in their stance and compliance with the LSA agreements.

In addition, the ranking system should consider the scarcity (or popularity) of resources in different geographic areas, and the type of incumbent operator, weighting the punishment or rewards, accordingly.

We propose that the LSA controller maintains a rank (R_k) for each licensee k with

$$R_k = \sum_{i=0}^{n} a_{k,i} \cdot e^{-\frac{t-t_i}{b_{k,i}}}$$

where $a_{k,i}$ and $b_{k,i}$ represent the magnitude and the temporal effect of the penalty or reward of event i from licensee k, respectively, while t_i is the time at which the penalty or reward was applied. $a_{k,i}$ takes negative values for penalties and positive for rewards.

Both $a_{k,i}$ and $b_{k,i}$ are functions of the type of misbehaviour, the demand for the resources that were misused, weights applied by the incumbent operator representing the incumbent's detriment from the LSA violation, as well as weights representing the longer term behaviour of the licensee.

The rate (R_k) of the licensee affects its ability to reserve the resources it wants, when other licensees are also interested in using the same resources. We identify four distinct ways the LSA Controller may choose how to allocate the shared resources:

- **Deterministic** – the LSA controller has *n* resource blocks available for allocation and chooses to allocate them to the *n* higher ranked licensees. This is the stricter resource allocation approach as it can lead to outright exclusion of malicious licensees in areas of high demand. On the other hand, it gives the highest rewards to those operators who contribute more to the common utility, for example those who collect rewards by releasing resources timely, or those who spend more effort in detecting malicious interferers.

- **Probabilistic** – when multiple licensees are contending for the same resources, the LSA Controller may choose randomly who to allocate the resources to. The contention probability of each contestant is a function of the rate (R_k) and is calculated using the equation:

$$p_k = \frac{c^{R_k}}{\sum_{i=1}^{K} c^{R_i}}$$

,where the parameter $c > 1$ determines the spread between the access granting probability between the K access seekers.

- **Rank-proportional allocation** – the licensee can only be allocated a fraction of the available resources. The maximum amount of resources (S_k) licensee k can be granted is given by the equation:

$$S_k = \frac{S_T c^{R_k}}{\sum_{i=1}^{K} c^{R_i}}$$

, where S_T is the total amount of resources available for all the access seekers. In this case, the allocation procedure is iterative since more than one access seekers are allocated resources. If, after the first round there are still resources available for allocation the allocation process is repeated for the available resources, and so on, until all the resources are allocated or there are no more access requests. In the long term, the effect of this allocation policy is the same with the effect of the probabilistic allocation.

- **Delayed access** – In this allocation approach, a delay d_k in serving a request for resources is added, depending on the rank of the Licensee. This way, LOs with lower rank are effectively given priority, but also misbehaving nodes are punished regardless on whether there are other requests for the same resources. The access delay for LO k is given by:

$$d_k = \begin{cases} -R_k t_p & , R_k < 0 \\ 0 & , R_k \geq 0 \end{cases}$$

,where t_p is the delay penalty time unit. This allocation approach is similar to the deterministic one, in that the resources are allocated to the access seekers with

the highest rank, but it has no effect on Licensees who have positive rank due to rewards. Also, this resource allocation approach may lead to resources being unused and therefore does not promote the overall more efficient use of resources.

9.2.1 Simulation results

We compare the different allocation policies by comparing the allocation of resources to five different access seekers, each having a different probability of being punished, or rewarded for its behaviour. Table 4 summarises the probability each user may misbehave, or be rewarded in each resource allocation period.

Table 4: Probabilities to misbehave and be rewarded for the simulated access seekers

User	Probability to misbehave	Probability to be rewarded
1	1	0.2
2	0.1	0.1
3	0.2	0.1
4	0.3	0.2
5	0.4	0

9.2.1.1 Deterministic allocation of resources

Figure 11 shows the result of the Deterministic resource allocation. In this case only the users with the highest Ranks is allocated the available resources. In this example, there are three resource units available for allocation and five users. The probability of misbehaving or wining a reward for each user are given in the table. We assume the time is slotted with every slot corresponding to a period when resources are available and allocated to three of the users.

The top figure shows the percentage of resources allocated throughout the simulation to each user. The bottom figure shows how the rank for each access seeker as it changes over time.

User 1 is always misbehaving, which leads to it being allocated the minimum amount of resources. On the other hand, User 2 has the lowest probability to misbehave which is rewarded by being allocated more resources than the rest of the users. The punishment and reward parameters are:

$$a_{reward} = 1 \quad a_{penalty} = -1$$
$$b_{reward} = 10 \quad b_{penalty} = 5$$

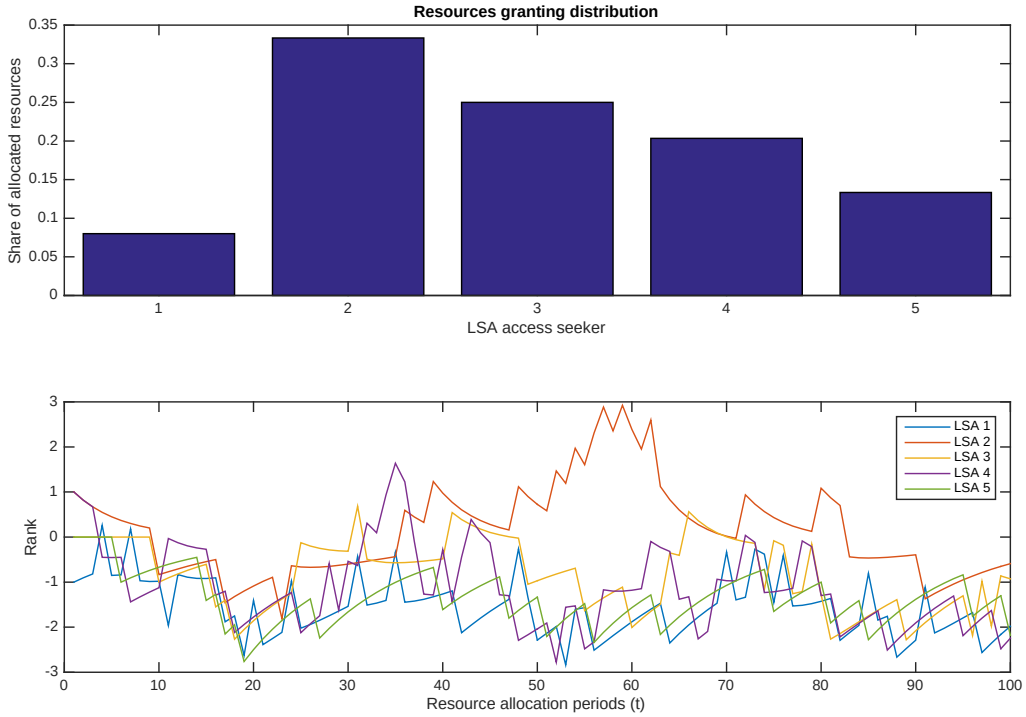


Figure 11: Allocation of shared resources to different access seekers (top) and their respective ranks (bottom) under deterministic allocation policy.

9.2.1.2 Probabilistic allocation of resources

First, we show the effect the random allocation policy has on two access seekers, one who always complies with the LSA agreement, and another who other always misbehaves.

The top two figures show the rank and the access granting probability when no rewards are given. For both users $a_{penalty} = -1; b_{penalty} = 10;\ c = 1.1$.

The lower two figures show the Rank and the Access granting probability if the misbehaving user receives a reward with 50% probability. The reward has magnitude $a_{reward} = 1$. $b_{penalty}$ and c have the same values as above, 10, 1.1, respectively.

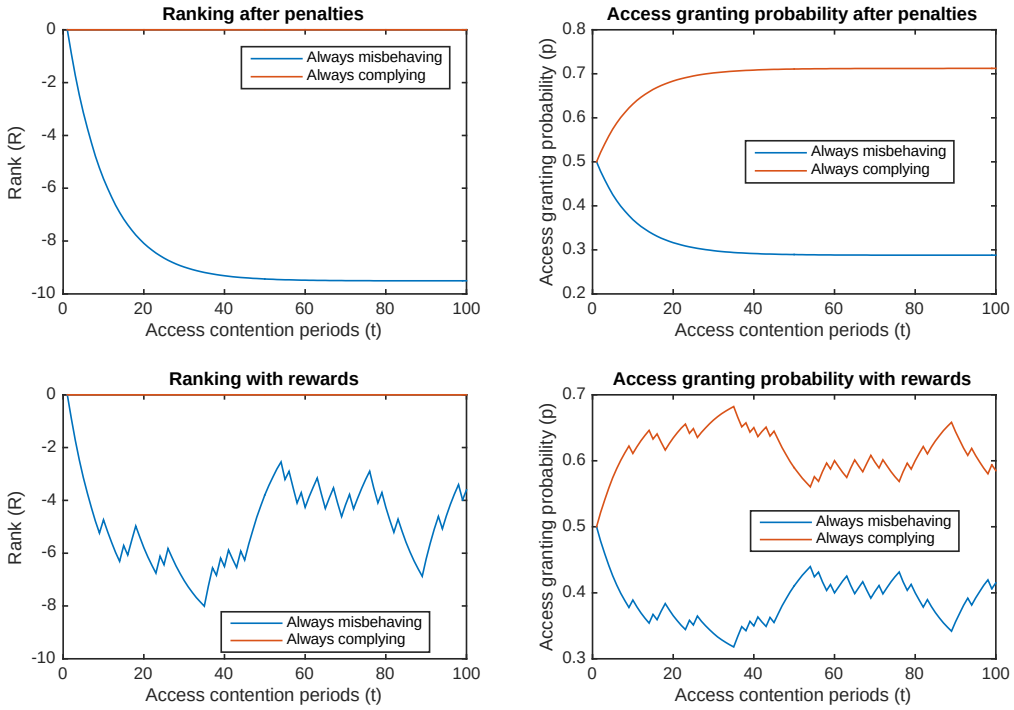


Figure 12: Ranking and access granting probabilities for an always complying and an always misbehaving user, without (top) and with (bottom) rewards.

Figure 13 shows the results with the Probabilistic Access Granting algorithm with the five users assumed also for the deterministic allocation case. The behaviour probabilities are given in Table 4. In this case only a single resource unit is available for allocation and the probability for each user to win it depends on its behaviour.

The random nature of the allocation protocol pushes the system towards being fair and allocating the resources more equally between the users. This is represented in the top figure which shows that the difference between the allocated resources to each user is lower than in the deterministic case. To some extend the effect of the user's behaviour on the resources allocation can be adjusted using parameter 'c'. In this simulation we have set $c = 1.5$.

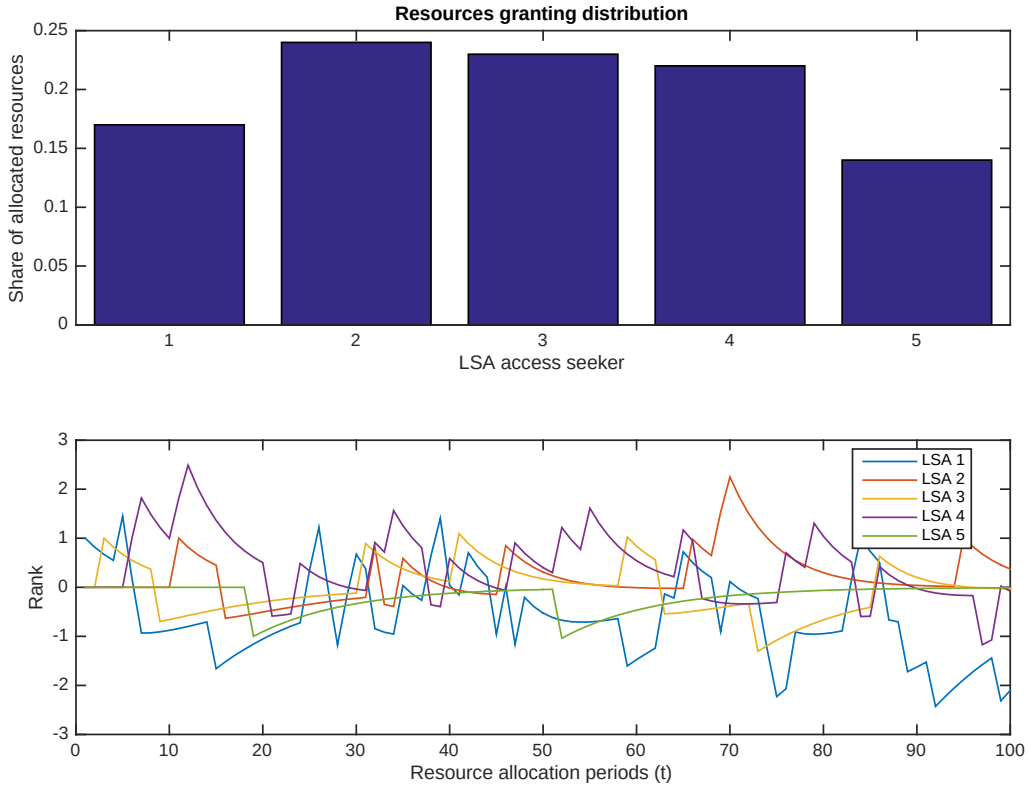


Figure 13: Allocation of shared resources to different access seekers (top) and their respective ranks (bottom) under random allocation policy.

9.2.1.3 Rank – proportional resource allocation

The Rank-proportional allocation of resources allocates the available resources based on the Rank of the Licensee operators. The parameter $c > 1$ regulates how sensitive the allocation is to the Rank of the users. The higher its value the bigger the gap between the operators with high and low Ranks. Figure 14 shows the resources allocated to the Licensee operators considered in Table 4 under the rank-proportional resource allocation protocol, for various values of parameter c. By adjusting the value of this parameter it is possible to influence how severe the punishment for misbehaviour is. Parameter c does not need to be static. Indeed, the Band Manager may adjust it when radio resources are more scarce, further benefitting well-behaving users, or reduce its value during less popular periods.

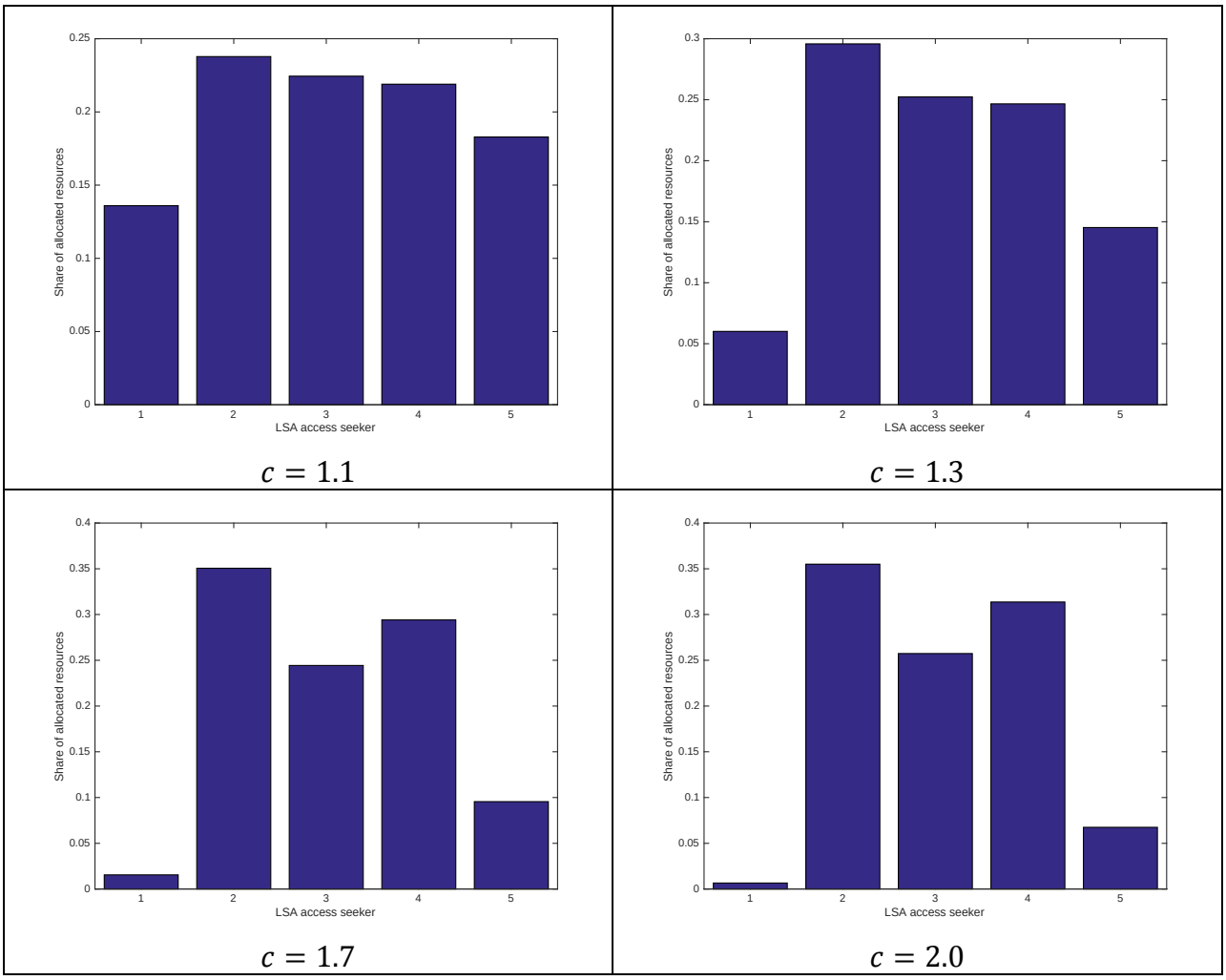


Figure 14: Resource allocation under the Rank-proportional protocol for various values of parameter c.

9.3 Penalty-weighted proportional fairness scheduling

When the spectrum is allocated to the licensee mobile network operators (MNOs), they have to comply with the regulations of LSA operation. For example, an MNO n can access the spectrum borrowed from an incumbent within a certain service area, using a certain carrier frequency, and during the allocated time period. However, it is possible that the licensee MNO violates the regulations by:

- Transmitting with more power and causing interference out of the service area
- Using a different carrier frequency than the allocated one
- Using spectrum for more time than permitted by the incumbent

We propose a framework to penalize the misbehaving mobile network operators (MNOs). The MNOs can violate the LSA spectrum use regulation in any of the above mentioned domains, i.e., power, frequency or time. However, our penalty framework can be introduced in one domain without any loss of generality. The amount of spectrum

allocated to an MNO is the main utility for the licensee operators. If they commit any of the above mentioned violations of LSA spectrum use regulations, it is sufficient to penalize them in future spectrum assignment.

9.3.1 Proposed Resource Allocation Algorithm:

- Define a penalty index (PEI) for a licensee MNO as follows:

$$\text{PEI}(n) = \frac{\text{No. of times spectrum usage rule was violated}}{\text{No. of times spectrum was assigned}}$$

- Define,

$$SI(n) = \big(\omega PI(n)\big) + (1-\omega) f\big(PEI(n)\big),$$

where ω is the penalty weight and $f(PEI)$ is a general penalty function whose values vary between 0 and 1; while PI(n) at instant t is given by,

$$\text{PI}(n) = \frac{\text{Allocated BW to the MNO n in the past}}{\text{Sum of BW allocated by the Incumbent}} = \frac{1}{W}\sum_{j=t-W}^{j=t-1} \frac{B_n^a(j)}{\sum_{n=1}^{N} B_n^a(j)}$$

where $B_n^a(j)$ is the spectrum allocated to MNO n at instant j with W denoting window size for the spectrum allocation history.

- Based on SI for each operator, apply the following algorithm:

1. Sort the MNOs with respect to SI in increasing order;
2. if available, offer the spectrum to the MNO with the smallest SI;
3. if the available spectrum is less than what required by the MNO at the top of the queue, the MNO can refuse to accept the offer, but it is still removed from the queue;
4. if the MNO accepts the offer, it is assigned BW and removed from the queue;
5. if there are more resources available for allocation, go back to step 2, with the new operator at the head of the queue.

We merge PEI with PI to have a Level 1 (L1, i.e. at the MNO level) spectrum management algorithm which encompasses the spectrum rule violation framework as well.
A careful look at the use of SI calculation for L1 algorithm unfolds a negative feedback dilemma. A $PEI > 0$ reduces the spectrum share of an MNO at the allocation instant. However, the reduction in spectrum share in the current spectrum allocation instant enhances the MNO's PI for the next spectrum allocation, because the PI calculation attempts to improve fairness if the spectrum share of an MNO reduces. The PI calculation has no mechanism to know whether the spectrum reduction is due to a 'deliberate' penalty imposed by the LSA regulator. Thus, a penalty imposed on a misbehaving MNO will not hurt the MNO in the long run. This is what we mean by negative feedback.

To overcome this problem, we propose a slight modification in the originally proposed L1 algorithm. We propose to do the spectrum allocation in step 1 of the algorithm based on SI as before. At the same time, we perform spectrum allocation decisions based on PI (solely). The 'fictitious' spectrum allocation decisions made on the basis of PI are stored in a separate database (without actual spectrum allocation). At the next spectrum allocation instant, the algorithm computes the value of PI (to be used in SI calculation) on the basis of the 'fictitious' spectrum assignment from the database. In this way, PI computation is completely oblivious of the negative penalty due to regulatory violation and avoids the negative feedback phenomenon.

9.3.2 Penalty Functions

In this section, we propose two penalty functions which have specific characteristics:

- **Linear function:** In this case, $f(PEI) = PEI$ and all the MNOs are penalized on a linear scale depending on their regulatory violation statistics.
- **Power function:** In this case, $f(PEI) = PEI^c$ where c is a constant. This function grows slowly in the beginning and much faster as PEI increases. It is left to the individual LSA regulators to decide how to construct the power function. The rationale behind the power penalty function is to penalize the offenders mildly in the beginning and increase the penalty at a faster rate as the offense increases. We believe that it is possible that the MNO misbehaving marginally might have done it unintentionally due to some hardware issues or lack of proper control plane signalling. A comparison of the different $f(PEI)$ is shown in Figure 15 for a few values of c.

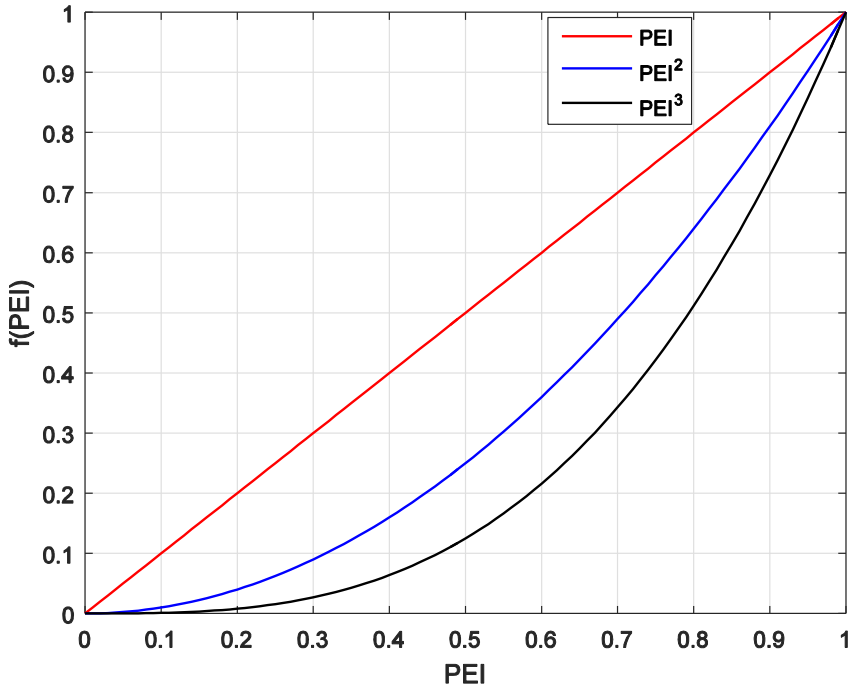


Figure 15: Growth rate of various penalty functions.

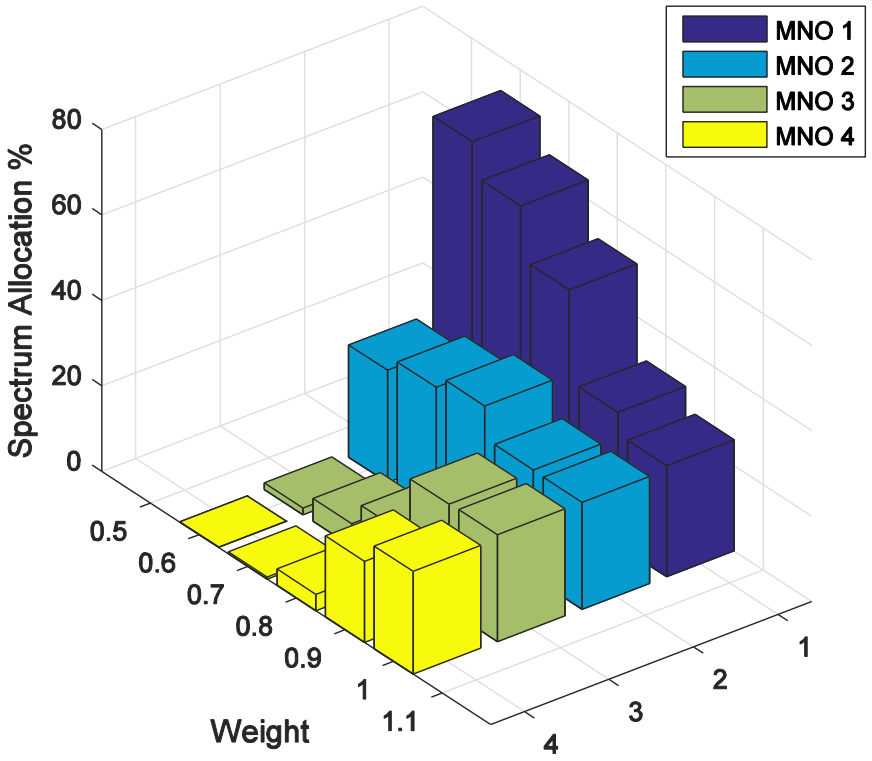


Figure 16: Spectrum allocation for linear penalty function.

9.3.3 Performance Evaluation

We use Monte Carlo simulations to evaluate the performance of the proposed algorithms. The window size W for computing PI is set to 20 to ensure more short term fairness. As PI computation for each MNO requires spectrum allocation in last W instants, we initialize simulations by having W time slots with zero spectrum allocation and random PI (between 0 and 1) values for every MNO. In the simulations, we consider N=4 (i.e. four MNOs) and incumbent spectrum B is normalized to 100 units without loss of generality. At each spectrum allocation instant, every MNO n chooses the demand randomly out of a vector of values [50,100] with uniform probability. We simulate 10,000 spectrum allocation instants to compute mean spectrum allocation for each MNO. Without loss of generality, we assume that an MNO accepts whatever spectrum is offered by the LSA band manager after running the L1 algorithm.

We evaluate the effect of penalty for violating the spectrum use regulations in Figure 16 and Figure 17. We plot the mean allocated spectrum as a function of weight ω. Note that an increasing value of ω implies more weight (importance) towards fairness. As ω decreases, the weight for regulatory violation penalty increases, proportionally. We model the parameter PEI such that MNOs 1, 2, 3 and 4 have average PEI values 0, 0.1, 0.2 and 0.3 respectively; the value of 0 implies no violation for MNO 1.

In Figure 16, we evaluate the mean spectrum allocated to each MNO when our penalty function is linear. When ω=1, the available spectrum is distributed among the MNOs equally (and fairly). When ω starts decreasing, the MNO 3 and MNO 4 with large PEI suffer while the other MNOs receive proportional incentive for behaving within the regulations. The MNO 1 gains incentive monotonically as a function of decreasing ω. However, MNO 2 gets incentive initially, but is penalized when ω is very low due to increasing weight for violation penalty and its (relatively) small PEI becomes significant.

In Figure 17, we evaluate the effect of violation penalty when the penalty function is a power function, i.e. PEI^c. In numerical evaluation, we use c=2. In general, the larger the c, the slower the penalty function growth rate in the beginning and steeper afterwards. As in Figure 16 the MNOs with large PEI suffer more in terms of spectrum access as ω decreases. In contrast to linear function, the power function penalizes the MNOs at a smaller rate initially; indeed the MNOs do not lose much share (as compared to linear function) of spectrum when ω is relatively large. As ω decreases further, the MNOs with large PEI are penalized. It is interesting that contrary to linear function case, MNO 2 with $PEI = 0.1$ is not penalized at all due to its small PEI, which validates our idea behind the power penalty function that the MNOs with small violations are not penalized much.

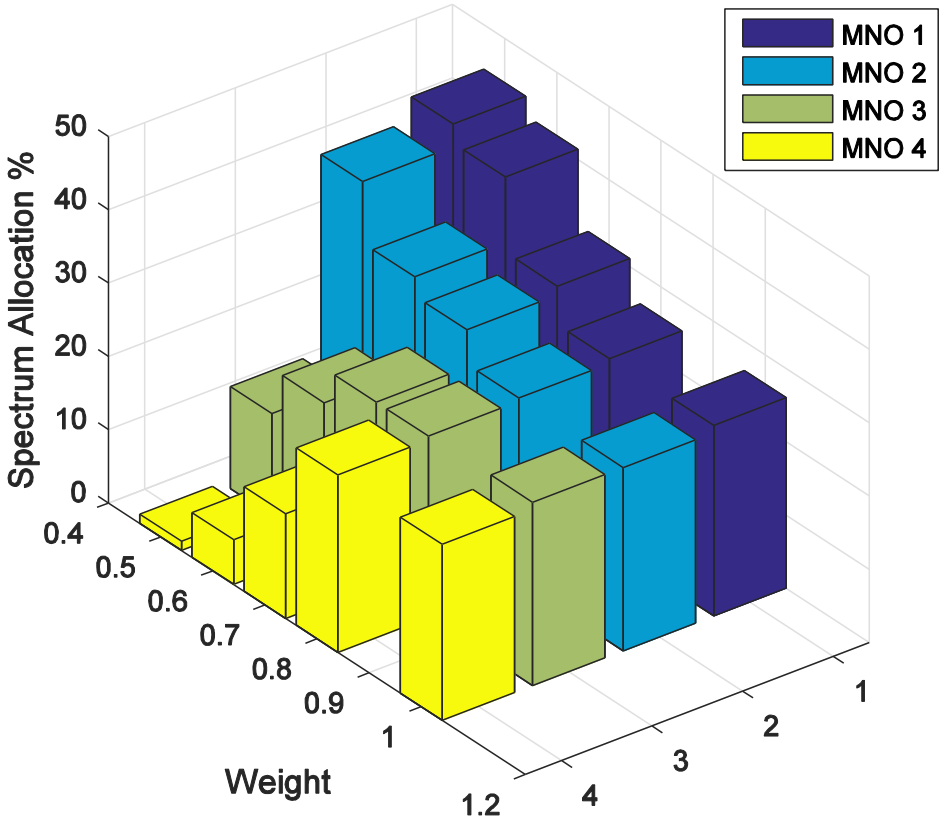


Figure 17: Spectrum allocation for exponential penalty function.

9.4 Conclusions

In this section we investigated ways in which the Band Manager can incentivise compliance with the agreed LSA rules and punish misbehaviour. We think that the right way to achieve that is by giving more resources to operators who respect the agreed rules and exclude from access those operators who constantly misbehave.

The proposed protocols are designed with adaptability in mind so that the Band Manager, NRA, or Incumbent operator can block misbehaving operators, without restricting access to operators who unintentionally (for example due to hardware problems, or misdetection from the network of sensors) have misbehaved.

10 Conclusions

ADEL's proposition pushes the boundaries of LSA from the current, rather static, paradigm to a more dynamic one with multiple Licensee and Incumbent operators sharing radio resources. In such dynamic conditions it is important for all operators to cooperate and to comply with the defined sharing rules. In this deliverable we investigated ways to safeguard access to the LSA infrastructure. We further proposed an algorithm that allows the detection of misbehaving nodes using the input from a number of distributed sensors. These sensors can be other LSA nodes, belonging either to the Incumbent, to the Licensees, to the NRA, or to independent Sensing network operators. The results show the link between the number of sensors and the detection accuracy, demonstrating the importance of cooperation to detect misbehaviour. We then propose resource allocation algorithms that take into account the operators' behaviour and compliance with the LSA rules in distributing the resources. The aim is to punish those operators who do not comply with the LSA rules by restricting their access to the shared spectrum. Furthermore, we proposed to incentivise operators who contribute to the misbehaviour detection task by improving their ability to acquire radio resources when they need them. The proposed protocols are highly customisable so that the level of punishment and reward can be adjusted based on specific conditions. For example, penalties can be higher when (or where) there is high demand for radio resources, or the rewards can be higher when there is need for additional sensing nodes to detect misbehaviour with a high probability.