Quality of Service and MObility driven cognitive radio Systems

FP7-ICT-2009-4/248454

QoSMOS

D6.4

Trust and security functions of the spectrum management framework

Contractual Date of Delivery to the CEC:	30-Apr-2012
Actual Date of Delivery to the CEC:	10th April 2013 (this issue)
Editor(s):	Keith Briggs (BT)
Author(s):	Csurgai-Horváth László (BME), Johanna Vartiainen, Janne Lehtomäki (UOULU), Santosh Kawade (BT), Bernd Bochow (Fokus), Ingo Karla (ALUD), Youngwook Ko (UNIS)
Reviewer(s):	Roland Beutler (SWR), Ramiro Robles (IT)
Workpackage:	WP6
Security:	PU
Nature:	R
Version:	Issue 2
Total number of pages:	72

Abstract:

This document studies some aspects of trust and security of the QoSMOS spectrum management architecture, as defined in D6.1, D6.2, and D6.3.

Table of contents

List of figures

1 Introduction

QoSMOS task 6.4 is dedicated to the study of the flexibility and robustness of the QoSMOS reference architecture, which is shown in Figure 1. Additionally, some security and mal-usage aspects were studied. Much of the work looked at in self-configuration and self-learning is current research and some further work needs to be done before being ready for implementation into products. Also, some of the partners here have looked at the same problem areas and suggested differing solutions. This is indicative of the state of flux in this field generally. Nevertheless, we are convinced that these are critical issues for the overall QoSMOS system and cannot be ignored.

Flexibility, robustness, and security and imprecisely defined properties, and they are inter-related. We did not attempt the impossible task of precise definition. This document focuses principally on the robustness of the algorithms to be implemented in resource management. By robustness of the architecture, we understand a level of redundancy in case any of the elements of the architecture fails. In general, robustness is related to the ability of a system to cope with failures or incorrect decisions given slight changes or uncertainty of the system input parameters. But robustness of the spectrum decision-making process is more precisely defined by in Chapter 5. By stability, we understand the ability of a system to maintain a given parameter of the system or the operational point of the system within a given controlled region. By flexibility, we understand the ability of the system to deal with a heterogeneous range of situations, without compromising accuracy too much.

More precisely, task 6.4 addressed self-configuration features, in spectrum management in particular. The main objective here is to enhance system capabilities to adapt to new situations, which might be crucial for operating in the presence of evolving competitive opportunistic users that potentially compromises the availability of spectrum opportunities and might effectively disable QoS-preserving network features. This partly complements WP5 work on approaching intelligent priority-driven spectrum resource management. But, while WP5 is addressing this issue from a QoS-driven perspective, WP6 is focussing on a flexible co-existence and etiquette-driven spectrum resource management considering up-coming and potential future wireless communication systems sharing the same spectrum.

Focussing on the dynamics of spectrum management, this task studied cognitive methods in self-configuration, self-management, self-learning and high-level decision-making and in interfacing with distributed and/or low-level decision-making. The purpose of this task here is to provide enabling features as well as complete services for efficiently handling coexistence issues and problems or compromising user-behaviour that may represent a threat to the dependable operation of the network as well as to licensed users, for example, as a reaction to a possible mal-use of certified equipment.

Among others, the task approached the problem of detecting, classifying and handling unexpected or unusual situations that may be caused by malicious users or may be simply an unusual traffic condition within an otherwise well-behaving network or network node. This task also addressed security features and methods for protecting incumbents as well as license-exempt spectrum users operating within shared spectrum. The effort allocated to this task did not allow elaborating on full-blown security solutions but rather gives a compact evaluation of vulnerabilities of spectrum management and will identify developments and solutions available that can be adopted to increase robustness of QoSMOS spectrum management against mal-use or attacks.

This document is structured as follows:

1. Chapter 2 looks at robustness, stability, and self-organizing aspects in a quite general way, from the point of view of distributed spectrum management.
2. Chapter 3 from looks at robustness enhancement and spectrum mal-use.
3. Chapter 4 looks at detection of malicious users
4. Chapter 5 studies robust decision-making processes for the QoSMOS spectrum manager.
5. Chapter 6 examines cognitive spectrum usage for femtocells.
6. Chapter 7 looks at the robustness of interference management, from the point of view of radio front-ends.

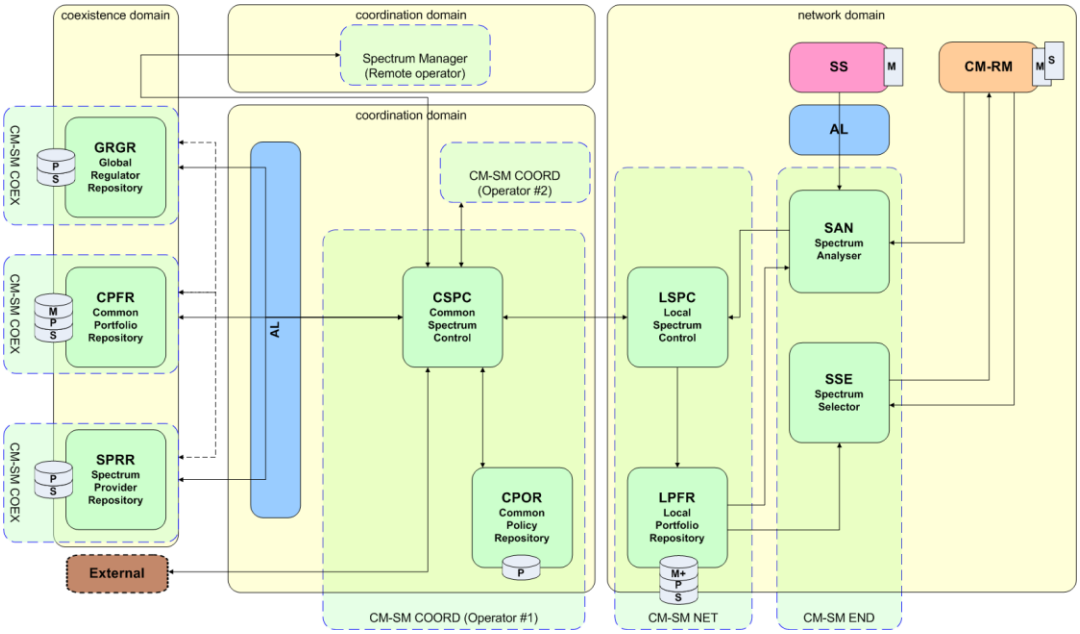

Figure 1 The QoSMOS reference model

2 Flexibility, robustness and stability in self-organizing distributed cognitive-radio spectrum management

2.1 Introduction to self-learning SON for cognitive radio

In cellular networks with their strong interactions and couplings between different groups of configuration parameters and between different independent entities, it is a non-trivial task to achieve stable and robust system operation and to ensure that the system flexibly adapts to current and changing situations.

Especially for cognitive radio, there is the challenge that potentially many different independent players could share the same wide available spectrum, with potentially limited cooperation and where the individual cognitive node needs to adapt and optimize quickly to the externally given constraints. This leads to a variety of potential issues which can impact safe operation, the system stability and the system does also need to be able to handle certain given external situation which includes erroneous behaviours.

There does not exist anything like a single "security/stability/robustness" -function or entity. Instead, the security, stability and robustness features have to be designed in and built in throughout the system. Safe operation needs to be ensured at every relevant step of the operation. In addition, potentially critical use-cases need particularly be handled and the potentially occurring issues need to be resolved.

Furthermore, the QoSMOS scenario is (or can be) so diverse, with different kind of accesses, cell layouts, different sources of interferences, cooperating and non-cooperating nodes, quickly varying and highly diverse traffic loads, that it is a large challenge to be able to let the system flexibly adapt to the given situation. This situation is so complex, that standard self-organizing networks (SON) models do only have a certain, limited, scope or can no longer appropriately be employed and configured; here it will even become required, that the self-X models adapt itselves to the given situation. This means that it is no longer suitable to use a static default SON model which configures and optimizes a (set of) parameter(s). But simulation studies have revealed that the underplaying SON modelling itself needs to adapt itself. Due to the high complexity, the only way is to use self-learning techniques for automatic SON model adaptation.

This chapter analyzes typical and possibly occurring issues and then how these can safely be resolved in cognitive radio systems. While the concepts are not restricted to a particular concrete use case, the issues and their way to safely resolve these are explained at the concrete example of distributed cognitive radio spectrum managers as explained in detail in the public QoSMOS deliverable D6.5.

The following picture illustrates schematically one typical scenario for modern cognitive radio systems. There is a heterogeneous and diverse network with a multitude of different small and large transmission nodes, such as cells or base stations. There is one spectrum manager within or for each node, and it has to be decided which parts of the spectrum or which frequency bands are best to be used – illustrated by the rainbow-colour-row; simultaneously it has to be decided which transmission power one cognitive node is allowed to use, where the circle and their arrows indicate the average coverage range in dependence of the transmission power. The mobile phones illustrate different traffic densities at certain

locations, which need to be considered when CM-SM decides on the best suited spectrum portfolio. This schematic picture does also illustrate the strong interactions between the CM-SMs.

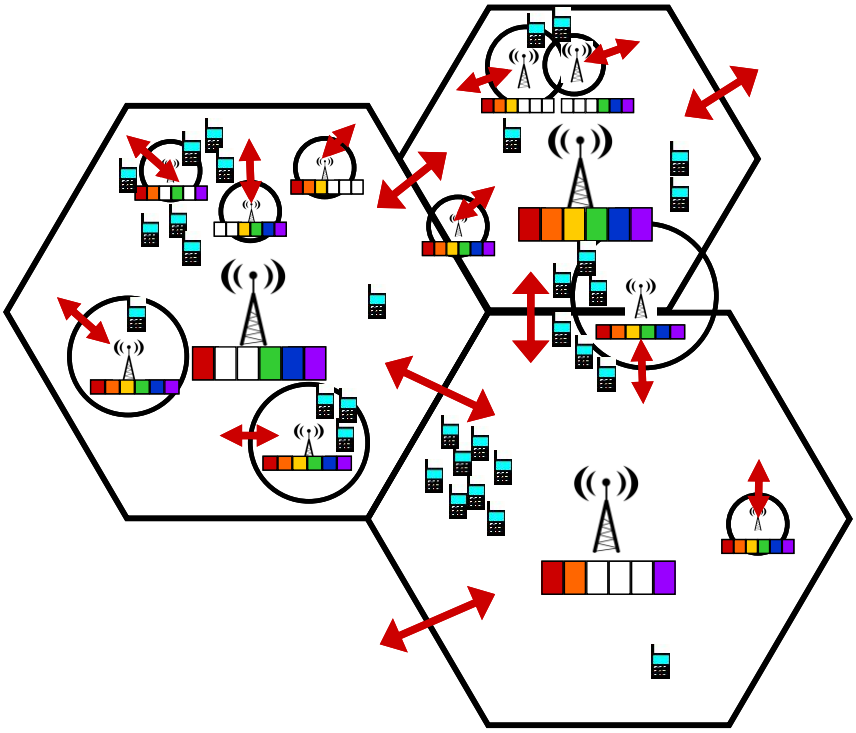

Figure 2 Schematic example of the diversity, interactions and couplings in modern cognitive radio systems.

2.2 Challenges and problem statement in distributed cognitive radio

In order to ensue stable, robust and safe operation in distributed cognitive-radio spectrum-management, there are several concrete challenges, issues, and threats, which need to be handled and resolved:

1) "Non-aligned" decisions between different but interacting, individual nodes:
   The following two types of critical effects do usually occur in cellular networks with distributed but independent decision engines, where there is a sufficiently strong mutual interaction and influence:
   - "Ping-Pongs" between two (or more) nodes:
     One node takes a decision, which is then revoked by another mode later again.
   - "Propagating Wave of Changes".
     It can happen that a parameter change one node triggers another node to change something which then triggers a third node to carry out an action, and so on.
2) Handling of erroneous behaviour and of "disturbing" other nodes and external influences:

- It is necessary to detect when other nodes do not cooperate or show an erroneous behaviour, and then to handle this situation in a good way.
- It is necessary to be able to react to external changes or external "disturbances" and to adapt to this new or changed situation.

3) Necessity to handle highly cell- and system-individual situation:
   - The distributed SON solution should optimize the situation individually for each cell, as in the potentially very diverse cognitive radio scenario; it is not possible to have the same configurations for each cell, possibly not even the same modelling. Each node and each cell needs to be optimized individually, while considering all the interactions and couplings with other cells and with other radio nodes and considering the particular situation and constraints in and around that node.
4) The node internal operation also needs to be robust in order to ensure safe, stable and robust functioning and decisions:
   - The decision node itself needs to control itself, and if needed to adapt and align itself to ensure the given strategy.
   - Due to the complexity of all the occurring situations, self-X techniques are the only way to handle the multi-parameter optimisations, but is has been found out that even the underlying self-X functions will have to be adapted according to the occurring situation.

2.3 Ensuring stability and robustness for distributed cognitive radio

The following chapters provide the solution concepts how to achieve and ensure this flexibility, security, stability and robustness aspects in cellular networks.

Large parts of the solutions below are quite generic and can be used in different designs and realisations. But for clarity, these are described concretely for the cognitive spectrum managers and their internal realizations as outlined in detail in the QoSMOS deliverable D6.5.

2.3.1 Ensuring stable decision making in distributed cognitive spectrum managers

Simulation studies have shown that a set of mechanisms and techniques are required to safely ensure stable system operation, these are:

1) **Local area considered for configuration and optimization:**
   The cognitive spectrum manager bases its decisions not only on its own situation, but it also analyses the situation in the spectrum managers in the surrounding area, e.g. in the surrounding cells. In this way, a spectrum manager can take decisions of which he assesses that it is also fine for its neighbouring spectrum managers. This local area assignment and optimization already achieves in most cases that neighbouring spectrum managers are already happy and that they commonly agree on the achieved parameter settings.

However, in certain cases, there do still occur the above outlined stability issues. These can be resolved by the following further techniques:

2) **Dynamically enlarging the knowledge scope and the size of the local area:**
The spectrum manager can dynamically increase the size of its local area. The knowledge base is enlarged and possibly also a larger amount of other spectrum managers are taken into account during its local area parameter optimization procedure. While this increases the computational effort, it further reduces the risk of contradictory decisions among neighbouring spectrum managers.

3) **Ping-Pong detection and resolving:**
The spectrum managers keep history lists of already previously occurred situations within its surrounding local area. Via these history lists, it can be detected when the same situation reoccurs again. When such a Ping-Pong or a Ring-Ping-Pong occurs, then the local area parameter optimization procedure chooses a different parameter set than before, not the same one as during previous optimization procedure at the same situation. This time a new good parameter set is determined and chosen, which is likely to be well suited to break the (Ring-)Ping-Pong loop.

4) **Suppressing and resolving of propagating waves of changes:**
Firstly, the parameter optimization algorithm of the spectrum manager strives for restricting the changes to the a close area, and only initiates changes more distantly if really needed. Furthermore, the local area optimization strives for initiating only parameter changes which are also good for the other spectrum managers involved. So the probability of moving waves of changes by design already very low.
However, if such behaviour should occur, then it can

   a. either be suppressed by dynamically increasing a kind of damping, the threshold for doing a parameter change,

   b. and/or by especially taking into account that the local area optimization shall strive for suppressing such ongoing parameter changes.

With these above techniques, it was found that the distributed spectrum managers achieve safely to always ensure network system stability despite of their fully independent and distributed decision engines operating on the same highly coupled and interfering parameters.

2.3.2 Inter spectrum manager interactions, triggers, timers and delays

The fully distributed spectrum manager (CM-SM) entities do all operate independently, but they altogether need to achieve a stable system operation; i.e. it needs to be considered that two CM-SMs could work simultaneously, which could result in overlapping decisions, which are not favourable. Therefore, it is needed to take a particular attention on the timers and delays when inter CM-SM messages or commands are being sent, and the following aspects all need to be considered:

The local optimization procedure of the SON entity of one CM-SM is (or can be) triggered by the following events:

1) A periodic timer, optionally with a short random time variation: Each SON entity of each CM-SM may “periodically” trigger itself to check the situation and to evaluate whether to run the local area optimization procedure.

2) When the CM-SM receives new status information, e.g. a changed configuration in its neighbourhood, or a new load or interference information, or new external constraints

(e.g. spectrum database), then the SON entity of the CM-SM is triggering itself to evaluate the situation to access whether or not to run the complete local area optimization procedure.

3) An external trigger, asking the CM-SM to assess and if needed to optimize the situation. An external entity (e.g. spectrum database) or the CM-RM has the possibility to ask the CM-SM to optimize its local area situation. The CM-RM may evaluate itself that there is the room for optimization (e.g. the CM-RM evaluates, that it may better be assigned more spectrum resources) and then the CM-RM asks its CM-SM to make a re-evaluation of the situation – and thereby considering the new – e.g., high load – situation within the CM-RM.

4) All trigger timings have a (small) random component in order to make it likely that different cells start and finish their optimization procedures at different times. (But when this simultaneous case should nevertheless occur, then it is handled as described below in next point).

   Depending on the urgency of a certain re-optimization for a certain node, different kinds of actions/events have different timers and delays in order to priories the order within which and the delay when a particular CM-SMs is triggered to run their SON optimizations.

5) Interrupts: If a CM-SM is currently running the optimization procedure, and exactly when executing the computations this CM-SM is at the same time receiving new external information, such as, for example, a changed spectrum portfolio in the neighbouring cell, then the already started optimization procedure is stopped, no spectrum or parameters are changed, and a new optimization procedure is scheduled to be re-started in the near future (with a small random delay component).

Due to the above random timers and random delays it is very unlikely that two messages are exchanged at exactly the same time, e.g. when two CM-SM simultaneously ask the other one to initiate parameter changes or when one CM-SM receives exactly simultaneously orders to perform contradicting changes. However if such an unlikely overlap should occur, then the self-observation of the CM-SMs does quickly detect such a conflict of contradicting messages or in contradicting parameter settings and it will then re-initiate –with a short random delay- the local area optimization procedure to resolve that previously arisen non-aligned situation in a self-healing way.

2.3.3 Robustness, handling erroneous behaviour and adaptation to occurring disturbances

The design of the distributed spectrum manager with its local area parameter configuration and optimization is already very well suited to handle in a robust way non-intended behaviour and situations. It could occur, that another node in the system does not cooperate, shows an erroneous behaviour, creates a disturbance, or that there is another (not controlled) external disturbance. This situation is easily detected by a spectrum manager, i.e. by its own received measurement reports and/or by observing that the other node does not set parameters as it is supposed to do.

Then the spectrum manager considers this situation as a fixed external disturbance that it cannot it cannot change certain external conditions. For example it takes into account another

node within its “influence sphere” has to keep its fixed, constant, parameter configurations. Or as another example, it takes into account that on a certain frequency band there is a certain (non-changeable) high interference level.

Then the local area optimization of a spectrum manager is then able to “optimize around” the non-cooperating nodes and to handle in the best possible way the external constraints. The local area optimization then adapts and optimizes all the remaining free parameters within the local area in such a way, that the situation is optimized under consideration of the external situation.

So, this distributed spectrum manager design is very robust and well suited to self-optimize and to handle erroneous behaviour and to cope with any external constraints. Due to the distributed nature of the design, other nodes quickly detect when one node should show erroneous or non-intended behaviour This detection can then be used to trigger the above optimization around that given situation, to send alarms, e.g. to an operation & maintenance centre, and -if supported by the erroneous node- to initiate self-healing procedures.

2.4 Ensuring safe and stable internal operation via self-learning

As already mentioned above, due to the very large diversity, it is no longer possible to have a fixed model which is used to set suitable node configuration parameters, such as which part of the spectrum and with which power is an CM-RM (or cell) is allowed to use. Self-adaptation techniques need to be used to even modify the underplaying SON model as manual configuration is not longer really feasible. This means that “self-learningly” the internal decision procedures and the internal equations need to be adapted according to the particular very individual situation. There is not a single “self-learning” function. Basically at any major step, the system needs to adapt its internal equations and their configuration parameters to the current situation.

In this way, the internal CM-SM Operation is able to adapt itself flexibly to the changing and given external situation (load, interferences, spectrum availabilities, …) and is robustly capable to achieve and ensure its configuration and optimization strategy.

The following two pictures illustrate where all self-adaptation, self-calibration and self-learning techniques have to be employed to ensure safely the robust and flexible operation of the CM-SMs in this possibly highly diverse QoSMOS scenario:

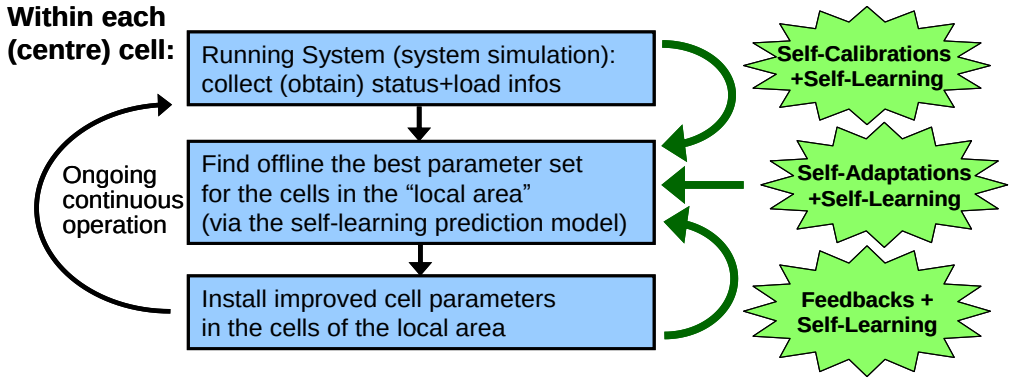

Figure 3 Self-X and self-learning techniques are needed at various steps of the SON model for cognitive radio spectrum managers

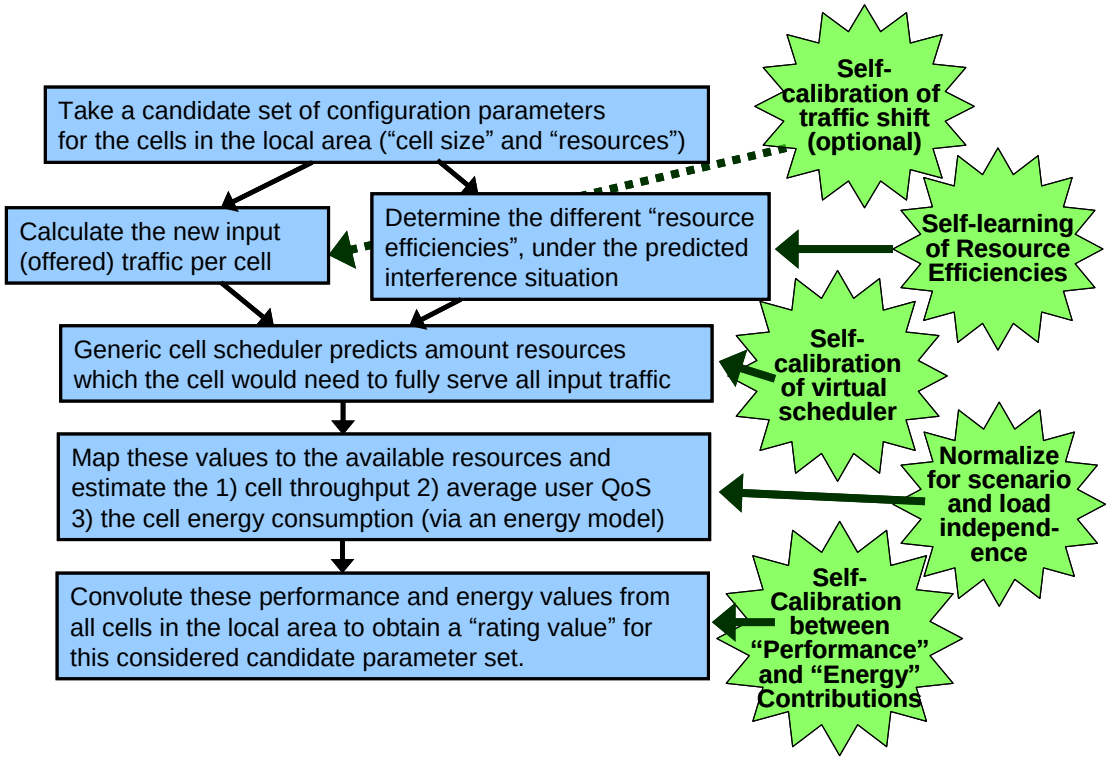

Figure 4 Self-X and self-learning techniques are required at many steps of the internal operation of the SON and prediction.

In the following, some of these Self-X and self-learning steps are sketched and explained in some more detail:

1) **Work with deviations from the current state** – instead of calculations from the beginning.

   Instead of starting predicting the values from zero, from an empty system, the SON + self-learning system takes the current situation as a starting point and then applies only

variations to the current state. This then limits the potential mismatch of the prediction model compared to the later in real system occurring situation after this parameter set would have been installed.

For example, the predicted amount of shifted traffic is calculated as a deviation from the current situation: When the cell border is (evaluated to be) shifted, then this causes a shift of that (average) traffic amount within that affected border area. The new traffic per cell is then calculated based on the current traffic load value plus or minus this predicted traffic shift.

2) Adapt (limit) algorithm step size according to the expected imperfection of the prediction

Within the distributed SON solution procedure, there is an algorithm which evaluates a variety of possible candidate parameter combinations. With perfect prediction it would be possible to search the full theoretically possible parameter space within one single algorithm step. However it may be required to restrict the parameter variation to a certain maximum value in order to ensure that the simplified prediction model is still sufficiently accurate. For example, it could be beneficial to limit the limit the (virtually evaluated) shift of the cell border to a few dB only and not to allow e.g. a 15 dB shift of the cell size within one single algorithm step. Iterative algorithm procedures will then further shift the cell border step-by-step if needed.

3) Adaptation of traffic shift prediction function:

As a starting point, at first the traffic shift is assumed to be linear in the amount of traffic in the cell border area of the shrinking cell. This is a good starting point and already works.

However, in the case that no detailed information about the traffic distribution within the cells is available, then it will become highly beneficial to let the system learn a scaling factor for the traffic shift via feedback of the previously achieved result. This feedback then does also allow to learn the typical traffic distribution within the unknown other cell. After the SON algorithm has chosen and installed a particular set of new configuration parameters, then the self-learning functionality compares the previously predicted traffic shift with the actually occurring one in order to tune the traffic shift prediction function e.g. via a scaling factor. There are (or can be) individual self-learning traffic scaling factors for each cell towards each of its direct neighbouring cells.

4) Self-learning of the generic “Resource Efficiencies”

These previously in the QoSMOS deliverable D6.5 introduced resource efficiencies represent in a generic way how well a particular resource (e.g. a certain part of the frequency spectrum portfolio) is able to provide e.g. data at a particular location and under the occurring interference situation. This generic representation is capable of describing the behaviour of different types of networks, and for the particular cell

individual situation. However, there is the challenge to set the key parameters for the values of the resource efficiencies. Due to the diversity of the possible scenarios and variety of occurring situations, the only way is to use self-X techniques to let the system set these key parameters itself.

The following steps are required:

a) The SON entity of the CM-SM collects information about the current state, i.e. as far as possible how well (under the current resource usage, distribution and cell size) the existing resources are able to serve the users, averaged over the time period as used within the underplaying distributed SON technique.

b) It shall be noted, that possibly or usually not all of the individual resource efficiencies can be determined (measured) from the system, e.g. because that type of resource and interference situation was not used and thus no measurement data are available.
In this case, these non-measured resource efficiencies are assumed to be approximated based on other available measurement values. This can, for example, be by taking values from a larger area (such as the whole cell) and/or by assuming that there is a certain (default-value) performance difference between interference-free and interference-suffering resources.

c) Self-Calibration of resource efficiencies:
Before the SON algorithm evaluates new candidate parameter sets, there is a calibration of the resource efficiencies used in the generic virtual scheduler model. The virtual scheduler is run for the currently active parameter set, using the initially measured resource efficiencies and then the virtual scheduler calculates resource wishes for the just now present situation. The resulting predicted cell performance of the virtual scheduler is then compared to the actual situation in the cell. Simulation studies have shown that there is typically a certain mismatch, as the simple generic scheduler is not as complex as the real system scheduler and as there are some approximation errors. Thus it is now crucial for correct SON operation to calibrate the virtual model to the real system situation. This is done via scaling the virtual resource efficiencies in such a way, that the virtual scheduler then calculates precisely the same system performance as the real system has just shown.
The virtual scheduler is now calibrated to predict perfect results for the currently active parameter set in the currently present situation.

These self-calibrated resource efficiencies are then kept constant during one SON algorithm step when various possible candidate parameter sets are virtually evaluated.

5) Self-normalisation of the metric to be generic for different technologies/scenarios

When calculating a predicted system performance, then the predicted values correspond to the concrete situation, e.g. to the offered traffic load. This leads to the case that in different scenarios and different cells within a cellular network, the performance prediction would return highly varying numerical values. However, the strategy of the network operator is typically represented by generic aims, which are independent of

particular concrete e.g. data-bit numbers. So, within one SON-algorithm cycle, the input values for the metric should be normalized.
For example, the actually occurring energy consumption can be normalized against the maximum possible energy consumption assuming with full power on all possible resources. For example the actually occurring user Quality of Service could be normalized against the case that all users would get fully served with completely their requested service. Or, for example, the system throughput could be normalized against the case that all the offered traffic would completely be fully served by the system.
With this normalisation, the metric then becomes system and load independent and the same metrics function does always represent the strategy of the network operator and can be used in a generic way.

2.4.1 Self-learning of the general energy-modelling performance

The SON algorithm decides on the best-suited parameter set based on its internal virtual metric to predict, based on the scheduler resource needs/consumptions, the resulting performance and energy consumption for that particular cell. This virtual metric does not need to create absolute values because it is only used to compare different candidate parameter sets against each other. However, the metrics does nevertheless need to correctly represent the major metrics contributions, such as the ratio between positive parts (system performance, user experienced quality of service) and negative parts (e.g., energy consumption). Otherwise there is the risk that the SON model drifts away from the real system by either favouring improving the performance or by minimizing the energy consumption, while in the real system there is a different balance between these two kinds of contributions.

Thus, the performance-to-energy ratio of the metric should self-learningly be calibrated to the actually occurring situation. The performance-to-energy ratio of the predicted new parameter set should be compared to the observed one of the real system and then a calibration factor is applied to, for example, the energy part of the metric, to ensure that the metrics to select the best candidate parameter set, represents the performance to energy behaviour of the real cell.

2.5 Summary and Conclusion

This chapter provides solution concepts to ensure flexibility, robustness and stability for spectrum managers. It resolves typically occurring issues in cellular networks with distributed cognitive decision engines. This set of functionalities has concretely been outlined at the example of the distributed SON for cognitive spectrum managers as described in detail in the QoSMOS deliverable D6.5. Altogether, these concepts create a novel solution approach, how the cognitive spectrum manager is able to actually configure and optimize the spectrum portfolio and its power settings; it actually manages to achieve concrete configurations and settings for the spectrum portfolio which is assigned to the CM-RM.

This complete SON approach, together with the self-learning solution, is capable of allowing distributed cognitive spectrum managers to configure and optimize highly interacting cell configuration parameters. It adapts itself in a self-learning way to the individual and current situation of the particular cognitive manager. Thereby, it employs internally a self-learning prediction model which performs fast off-line calculations without needing direct system feedback.

It is a step towards the vision to simply put any cognitive entity, for example for a cell, into a very diverse, heterogeneous environment, and then the SON entities simply adapt and optimize themselves automatically to the individual, currently given situation and to quickly changing situations while thereby resolving the major inter-cell interactions and parameter couplings.

This distributed self-learning approach includes, that the cognitive spectrum managers are capable to cope and optimize themselves in the best possible way to changing external influences, quickly varying scenarios, as well as also to an externally given non-changeable constraints, such as constraints from spectrum availabilities and to interfering cells from other non-cooperating network vendors. In the same way, the distributed system detects, handles and copes in the best possible way with (if occurring) erroneous behaviours from other nodes in order to ensure always a robust and stable system operation.

3 Robustness enhancement and spectrum mal-usage detection

3.1 Overview

In this chapter we focus on the management and system control issues in mobile cognitive radio (CR) systems exploiting "TV white space" (TVWS) [1]. The investigated scenario is a cognitive management (CM) system operating in a geographical area with fixed TV broadcast transmitters, supplying fixed users (often called as incumbents) and mobile users (in common terminology opportunistic users) in the same UHF frequency band. Our goal is to improve spectral efficiency in the geographical area by exploiting the spatial opportunities of the mobile terminals. The map of the incumbent system (the physical structure of the radio network) determines a static radio environment. This environment can be characterized by signal-to-interference-noise (SINR) ratio, which determines the sufficient radio transmission power levels necessary to service the incumbent users. Nevertheless, there are specific areas where the system allows for opportunistic usage of the same frequency band ("the spatial white spaces") without disturbing the incumbents [2, 3]. In order to ensure the required level of the service quality, such a system usually contains a central control and management unit with cognitive resource and spectrum management (CM-RM and CM-SM) functionalities. The CM is responsible for control of the opportunistic system, so guaranteeing operation of the incumbents by collecting, storing and processing information and performing decision processes on the spectrum usage of the opportunistic users. Applying a geographical database of the SINR guaranteeing incumbent's services, the gathered location information of the opportunistic users can determine the possibility of the secondary usage of white spaces. This requires periodic position updates at the CM reported by the moving user. However, the exact location is unknown between two consecutive reports, and therefore the opportunistic user may violate SINR requirements of the primary system. The outcome of this research is the investigation the effect of location sampling on the system conformance measured by mal-usage of the available resources.

3.2 Introduction

A fixed terrestrial radio service, like a TV broadcasting system, with specific parameters as geographical location, transmission power and antenna characteristics determines the coverage area where the service quality is guaranteed for the incumbents. Depending on the above mentioned characteristics, an investigated area may have locations where the primary service is not available due to low local received signal quality, which can be characterized for example by the SINR value. In this case the channel can be utilized for other purposes, for example for secondary usage by cognitive radios. In this study the case of moving cognitive radio is studied and modelled, emphasizing the role of the CM during the decision process. The efficiency of the CM operation can be qualified by the statistics of the mal-usage, like the number of erroneous channel usage that can be false positive or negative as well.

3.3 Cognitive manager for moving radio

In this section we introduce the role of the CM by using the definitions and terms of QoSMOS [4].

Cognitive management, providing services to opportunistic radio systems, consists of two more or less separated, but cooperating functions: Resource Management (CM-RM) and Spectrum management (CM-SM). Resource management is responsible for the optimal utilization of the given spectrum portfolio that is assigned to opportunistic entities by

spectrum management. Cognitive management functions interact with several other QoSMOS functional entities, such as coordination and coexistence domain databases (Global Regulator Repository, Spectrum Provider Repository, Common and Local Portfolio Repository), Core Network Management, Spectrum Sensing, User Application and transceiver subsystem. Both spectrum and resource management decisions are based on contexts communicated between these entities via interfaces.

Optimization steps are made in cognition cycles where synchronous operation of various functions is mandatory. However we cannot assume total independence between CM-RM and CM-SM decisions, since CM-RM decision (e.g. on modulation) may influence optimal CM-SM decision (on spectrum assignment) considering minimal interference, and vice versa. In the mobile case the time for optimization is limited, because otherwise the decision would not be optimal in the changing environment. Context gathering and processing, context communication and decisions take time, consume bandwidth and mean computation intensive tasks; therefore time necessary for the cycle to complete has a minimum which is restricted by the size of the system, the computational power offered by equipment (so on the price), and the complexity of optimization algorithm.

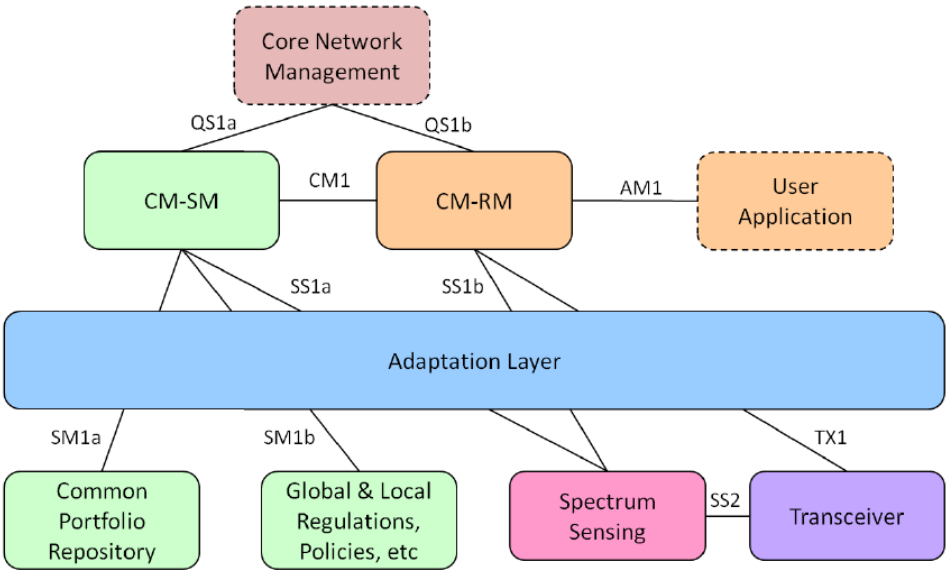

Figure 5 QoSMOS System Reference Model [9]

Optimal resource allocation and low communication overhead requires hierarchical cognitive management topology where certain decisions and context processing tasks are delegated to lower hierarchical levels. As we go upwards in this hierarchy the granularity of context information decreases (context aggregation), the spectrum part to be assigned and the managed geographical area increase. On the other hand the hierarchical topology alone would not provide optimal solution, because decisions made by spectrum and resource management of independent devices (e.g. mobile terminals) on the same hierarchical layer could result in suboptimal network conditions. Hence scope (parameter set, and value range) of delegated decisions might be restricted.

3.4 Resource Management (CM-RM)

Resource management offers data transport services to user applications for the required bandwidth, QoS, according to the actual radio environment and network conditions. It sends request to spectrum management for radio frequency assignment and optimize utilization of

the received spectrum portfolio by controlling the transceiver subsystem. In the request CM-RM communicates equipment (e.g. capabilities), bandwidth and QoS requirement and mobility (e.g. location, speed) related context. The poor accuracy of any of this context information could cause reduced spectral efficiency and/or increased interference to primary users. The balance of context sampling period and accuracy must be carefully designed, because system performance may dramatically decrease (or expenses due to computation increase) if balance is not set appropriately. Besides above functions CM-RM controls spectrum sensing, processes and communicates the measured spectrum information to spectrum management.

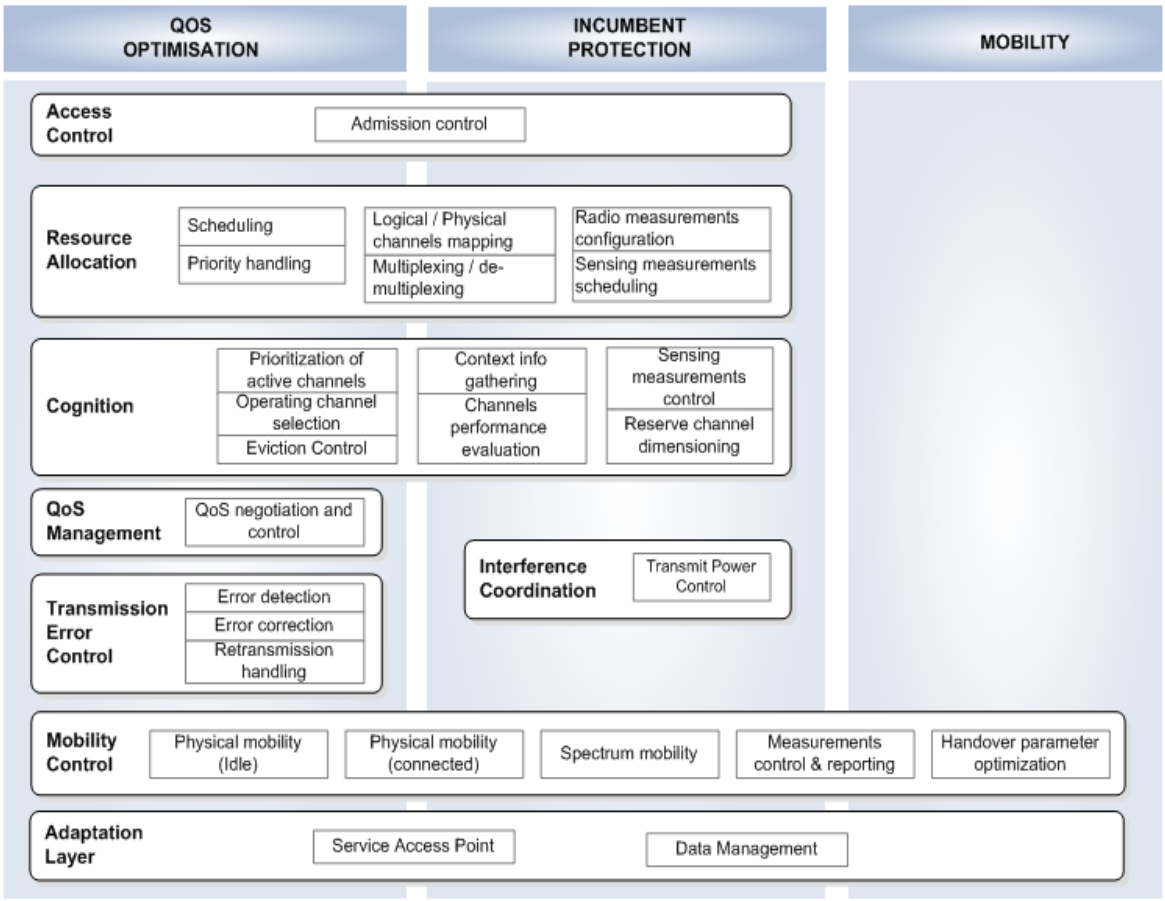

Figure 6 QoSMOS Resource Management QoS and Mobility functions[10]

3.5 Spectrum Management (CM-SM)

Spectrum management takes care for optimal spectrum allocation for geographical regions, cells and end devices, considering overall QoS, mobility, radio environment and spectral efficiency of the whole network. CM-SM connects to databases that stores spectrum portfolio and policies for retrieving available frequencies and usage restrictions, and it combines the information stored there with spectrum sensing data while deciding on spectrum assignment. Resource management provides input context and spectrum requests for cognitive spectrum management decision cycle. Requirements regarding time efficiency of processing of spectrum requests in case of mobile terminals are higher, because latency may result in frequency mal-usage, hence increased interference to primary service.

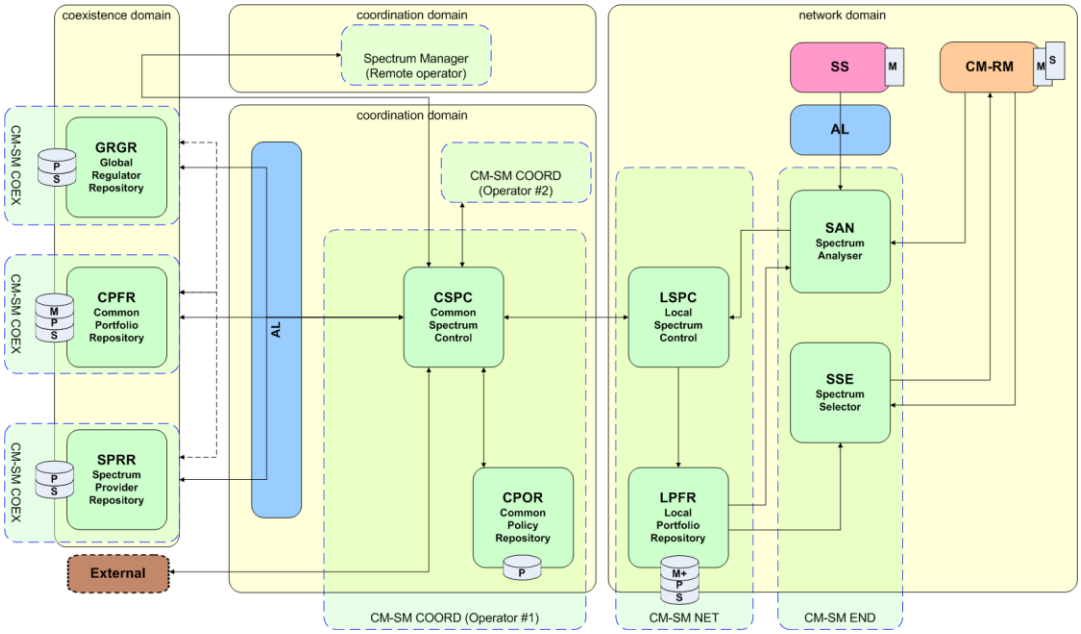

Figure 7 QoSMOS Spectrum Management Reference Model [11]

3.6 Geographical location database for CR environment

In our approach we assume a static arrangement of transmitters and receivers as parts of the incumbent radio system. Important system parameters are geographical positions of equipment, transmitter frequency, power and receiver and transmitter antenna characteristics [5]. The following equation gives the value of path attenuation on the radio channel where P_{out} is the power fed to the transmitter antenna and P_{in} is the effective power on the receiver antenna (here lg is log base 10):

$$a_{path}^{[dB]} = 10 \lg \frac{P_{out}}{P_{in}} \qquad (1)$$

For free space propagation the path attenuation can be expressed also as the function of path length D, the wavelength λ and the transmitter and receiver antenna gain, G_T and G_R:

$$a_{path}^{[dB]} = 20 \lg \frac{4\pi D}{\lambda} - G_T^{[dB]} - G_R^{[dB]} = 32.44 + 20 \lg f^{[MHz]} + 20 \lg D^{[km]} \qquad (2)$$

Besides the useful signal usually there are interfering radio sources, that may cause disturbances if their frequency range is close to the frequency band of the useful signal. In the investigated topology there are multiple transmitters and we assume that a specific incumbent connects always to the transmitter that provides the best service in the area. In this system the signal of the other transmitters causes interference, and so therefore degrades the quality of service in the system.

For this topology (Figure 8), if we know the power of the transmitter, where the incumbent is connected, by using (1) the received power can be calculated. The power of the interfering signals can be taken into account as the sum of the received power from the remaining transmitters in the system.

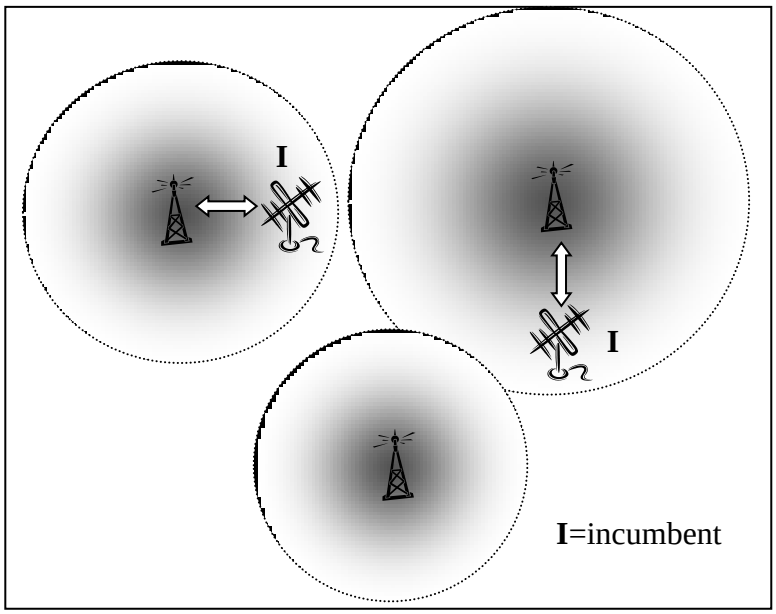

Figure 8 Simple topology for incumbents

The ratio of the useful and the interfering signal powers results the Signal to Interference Ratio (SIR). If the power of the system noise has significant value with a level comparable to the interferers, the Signal to Interference Noise Ratio (SINR) can be calculated, but in the current study we do not apply additional noise.

The quality of service for the incumbents is determined by the SIR/SINR at the receiver location. Depending on the applied modulation system, an SIR/SINR margin can be determined to ensure error-free operation.

In the investigated cognitive system, opportunistic users may exist in the above topology. Their transmitters appearing as an interferer source, therefore their contribution to the incumbents' SIR/SINR must be taken into account. It is the task of the cognitive manager to register the location of the opportunistic user(s) and determine the actual SIR/SINR map by using the geolocation database of the incumbent system topology [6]. In our study the movement of the opportunistic users is also allowed, and this option significantly increases the tasks of the CM. The moving of the cognitive radio continuously changes the signal/interference relations in the system. However the cognitive radio may continuously monitor and report its own conditions and environmental data to the CM (spectrum sensing, position recording with GPS, etc.), the amount of the transmitted information should be limited in order to reduce the load of the service channel. Our goal is to find a solution to reduce the traffic of these service data and find an intelligent solution that can be implemented in the CM to estimate the unknown parameters of the moving opportunistic user between its two reporting period.

3.7 Heuristic movement simulation and estimation the system parameters

To utilize the white spaces by the opportunistic users we have to know exactly, if in the current position the incumbent's signal quality will not be degraded. In order to achieve this goal, one of the main tasks is that the CM manages the physical architecture of the system as a geolocation database and provides the relevant information to the mobile terminals.

The applicability of a selected frequency depends on the SIR value of the current location and frequency. During our simulations we locate multiple transmitters in a hypothetical geographical area. The incumbents are always serviced in the coverage area by their closest transmitter. The coverage area of the multiple transmitters designates an SIR map of the area. In the area where the SIR is under a defined threshold the incumbents cannot be served, thus for opportunistic users this area and frequency can be utilized. Contrarily, if the moving terminals approach the coverage area they has to cease transmitting, or change frequency, to avoid degradation of incumbent's signal quality [7].

Since communication with the cognitive radios has significant overhead, it is impossible to provide SIR information to CM with infinite resolution. This means, between two telemetry cycles estimated trajectory should be used to decide about future behaviour.

There are several possibilities for trajectory estimation, such as Markov Chain methods, Neural Networks etc., where training has a key role on the systems overall effectiveness. Without those training sets, we intend to demonstrate a simple heuristic based on the assumption, that the opportunistic user most likely goes straight forward, without direction change [8]. Hence the heuristic simply gets the two last known positions (where former telemetry event was placed), and presumes the terminal will move with the same speed to the same direction.

The realised test does not use different frequencies, so the decision condition based on the heuristic is whether to transmit or not. The goal of the test is to evaluate how effective the heuristic is, by counting the mal-usage in the system. In our case *false positive* means the mobile terminal violates primary communication, while *false negative* means it does not use the communication channel, even though it is possible.

We performed simulations over a hypothetical 35*35 km area with four low-power TV transmitters with commonly used frequencies. The parameters of the simulation (transmitter frequencies, power and antenna characteristics) are summarized in Table 1.:

Table 1. Simulation parameters (4 transmitters)

	Rel. location x, y [km]	Frequency [MHz]	Power [dBm]	Antenna gain [dB]
1.	6, 6	498	40	15
2.	27, 12	610	40	15
3.	24, 27	722	40	15
4.	10, 20	818	40	15

The transmitters are equipped with four equivalent 90° sector-antennas with the following characteristics:

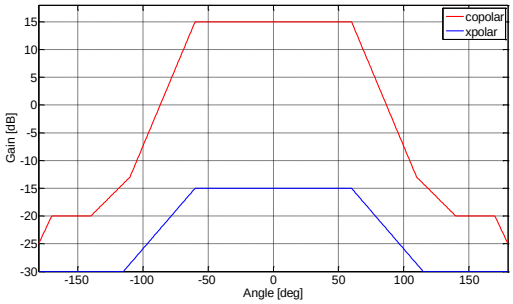

Figure 9 Transmitter antenna characteristics

During the calculations we suppose line-of-sight conditions; furthermore no shadowing or reflecting objects are considered. The opportunistic user was considered to move across this area with constant speed while its transmission is controlled by the CM. The geolocation database and the periodically reported position of the cognitive radio provide the required information to the control process. From the viewpoint of incumbents the transmitter of the cognitive radio appears in the area as an additional interferer source. If we suppose that the transmitter operates as an isotropic radiator, the power $P_{interferer}$ at distance d can be calculated from the transmitter power $P_{transmitter}$ by the following equation:

$$P_{interferer} = P_{transmitter}\left(\frac{\lambda}{4\pi d}\right)^2, \qquad (3)$$

where λ is the wavelength. During the simulations we utilized a constant *27* dBm transmit power and *0.49 m* wavelength (610 MHz).

The following figure depicts the SIR map in the transmitter's coverage. The black path marks the route of the cognitive radios; the dots are the positions that are reported to CM. The time and geographical distances between the reported positions are depending on the speed of the object and the sampling period; in this simulation the number of this positions was 30. The white crosses are the estimated positions using the simple heuristics.

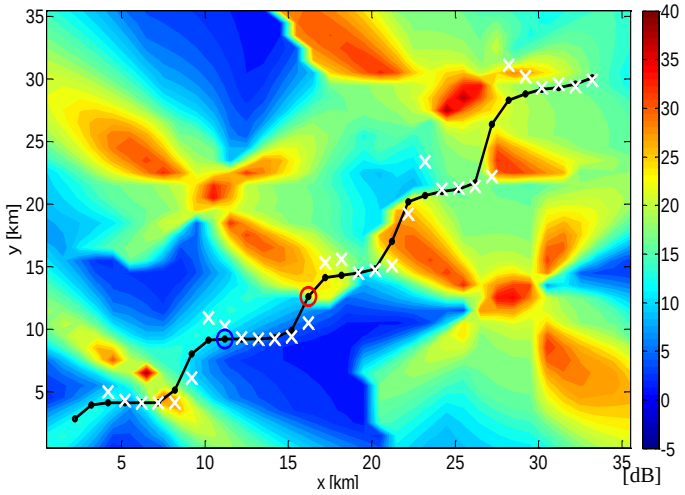

Figure 10 SIR map around the transmitters

We applied a 15 dB SIR threshold to enable or disable the opportunistic user; if the SIR is below this value at the investigated location the operation of the cognitive radio is allowed, otherwise disabled.

In case of a false positive decision the point is marked with red circle, while the false negative case is denoted with blue. In the following figure the area around the two types of false cases is detailed:

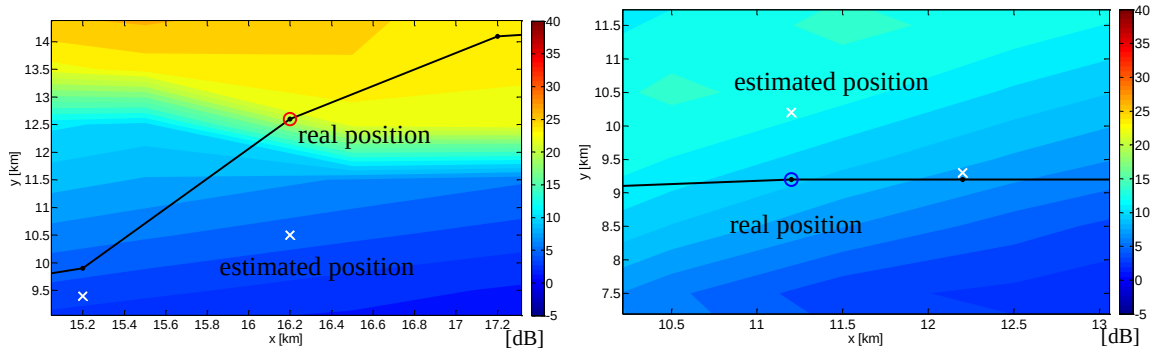

Figure 11 False positive and false negative cases

Further simulations with different moving path may result in a different number of false detections; however, with the above settings this number is usually below 10 for the current simulation area.

3.8 References

[1] Michael Fitch, Maziar Nekovee, Santosh Kawade, Keith Briggs, and Richard MacKenzie: “Wireless service provision in TV white space with cognitive radio technology: a telecom operator's perspective and experience”, IEEE Communications Magazine, March 2011 pp. 64–73.

[2] M. Mueck, D. Noguet: “TV White Space Standardization and Regulation in Europe”, 2nd Wireless VITAE conference, 2011, Chennai, India.

[3] Kazushi Muraoka, Hiroto Sugahara, Masayuki Ariyoshi: ”Cognitive Radio Mobile Network Utilising White Space Spectrum”, IEICE Society Conference 2010, Osaka, Japan.

[4] D. Noguet, R. Datta, P. H. Lehne,M. Gautier, and G. Fettweis: “TVWS regulation and QoSMOS requirements, 2ndWireless VITAE conference, 2011, Chennai, India.

[5] M. Engels, F. Petre: “Broadband Fixed Wireless Access - A System Perspective”, Springer, 2006.

[6] D. Gurney et al., “Geo-Location Database Techniques For Incumbent Protection in the TV White Space,” Proc. IEEE DySPAN, Oct. 2008.

[7] S. Pagadarai, A. Wyglinski, and R. Vuyyuru, “Characterization of vacant UHF TV channels for vehicular dynamic spectrum access,” in IEEE Vehicular Networking Conference (VNC), 2009, pp. 1–8.

[8] P. Marshall: “Recent Progress in Moving Cognitive Radio and Services to Deployment,” 9th IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks, Newport Beach, CA. June 2008.

[9] FP7-ICT-2009-4/248454 (QoSMOS) Deliverable 2.2: System architecture options for the QoSMOS system

[10] FP7-ICT-2009-4/248454 (QoSMOS) Deliverable 5.2: Final framework description (Part I), preliminary cognitive manager structure (Part II) and first mechanisms for QoS support (Part III)

[11] FP7-ICT-2009-4/248454 (QoSMOS) Deliverable 6.1: Initial description of spectrum management framework, requirements, analysis and approach selected – Executive Summary

4 Malicious users

4.1 Malicious users

Malicious users may be unintentional (device malfunctioning) or intentional (selfish and malicious users). Regardless of this, malicious users cause severe problems. For example, in cooperative systems many sensor selection methods are vulnerable to malicious users because false sensing data may degrade the performance of cooperative sensing.

Malicious behavior causes abnormalities which can be detected. In statistical point of view, malicious users are outliers or nonstandard observations. Outlier can be defined as data samples which differ significantly from the remainder of the data. There exist several methods to detect these outliers. Some methods define outliers to be points that do not lie in clusters (groups). For example, in signal processing, narrowband signal is outlier and noise belongs to the well-behavior data. More sophisticated methods classify outliers to be points which do not behave like the norm. In this kind of approach, outliers are detected investigating data characteristics that deviate significantly from normal (average) behavior. In high dimensional data, the problem is more challenging. One possibility is to use a technique based on the densities of local neighborhoods. However, computation is quite difficult. Other possibilities are, for example, to use subspaces or observe the density distributions of projections from the data.

Malicious users' attacks can be targeted on different functions as spectrum mobility, spectrum management, learning engine and spectrum sensing and sharing.

In spectrum mobility, a handoff process is needed when a node needs to change a transmission band and move without any breaks in the communication. Malicious attack can fail the handoff, for example, via jamming the network or pretending to be a primary user and, thus, force the node to change its band. These attacks can be at least partially avoided, for example, by increasing the number of channels. In addition, it is possible that a malicious user takes control of the common control channel and changes its parameters concerning unoccupied bands. To prevent this kind of attacks, common control channel has to be secured using standard AAA techniques (authentication, authorization, auditing).

In spectrum management, a spectrum sensing data falsification attack may cause difficult problems for the spectrum decision function, thus reducing the performance of the system. Filtering can be used to filter false reports by applying majority or voting rules. In addition, punishment strategy can be adopted to accelerate the influence. However, the hidden node problem is not taken into account in this approach. In learning engine, if a malicious user sends continuously false sensing results, these results come part of the known historical information. Solutions to this are to be more critical of the accepted information, or define so called trust metrics [Cla08]. Trust means how fair the behavior of a device is. [Zar09]

Denial of service (DoS) attacks are usually against spectrum sensing and sharing. Possible counter-measures include detection and prevention of malicious users attacks as well as modifying the modulation scheme so that it is more difficult to have effective DoS attacks. Authentication and trust management systems have also been proposed. In [Wan09], suspicion level of SUs is calculated based on their past reports. Therein, trust value indicators were proposed.

Malicious users who send incorrect sensing data may degrade the performance of cooperative sensing [Kal08]. In addition to being malicious, a node can be a malicious user due to device malfunctioning or selfish reasons. A selfish node may sense that there is no signal present but tells to other ones that there is a signal so it can use the free space itself. The node can send false sensing information always ('always yes' or 'always no') or only sometimes. A malicious user sending 'always one' is probably due to device malfunctioning or there is a simple malicious user having no intelligence. Malicious user can also send always opposite sensing results. That is, when PU is present, malicious user sends '0' instead of '1'. Device malfunction may also cause random energy values. Primary user emulation (PUE) attack [Che08b] means that malicious users mimic PU in order to prevent other SUs coming to the band. The goal in PUE attacks is to prevent spectrum resource usage. In selfish PUE situation, the goal is to maximize own spectrum usage, as in malicious PUE situation the goal is to cause denial of service. According to [Cla08], devices can be taught things by malicious elements of their environment, thus leading to sensory manipulation attacks, belief manipulation attacks, and cognitive radio viruses. Malicious user sending false sensing data to the fusion center in order to increase the probability of incorrect sensing results is known as Byzantine attack or spectrum sensing data falsification (SSDF) attack [Raw11]. 'Denial of service' attacks include, for example, common control channel attacks and location/ sensing/ transmitter/ receiver failures [Bro08]. Many sensor selection methods are vulnerable to malicious nodes always sending ones [Kha10]. In general, false sensing information may reduce P_d (or increase P_{fa}) of fusion center. In cooperative sensing, fusion center makes the final decision is PU present or not, and wrong sensing information may affect to that decision. Malicious users also manipulate other SUs adaptation.

When the strategy of the malicious node is known, Bayesian detection can be applied. However, the strategy is usually not known. Passive attack-proof cooperative sensing applies robust signal processing techniques in order to limit attackers' impact. In the proactive approach, honest SUs detect malicious users, and reports from malicious users are rejected. For example, *a posteriori* probabilities which SU is a malicious user are computed when the malicious users' strategy is assumed to be known. However, it is not very realistic to assume that the strategy is known because it can be arbitrary. In addition, malicious user can modify its strategy based on the method what is used to detect malicious users. Also malfunction which leads to wrong sensing reports by accident is not predictable.

In cooperative sensing, malicious nodes like 'always yes' and 'always no' can be identified by comparing energy distributions. 'Always yes' nodes increase P_{fa}, just as 'always no' nodes decrease P_d. Energy value of a malicious node differs in distribution from the energy value distribution of non-malicious nodes [Kal08]. Fig. 1 presents some examples about distributions for decisions (probability mass functions). Usually, the distribution is binomial and it depends on the probability. Instead, 'always yes' and 'always no' lead to uniform distribution. 'Always yes' decision means that the channel is always said to be occupied (always one), as 'always no' means that the channel is always said to be free (always zero). Malicious users sending 'always one' are more harmful than malicious users sending 'always zero'. The problem is that received SNRs may vary between nodes. For example, a node with a poor received SNR does not detect the signal and, thus, sends zero even though there is a signal present.

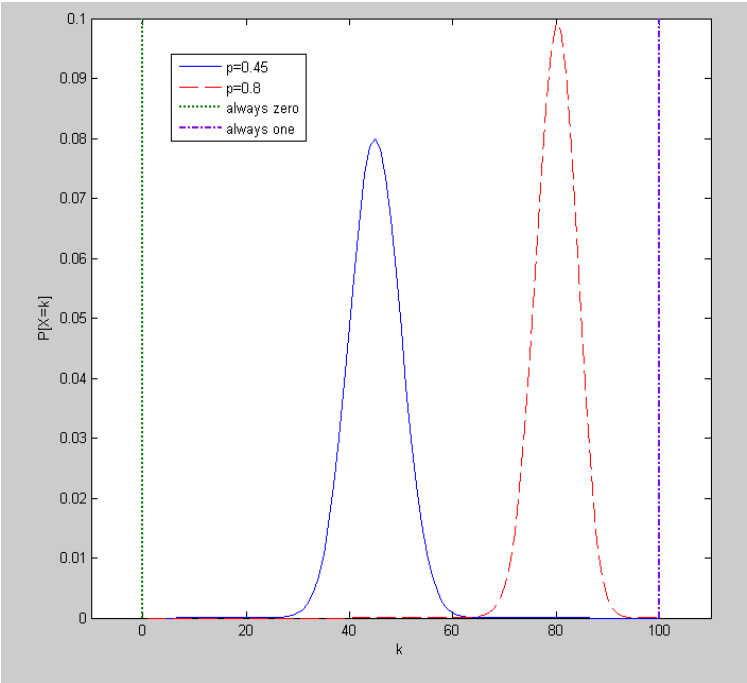

Figure 12 Examples of distributions for decisions, n=100. Binomial distribution for *p*=0.45 and *p*=0.8, uniform distribution for 'always zero' (*p*=0) and 'always one' (*p*=1). Here, *n* denotes the sequence of experiments and *p* denotes the probability.

Pre-filtering of sensing data can be based on outlier detection [Bar94]. In the pre-filtering method [Kal08], upper and lower bounds are defined based on the first and third quartiles of energy values. Malicious users' energy will be outside the upper and lower bounds. The trust factor that is used as a weighting factor for each user measures the reliability of users. Trust factors are calculated from the past and present sensing data by all users [Kal08]. Constant path loss between CR sensors and PU transmitter was assumed. According to the simulations in [Kal08], 'always yes' and 'always no' users were identified easily up to 20% malicious nodes. The method identifies malicious users if their distribution differs from the underlying distribution of the legitimate nodes. However, the method is not able to handle complex malicious users.

In [Kal10], robust outlier detection techniques were studied. Therein it was focused on malicious users giving false high energy values in the case when there are no PU signals present. Non-parametric outlier detection methods that do not need any *a priori* knowledge of underlying data distribution parameters were considered. Uncertainty in the noise measurement has no effect; no feedback from PU and no location information of PU transmitter is required. Three methods were proposed. In method one, magnitudes of the outlier factors computed using bi-weight as the location estimate and BWS as the scale estimate are compared. In method two it is assumed that PU transmits dynamically and malicious users' energy detection behavior does not follow the behavior of other nodes, and this can be used to detect malicious users. In method three, spatial information is used. Simulations indicated that method two outperforms method one, except in the situation when PU SNR values were low because there were not enough non-malicious users that had good channels.

Heuristic algorithm was proposed in [Che08]. Therein, the weight of each SU is computed and the weights are applied to balance the likelihood ratios of SUs in the sequential probability ratio test. Real-valued observations had to be reported. Knowledge about malicious users' strategies was not required. Therein, reputation-based mechanism is used. If users' local decision is consistent with the fusion centers final decision, reports from that specific node will have more weight in the decisions in the future.

The method proposed in [Wan09] assumes that there is not more than one malicious user and its strategy is known by the fusion center. *A posteriori* probabilities are computed using Bayesian rule. In [Wan09b], the method is generalized to handle more than one malicious users. Onion-peeling based approximation is used to reduce computational complexity. In [Che08b], a transmitter verification scheme LocDef (localization based defence) is proposed to handle PUE attacks.

Abnormality-detection approach has been proposed in [Li10]. The method is based on the abnormality (i.e. outlier) detection in data mining. Each SUs report histories are placed in a high-dimensional space end the abnormalities caused by malicious users are detected from that space. The threshold is set dynamically. The method does not require any knowledge of the malicious users or their strategies. However, if the SUs sensing reports are available, the method does not operate properly. When the malicious node does not know other nodes' reports about false alarm probabilities and mis-detection, the method detected the malicious node as the number of spectrum sensing round tend to infinity. This calls protection of SUs reports.

In [Ade11], method that detects malicious users without any *a priori* knowledge was proposed. The method is based on the non-parametric Kruskal-Wallis test. In [Raw11], a method to find Byzantine attacks was proposed. In the simple and effective scheme, simplified symmetric attack strategy based on the usage of reputation metric is used to count mismatches between the decisions. That is, users whose reputation metric exceeds a fixed threshold are isolated.

Malicious users (fraud) are problem also in other sciences. Usually, fraud is defined to be criminal deception. Examples are computer intrusion, money laundering, medical fraud and e-commerce credit card fraud. In paper on 'Data mining and knowledge discovery' [Faw97], cellular cloning frauds are detected by checking suspicious changes in user behavior. This is done using automatic design of user profiling methods that uses data mining techniques. To find signs about fraudulent behavior among a database that consists of customer transactions, rule-learning program is used. A set of monitors is created based on these signs. The set of monitors indicates abnormalities. The monitor's outputs are used as characteristics in a system that learns to combine existing signs in order to generate high-confidence alarms.

In [Bol02], a review of statistical fraud detection is presented. There it is said that the best way to reduce frauds is to use prevention technologies. However, as the frauds are adaptive, fraud detection methods are still required. Both statistics and machine learning provide effective technologies to detect frauds. Statistical methods are supervised (databases are used to detect fraud-types that are known) or unsupervised (nonstandard observations, that is, outliers, are examined closely). Supervised methods include, for example, linear discriminate analysis, logistic discrimination and more powerful neural networks and rule-based methods as BAYES, FOIL and RIPPER. In supervised methods, there is a problem of unbalanced class size, because there are much more normal transactions than fraudulent ones. Unsupervised methods are usually combinations of profiling and outlier detection methods, for example,

digit analysis using Benford's law. In statistical analysis, some kind of suspicion scores are used, so that high score means nonstandard observation. There exist several ways to compute these scores, because there are different kind scenarios and frauds behavior differ. Suspicion scores can be based on models or patterns like previous usage patterns, standard expected usage patterns and fraud patterns. Updated databases can be used to store the scores, so the scores can be rank ordered. One of the problems is that fraudulent detection requires effort and costs. That is, the more precise frauds are detected, the more effort and cost is needed.

Credit card fraud has been of interest for a long time, because it cause losses that are billions per year [Bol02]. That kind of fraud may be, for example, theft, application fraud or counterfeit card. In application fraud, wrong personal information is used to get a credit card. Statistical model that monitor behavior over time can be used to detect those. In the case of counterfeit card, changes in transaction patterns can be used to detect fraud. Credit card databases contain information on each transaction (account number, type of credit card and purchase, name, size and date of transaction, etc.) and this information is used.

In the literature, it is usual that data analytic tools are illustrated rather than described in detail. This is because it is not desired that possible fraud users know at what way they are detected.

The forward consecutive mean excision (FCME) algorithm [Var10], an iterative energy-type outlier detection method, is proposed here to be used for detecting simple malicious users sending '(almost) always ones' and '(almost) always zeros' [Var12]. The FCME algorithm is obtained by rearranging the samples in an ascending order according to their energies. After the sorting, the FCME algorithm calculates mean of a small initial set which consists usually about 10% of the smallest samples. The FCME algorithm iteratively calculates a new value for mean and a new threshold T_h until there are no new samples below the threshold (see Fig. 2). The computational complexity of the FCME algorithms is $N\log_2 N$, where N is the length of the input vector. In malicious user detection, samples in vector are means of decisions. That is, first sample in vector is the mean of first node's sensing period results (1 or 0).

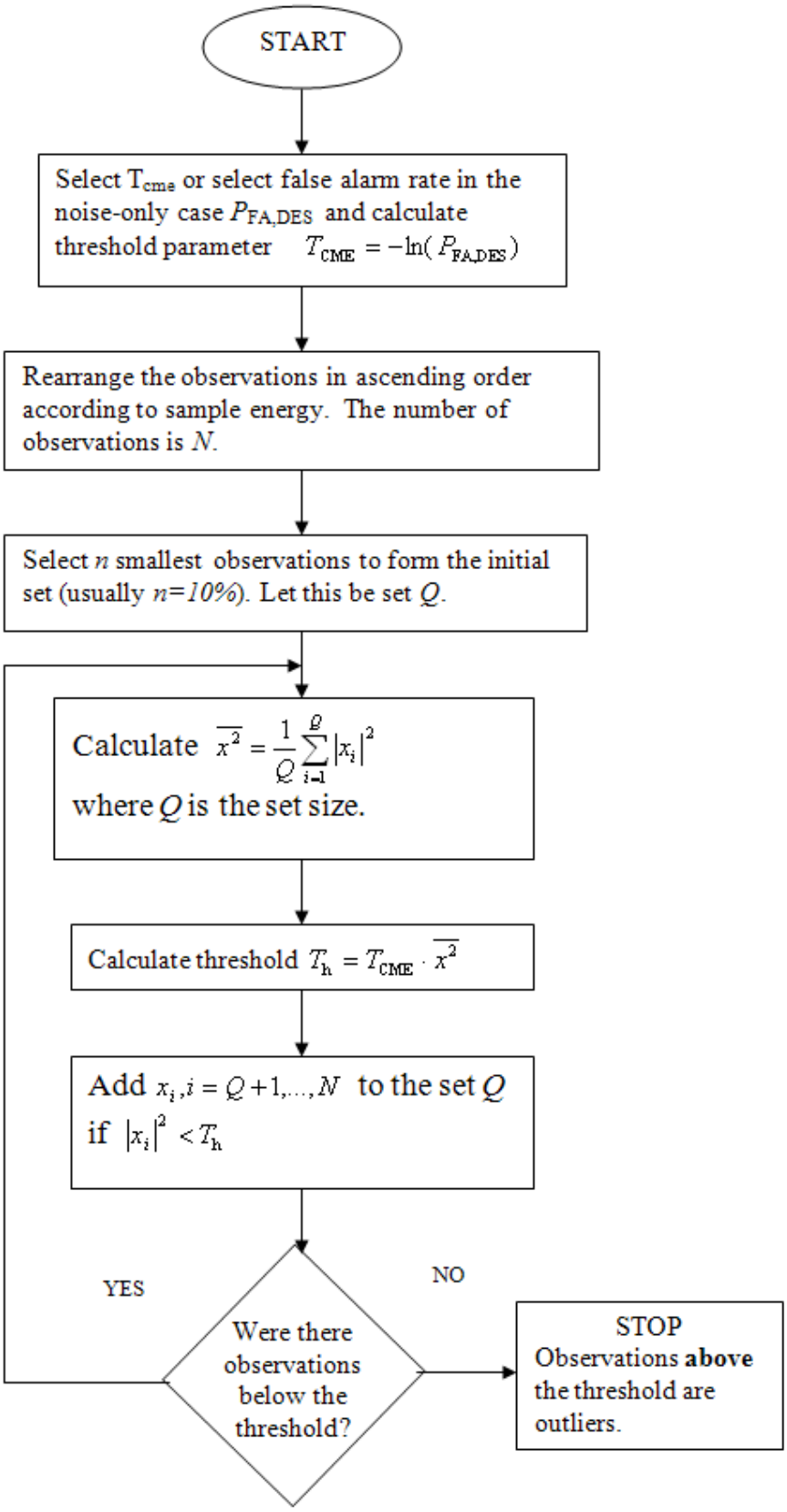

Figure 13 The iterative FCME algorithm

Let us consider the situation when there are M=5 cognitive nodes that send their sensing decisions to the fusion center, so that '1' means that the channel is occupied and '0' means that channel is unoccupied. The PU signal is present randomly 50% of the time and each node locally finds PU signal with probabilities P_d=0.8 and P_{fa}=0.1. Below is presented one decision matrix 'outs' for these 5 nodes for 10 sensing periods (Fig. 3). Node 4 is a malicious node sending always one. That is, column 4 consists of ones.

```
outs =

     0     0     0     1     0
     1     1     1     1     1
     1     0     0     1     1
     0     0     0     1     0
     1     1     0     1     0
     0     0     0     1     0
     1     1     0     1     1
     0     0     0     1     0
     1     1     0     1     1
     0     1     1     1     1
```

Figure 14 Decision matrix, *M*=5 nodes and 10 sensing periods. For each node, *Pd*=0.8 and *Pfa*=0.1. Node 4 is a malicious node sending 'always ones'.

The modified FCME algorithm computes mean of each column. In this case, the received vector of means is V=[0.5,0.5,0.2,1,0.5]. With threshold parameter T_{cme}=1.7, the threshold is T_h= 0.7225. Values in vector V which exceed the threshold T_h are considered to be from a malicious user. Now, $V(4)$=1>0.7725, so node 4 is decided to be a malicious node.

It is also possible to modify the FCME algorithm so that also 'always zero' malicious users are detected. This is possible using threshold parameter <1 and classifying decisions *below* the threshold to be from malicious users. Consider M=8 cognitive nodes with parameters as in the previous case. Now, there is also a malicious user sending always zero. Now, user 1 sends always ones and user 4 sends always zero.

```
outs =

     1     0     0     0     0     1     0     0
     1     1     1     0     1     1     1     1
     1     1     0     0     1     1     1     1
     1     1     0     0     1     1     1     1
     1     0     0     0     0     0     0     0
     1     1     0     0     1     1     0     0
     1     0     0     0     0     0     0     0
     1     0     0     0     0     0     0     0
     1     1     1     0     1     0     1     1
     1     0     1     0     1     1     1     1
```

The received vector of means is V=[1, 0.5, 0.3, 0, 0.6, 0.6, 0.5, 0.5]. With threshold parameters T_{cme1}=1.9 and T_{cme2}= 0.7, the thresholds are T_{h1} =0.8143 and T_{h2} =0.1867. Values

in vector V which are above the threshold T_{h1} and below the threshold T_{h2} are from malicious users. Now, V(1)> 0.8143 and $V(4)$<0. 1867 so nodes 1 and 4 are correctly decided to be malicious nodes.

Monte Carlo simulations were also performed in the case of considering the performance of the FCME algorithm. The PU signal was present randomly 50% of the time and each node finds the PU signal with probabilities P_d=0.8 and P_{fa}=0.1. The size of the initial set was 4 nodes; threshold parameters were T_{cme1}=1.9 and T_{cme2}= 0.7, there were 12 nodes and 20 consecutive decisions were taken into account. The number of Monte Carlo iterations was 10,000. Here, detection was performed only if the malicious node was detected. First, detection of 'always one' malicious user was considered because it causes more harm than a 'always zero' malicious user. When there were one 'always one' malicious user, it was detected in 96% of the cases. No 'always one' malicious users were falsely found. When there was one 'always zero" malicious user, it was found in 99.7% of the cases. 'Always one' malicious users were falsely found in 0.3% of the cases. When there were no malicious users at all, the FCME algorithm falsely found 'always one' malicious user in 0.1% of the cases and 'always zero' malicious user in 0.5% of the cases.

Next, the 'almost always one/zero' case was studied. When there were one 'almost always one' user which sends once decision 0 and otherwise decision 1, it was detected in 90% of the cases. In that case, always zero' malicious users were falsely found in 0.4% of the cases. When there were one 'almost always zero' user which sends once decision 1 and otherwise decision 0, it was detected in 99.5% of the cases. In that case, 'always one' malicious users were falsely found in 0.3% of the cases.

When there was one 'always one' malicious user and one 'always zero' malicious user present at the same time, the FCME algorithm found 'always one' malicious user in 80% of the cases and 'always zero' malicious user in 99.7% of the cases. In the presence of both types of malicious users, the initial set affects to the detection performance of the FCME algorithm, because it takes the smallest samples to the initial set. The performance of the FCME algorithm can be enhanced by leaving one (or two) smallest samples outside the initial set. In that case, the FCME algorithm found 'always one' malicious user in 93% of the cases and 'always zero' malicious user in 93% of the cases. This type of initial set selection has slight effect to the detection performance of 'always one' malicious users.

4.2 References

[Ade11] F. Adelantado and C. Verikoukis, "A Non-Parametric Statistical Approach for Malicious Users Detection in Cognitive Wireless Ad-Hoc Networks ". IEEE International Conference on Communications (ICC) 2011.

[Bar94] V. Barnett and T. Lewis, "Outliers in Statistical Data," Wiley Publisher, 1994

[Bol02] R. J. Bolton and D. J. Hand, "Statistical fraud detection: A review". Statistical Science, 17 (3), pp. 235-255, 2002.

[Bro08] T. Brown and A. Sethi, "Potential cognitive radio denial-of-service vulnerabilities and protection countermeasures: A multi-dimensional analysis and assessment," Mobile Netw. Applicat., vol. 13, no. 5, pp. 516–532, 2008.

[Che08] R. Chen, J. M. Park, and K. Bian, “Robust distributed spectrum sensing in cognitive radio networks,” in Proc. IEEE Conference on Computer Communications (Infocom), 2008.

[Che08b] R. Chen, J.-M. Park, and J. H. Reed, “Defense against primary user emulation attacks in cognitive radio networks,” IEEE J. Sel. Areas Commun., vol. 26, no. 1, Jan. 2008.

[Cla08] T. Clancy and N. Goergen, “Security in cognitive radio networks: threats and mitigation,” in Proc. 3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CrownCom), May 2008.

[Faw97] T. Fawcett and F. Provost, “Adaptive fraud detection”. Data Mining and Knowledge Discovery, 1 (3), pp. 291-316, 1997.

[Kal08] P. Kaligineedi, M. Khabbazian, and V. K. Bhargava, “Secure Cooperative Sensing Techniques for Cognitive Radio Systems,” in Proceedings of the IEEE International Conference on Communications (ICC), pp. 3406-3410, May 2008.

[Kal10] P. Kaligineedi, M. Khabbazian, and V. K. Bhargava, “Malicious User Detection in a Cognitive Radio Cooperative Sensing System,” IEEE Transactions on Wireless Communications, vol. 9, no. 8, pp. 2488-2497, August 2010

[Kha10] Z. Khan, J. Lehtomäki, K. Umebayashi, and J. Vartiainen, ”On the Selection of the Best Detection PerformanceSensors for Cognitive Radio Networks”. IEEESignal Processing Letters, vol. 17, no. 4, April 2010.

[Kha10b]Z. Khan, J. Lehtimäki, M. Mustonen and M.Matinmikko, ” Sensing order dispersion for autonomous cognitive radios “. Sixth International Cognitive Radio Oriented Wireless Networks and Communications (CROWNCOM) 2011 .

[Li10] H. Li and Z. Han, “Catch Me if You Can: An Abnormality Detection Approach for Collaborative Spectrum Sensing in Cognitive Radio Networks,” IEEE Transactions on Wireless Communications, vol. 9, no. 11, pp. 3554-3565, November 2010.

[Raw11] A. S. Rawat, P. Anand, H. Chen and P. K. Varshney, “Collaborative Spectrum Sensing in the Presence of Byzantine Attacks in Cognitive Radio Networks. IEEE Transactions on Signal Processing, vol. 59, issue 2, pages 774-786.

[Var10] J. Vartiainen, “Concentrated signal extraction using consecutive mean excision algorithms”. PhD thesis, University of Oulu, Finland, 2010.
http://jultika.oulu.fi/Record/isbn978-951-42-6349-1

[Var12] J. Vartiainen, "Always One/Zero Malicious User Detection in Cooperative Sensing Using the FCME Method". Accepted to Crowncom 2012, Stockholm, Sweden.

[Wan09] W. Wang, H. Li, Y. Sun, and Z. Han, “Attack-proof collaborative spectrum sensing in cognitive radio networks,” in Proc. Conference on Information Sciences and Systems (CISS), 2009.

[Wan09b] W. Wang, H. Li, Y. Sun, and Z. Han, “CatchIt: detect malicious nodes in collaborative spectrum sensing,” in Proc. IEEE Conference on Global Communications (Globecom), 2009.

[Zar09] S. T. Zargar, M. B. H. Weiss, C. E. Caicedo and J. B. D. Joshi, “Security in Dynamic Spectrum Access Systems: A Survey”. Telecommunications Policy Research Conference, Arlington VA, 2009. http://d-scholarship.pitt.edu/2823/1/SecurityInDSASystems_A_Survey_JSAC.pdf

5 Robust decision-making in spectrum management

5.1 Introduction

Decision-making in cognitive spectrum management depends on a number of assumptions regarding the environment that is operated upon, the context acquisition and filtering processes, and the knowledge about the system's responses upon certain stimuli, summarized in the environment and systems models. In order to optimize decision-making and to minimize the risk of false decisions that may result in inefficient use of scarce resources or harm to incumbents, robustness of decision-making while utilizing incomplete or uncertain information, or dealing with unexpected system behavior must be considered throughout system design and training.

Robust decision-making is understood here as being insensitive with regard to small deviations from assumptions. It is not meant to compensate for a lack of system security or significant misbehavior of a system, nor can it repair an ill-designed system. Robust decision-making depends on the ability to manage uncertainties or, in general, considering strict (severe) uncertainty, risk and certainty of the information upon the state of the environment. Strict uncertainty, which includes ignorance, is the most demanding case. It can be dealt with transforming into either certainty or risk by applying worst-case scenarios (*maximin* principle) or assuming state space properties (insufficient reason).

5.2 Increasing robustness for the QoSMOS CM-SM

Building upon the initial descriptions of the QoSMOS cognition cycle, the interaction of CM-SM and CM-RM, and the internal architecture of the CM-SM cognitive engine in [D2.3, D6.3, D7.2], the basic computational flow is shown in Figure 5-1.

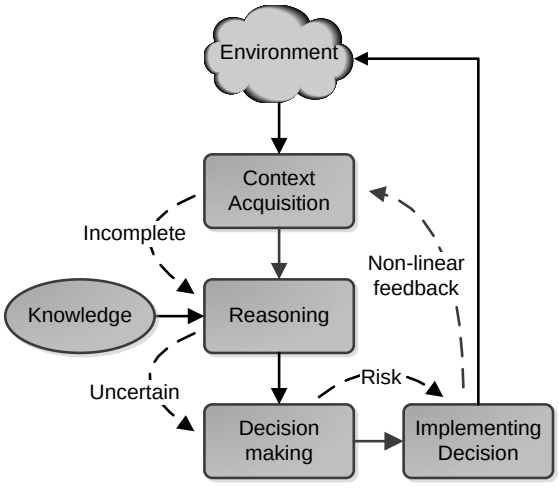

Figure 5-1: Basic computation of decisions in the QoSMOS CM-SM

Context acquisition generates facts from observing the environment, and forwards these facts to a reasoning engine. Since context acquisition in principle cannot observe the environment in whole and depends in this observation on the technical limitations of sensor implementations in terms of timeliness, resolution and accuracy, facts generated by context acquisition inherently represent incomplete information.

Reasoning operates on facts obtained from context acquisition and generates facts as an outcome of applying knowledge to incoming facts. Since knowledge relies on observations (including earlier experience), on models (of the environment and the system) and potentially on reasonable assumptions and extrapolations from earlier experience external to the environment and system under consideration, derived facts are inherently uncertain.

Decision-making operates on facts and generates a decision in terms of a fact to implement, a target parameter or set of parameters of the system, or a system state to attain. The implementation of a decision mediates between the decision taken and the system to configure. It both has knowledge about the syntax and semantics of a decision and the parameters of the system that can be configured. Depending on the complexity of both decision and parameter set, the implementation of a decision is approximate.

Implementing a decision acts upon the environment, potentially affecting the state of the environment in an unexpected way due to incomplete observation or undesired side-effects. In consequence, implementing a decision results in a non-linear feedback on observed context and hence on follow-up decisions.

5.2.1 Enhancing robustness by reasoning on the potential impact of a decision

A first measure to increase robustness is in reasoning on the potential effect of implementing a decision by assessing the impact on an environment model (Figure 5-2). Decisions presumed to generate an undesired effect on the environment would be judged down by this reasoning and may result in re-evaluating facts, aiming to produce a different decision. A well-known realization of this approach is through policy reasoning and enforcing. In the course of this realization decision-making may become iterative, issuing the implementation of a decision only if it has been approved. In order to allow evolving from earlier decisions, final reasoning needs to provide new facts along with a disapproval notification, that decision-making can consider.

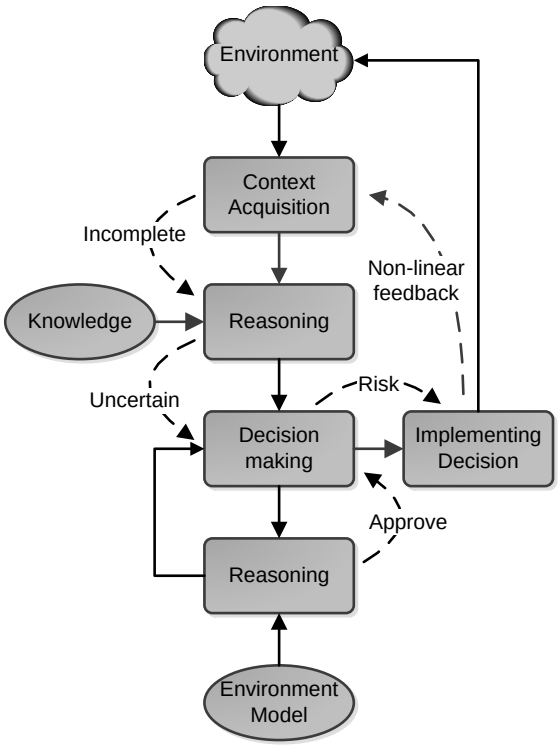

Figure 5-2: Enhancing robustness of decisions by estimating the impact of a decision

The effect on robustness of decision-making is mainly in predicting unfavourable effects on the (modelled) environment before applying decisions. It may result in having no decision at all, which somewhat restricts applicability to protective measures ("better no decision than a bad one"). Thus reasoning on the potential effect of a decision based on uncertain context is an application of the *minimax* principle [Wald45] transforming the problem into a decision-making under certainty through considering worst case scenarios in the environment model or in the policies.

In the first place the environment model focuses on minimizing the risk of false (i.e. harmful) decisions, regardless of its impact on false alarms on the efficiency of decisions. Jointly optimizing the environment model for minimizing the risk of harmful decisions and of false alarms decreasing efficiency by disabling certain decisions due to an uncertainty of the model is subject to further work. It may involve reasoning on the model utilizing case-based reasoning [Aamodt94] as well as an application of the information-gap decision theory [Ben06] to optimize the region of uncertainty of the environment model.

Summarizing, robustness of decision-making can be increased by reasoning upon the potential impact of a decision on the environment, assessing the impact on a model of the environment and prohibiting decisive actions if an undesired impact is likely. Since blocking decisions may result in a deadlock of the cognitive system, this method must be applied carefully and some effort is needed in providing a suitable environment model.

5.2.2 Enhancing robustness by context filtering

Uncertainty of context information clearly introduces risk into decisions and potentially leads to inaccurate or harmful decisions. The main sources of context uncertainty that need to be considered are untrusted context parameters, missing or unobserved parameters, and inaccuracy of observed context parameters.

Context filtering usually refers to the process of selecting or processing parameters that form context information. In the scope of robust decision-making context filtering additionally includes reasoning upon relevance of context parameters and upon trustworthiness of context parameters and sources of context parameters (Figure 5-3).

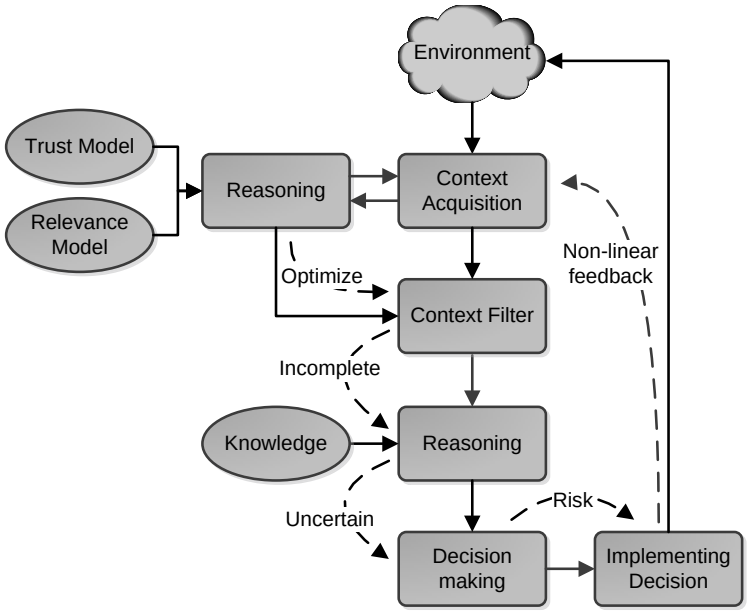

Figure 5-3: Enhancing robustness of decisions by context filtering

In information science, **relevance** can be defined as a "cognitive notion in use when interacting within and without in cases where a matter is at hand" [Sar96]. Relevance is a subjective metric and is valid for a certain information object in a given context, for a given task or topic (also referred to as the "aboutness"), and with regard to the judgement of the receiver of information or that of a larger community (i.e. the "assignment of a value of relevance" in a given context and at a given point in time).

Trust in information basically is a subjective metric similar to relevance of information. It is determined by evaluating and judging trustworthiness by the receiver of information, by a trusted third party or by a community. Trust metrics may be empirical (e.g. based on reputation) or formal (e.g. model-based or probabilistic).

Utilization of common trust and relevance models in distributed decision-making (in contrast to taking local judgements upon trust and relevance) enables to achieve a higher degree of consistency of decisions across diverging decision points in a distributed system, which is a crucial issue for the QoSMOS model utilizing dedicated and distributed CM-RM and CM-SM entities. Hence, in a dynamic environment, some means for exchanging information on the trust level of information sources is needed, and may mandate a certification authority acting as a central point that provides judgements on trustworthiness. In consequence the assumption of transitivity on trust (e.g. trustworthy context information sources always deliver trusted information) and fusion of trust (e.g. less trusted information becomes more trustworthy if confirmed by several less trusted but independent information sources) becomes a system attribute requirement.

In a first approach **uncertainty of context parameters** may be treated with by decision-making under risk, maximising a utility while considering all of the state space and the decision space (i.e. exploring all potential decisions and their potential impact on the environment based on the context and all potential deviations of context from some unknown truth value). That seems impractical for two reasons:

a) Unobserved, untrusted and inaccurate context parameters show a different level of uncertainty. Unobserved parameters are of severe uncertainty, while inaccurate

parameters may be certain (within reasonable physical limits) or may introduce risk. The certainty level of untrusted parameters depends on the trust model applied. Hence, the distribution function on the state space is different for individual context parameters and may vary over time and with operations applied to parameters (e.g. by error propagation), which is significantly increasing computational complexity.

b) Reasoning and decision-making cannot be separated from context acquisition and filtering any longer since decision space depends on the state space of context. For an ontological model, a single well-defined context results in an evident decision (e.g. in case-based reasoning). For other models (that do not rely on a-prior knowledge) the decision space is open and decision-making may become formulated as a game. Here also computational complexity (if not being incomputable) becomes the limiting factor.

The **approach** followed here in the first place rather limits the number of parameters to consider for creating context (in consequence limiting the state space of context) by **reasoning on the relevance of context parameters** and their impact on the decision space. If the impact of a parameter on the decision is significant, it receives higher relevance and higher trust requirements based on the trust and relevance models provided. In consequence, reasoning on context creates precedence for relevant and trusted context parameters. Optimization of trust and relevance model is a dedicated reasoning process similar to developing an environment model. These models currently are considered a-prior knowledge (i.e. are provided prior to operations) and are not yet optimized during operations (i.e. after being deployed) by learning, for example, but may be adaptive to a certain degree.

Nevertheless in situations including severe uncertainty prioritisation only is not feasible since it might narrow the decision space until no decisions can be taken. This situation is best described by having less trusted (or uncertain) context parameters attain high relevance. In these situations filtered context must be tagged and considered accordingly when reasoning on this context in a later stage of processing, for example in choosing an appropriate environment model (e.g. by increasing suitable safety margins).

Since context information in general includes observing several context parameters simultaneously, trust and relevance models must be suited for considering fusion of trust, relevance and uncertainty when performing operations on context parameters:

- Trust, relevance and uncertainty are assumed invariant through unary or monadic operations.
- The impact of dyadic (or more general n-ary) operations on context parameters is assumed as follows:
    - Uncertainty follows well known error propagation models considering, for example, probabilistic models for numerical context parameters (i.e. applying the operation under consideration to the random variables of the parameters under consideration). Non-numerical parameters may need to be represented by describing attributes having a uniform distribution function on the state space.
    - Relevance is additive with the number of parameters under consideration, but invariant with regard to the number and kind of operations applied.

- The trust level receives the minimum value of all parameters involved in an operation if no additional measures are taken. The trust level can be increased by specific operations considering the characteristics of the information sources involved. This approach is for further study.

Summarizing, uncertainty of context is inherent but can be partly compensated by optimizing reasoning in context filtering and in decision-making along with considering a suitable environment model for validating decisions taken.

5.2.3 Enhancing robustness by concurrent reasoning

Decision-making in the context of the QoSMOS CM-SM is a two-step process consisting of problem-analysis and decision as follows:

1. A reasoning process that draws conclusions from facts and deduces new facts required for developing alternative actions;
2. A cognitive process that selects a course of action from several alternatives determined by deduced facts.

In that, a decision may be tentative and may require further reasoning to evaluate possible consequences before taking decisive actions (e.g. by utilizing an environment model). Alternatives developed may be congruent or adverse, complementing or may include or demand further sub-decisions. The latter nicely complements the model of reasoning on trust and relevance discussed above, considering that each tentative decision may have a different relevance or risk (i.e. originated from facts deduced from context of a different level of uncertainty). For example, if a tentative decision deduces from uncertain or untrusted context, it is reasonable to subdivide a decision (e.g. by increasing the number of alternatives) such that the selection of decisive actions is broken down into complementary actions of different relevance or risk level, and giving precedence to actions of higher relevance or lower risk depending on the desired decision. In addition, reasoning on numerical, symbolic or sub-symbolic facts can be distributed to suitable reasoning engines.

Alternatives for the course of action may be developed by distinct **concurrent reasoning processes**, each having a distinct (usually narrowed) scope and potentially operating on a different (usually most relevant for that scope) state space. Clearly, further measures must be taken to ensure that a limitation of the state space considered by partitioning context through, for example, neglecting context parameters does not increase uncertainty of context to an undesired level. Deciding upon which context parameter is of less importance for a certain decision goal, or if parameters considered are independent from those neglected is decision-making under risk by itself. This approach can be seen as having several decision engines in parallel, competing for being recognized for decisive actions based on their individual strength or shortcomings.

Figure 5-4 shows a potential realization where context classification is used to distribute context information considered as relevant for a certain decision goal to parallel focused reasoning engines. Classification and merging of facts deduced by these may consider risk or relevance factors (with regard to the trust and uncertainty consideration of input context classification) to prioritize the outcome of previous reasoning. If realized as a dedicated reasoning engine, classification of facts deduced can be used to detect contradictory or implausible facts, and in that can assist further in selecting suitable reasoning results for decisive actions, or may be feed back to the initial context classification for enhancing initial

classification. An initial state space model is considered a-prior knowledge that may be based upon a-prior knowledge upon context and context parameters.

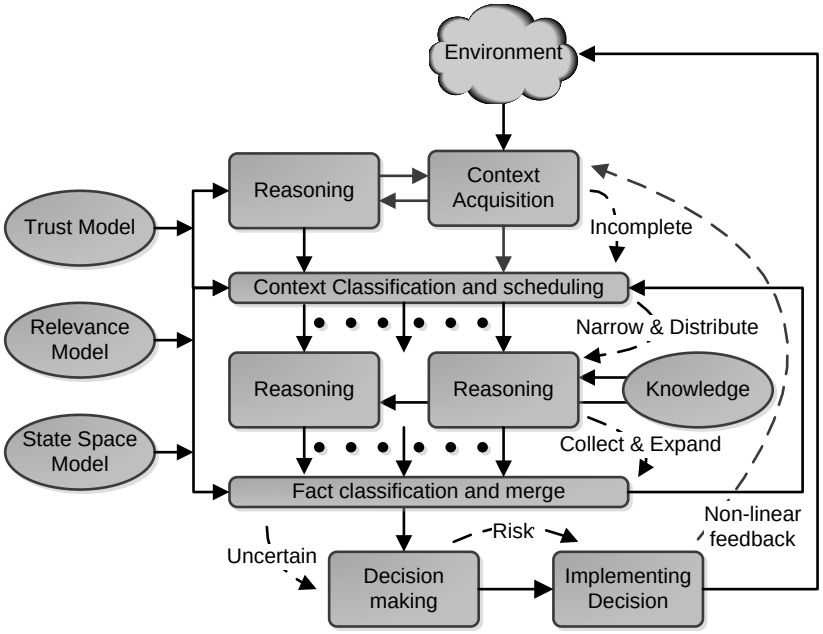

Figure 5-4: Enhancing robustness of decisions by concurrent reasoning

Automated reasoning is a large area of artificial intelligence and touches many related topics such as mathematical logic and proof theory. It is most commonly associated with valid deductive reasoning although a plethora of different principles have been developed beyond that (for more details see [Wos92][Reas11], for more details on methods already considered for QoSMOS see [D6.1]).

- Logical Reasoning – given a precondition, a conclusion, and a rule that the precondition implies the conclusion – is distinguishing between deduction (determining the conclusion), induction (determining the rule) and abduction (determining the precondition).
- Probabilistic (statistical) reasoning is based on probability logic and deductive reasoning. It assigns probabilistic values to facts and inference to handle uncertainty. Most prominent realizations are Bayesian logic (using probability as a measure of a state of knowledge) and Fuzzy logic (using many-valued logic that is approximate rather than fixed and exact). The most prominent application area is in Game theory (decisions of players depend on decisions of other players).
- Non-monotonic reasoning is one in which the axioms and/or the rules of inference are extended to make it possible to reason with incomplete information (in contrast to monotonic reasoning, which presumes that information is complete, consistent and only changes if new facts are added).
- Case-based Reasoning is the process of solving new problems based on the solutions of similar past problems. The process is formalized in a four-step procedure (Retrieve, Reuse, Revise, and Retain). It is based on symbolic (non-numerical, in contrast to numerical or sub-symbolic) data.

- Commonsense reasoning is a generalized form of case-based, logical and fuzzy reasoning operating on huge knowledge bases (i.e. the common sense). It tolerates incomplete knowledge and allows revision of earlier decisions (e.g. mimicking emotional thinking).

Practical realizations of automated reasoning systems often utilize various aspects of the above. For example, a neural network implements both reasoning and learning in a connectionist model thus realizing instance-based, non-monotonic inference, and game realizes non-axiomatic reasoning by utilizing a knowledge base (form the structure of the game a-prior known as optimal for the problem) and learning form experience.

Summarizing, robustness of decision-making can be increased by scheduling context information (e.g. based on trust and relevance associated with distinct context parameters) to concurrent / competing reasoning engines, in that narrowing the scope of a decision towards taking sub-decisions distinctively incorporating more or less risk when applied to the environment. Since this is a complex and rather holistic approach to increase dependability of decision-making, care must be taken when optimizing trust, relevance and environment model, and when developing the state space model, which incorporates relations and dependencies between context parameters that make up the context information used in reasoning on the potential impact on the environment.

5.3 Description of the CM-SM robust decision-making method

5.3.1 Sources of uncertainty

Robust decision-making gets relevant for QoSMOS for a number of reasons. The most prominent are

- Context information from uncertain sensing data (including malicious/defective sensors);
- Trust issues with databases or knowledge repositories (including TV white space databases and policy stores);
- Undesired side-effects of distributed cognitive decision-making (including incomplete environment model/observation);
- Trust issues or uncertain information from actors on the environment (including CM-RM and user equipment acting autonomously).

Security of communications as well as authenticity and integrity of sensor readings is presumed here and can be ensured by well-known means of link encryption, authentication and authorization, certification and revocation.

Sensing-related uncertainty is subsumed by uncertainty of context related to accuracy and trust associated with sources of context information as outlined by previous sections. Context uncertainty includes false or missing context information due to:

- Sensor limitations or shortcomings (e.g. aggravating accuracy, timeliness, positioning or tracking, etc.);
- Defective sensing equipment (e.g. producing occasional outliers for some sensor readings);

- Sensing equipment under attack (e.g. occasionally blinding out sensors by RF jamming);
- Malicious sensing equipment (e.g. modified sensors that conduct attacks).

Often, context uncertainty cannot be tracked down to a certain parameter, cause or origin and thus must be handled by robust decision-making, in consequence increasing the risk for false or harmful decisions.

Trust issues with databases such as white space geolocation databases and related repositories (e.g. policy databases) are assumed to be trusted context sources, and context information obtained from databases thus is also considered trustworthy information. Nevertheless, this trust chain may be corrupted if propagation or terrain models are inaccurate, the database itself is ill-maintained, or its decisions are influenced by other actors, such as untrusted or undetected malicious clients to the database. Although database information has higher relevance compared to other context information (because of a high trust level of the context source and an assumption on transitivity of trust), it still may bear increasing risk in decision-making, which must be considered by an appropriate trust model. The trust model may need to consider that the trust level of a database is not permanent but must be (continuously) approved by an authority or by complementing context from independent (secondary) sources. For example, if a database delivers information that proves unreasonable or implausible after verification by measurements, an alternative database may be consulted prior to decision making.

Another source of uncertainty is in the distributed nature of cognitive managers in QoSMOS which may cause severe uncertainty on context obtained and may result in trust issues upon devices acting on the environment: from the QoSMOS reference model [D2.3] it follows that the CM-SM takes decisions on the composition of a spectrum portfolio, in that responding to an explicit request of the CM-RM or to an instruction of an authority. The portfolio composed then is communicated to the CM-RM and in consequence is applied to the environment in part or in whole.

The issue of **trust in actors** is rising since the CM-RM is not reporting on the way it applies a portfolio obtained to the environment (i.e. if it utilizes all available spectrum allotted or if it keeps part of the spectrum assigned by the portfolio for backup purposes, or leaves this decision top user equipment). Thus, the CM-SM is operating on uncertain context since it cannot assume that the spectrum allotted is used as intended. Both is a trust issue and an issue of incomplete observation jointly.

Incomplete observation and further trust issues also may result from the fact that distributed CM-RM entities act as observers on the environment involving dedicated sensors and user equipment. In consequence the CM-RM is selecting context parameters and operations on parameters following its internal metrics and preferences not involving the CM-SM. The CM-SM in turn obtains (part of) this context through the request of the CM-RM for providing a spectrum portfolio. It may not have the means to judge upon trust, relevance and, hence, uncertainty of context obtained from the CM-RM along with a portfolio request.

5.3.2 Risk factors and metrics

In the scope of cognitive spectrum management uncertain context may cause decisions harmful to incumbents or other coexisting users, or may cause an increase of interference which is annoying or degrading but may not cause harm, or may result in inefficient spectrum

utilization. In general, risk factors need to be mapped onto one or more contributing measurable parameters. To determine the level of contribution of a parameter to a certain risk factor in turn requires suitable metrics for both and a valid model of impact. An initial approach for identifying risk factors and contributing parameters is given below.

1. Identify system vulnerability.
2. Identify risk factors as the metrics of the vulnerability and identify metrics of risk factors.
3. Identify parameters that may affect risk factors identified and set metrics for parameters identified.
4. Identify sources of contributing parameters and determine sources of uncertainty for contributing parameters (consider accuracy and trust levels for parameters under consideration).
5. Identify models describing the effect on the risk factors by contributing parameters.
6. Evaluate relevance of parameters in contributing to a system optimization goal.
7. Evaluate for all relevant subsets of parameters if the effect of contributing parameters on risk factors can be minimized through balancing accuracy, trust and relevance levels.
8. Select most suitable subset of parameters satisfying system optimization goals while minimizing impact on risk factors.

This approach is very similar to the well-known methods for threat analysis: Steps 1…3 determine 'key system vulnerabilities' and associated risk factors while steps 4…5 determine 'attackers' and 'attack goals'. Finally steps 6…8 create a 'resolution plan' which here is based on the assumption that there exists redundancy in context parameters, which allows to select subsets of context parameters from a larger set that can still accommodate system optimization requirements but has minimum impact on risk factors.

The following gives an example how the approach can be applied in practice:

Identify system vulnerability – A failure to obtain close estimate of the interference sensitivity of a victim device may cause harmful interference to an incumbent.

Identify risk factors – The estimate of an incumbent transmitter's signal strength may be too high or the interferer signal may be stronger than expected at the victim device's location.

Identify parameters that affect risk factors – Location of the victim device and signal strength of incumbent and interferer at this location.

Identify sources of contributing parameters and sources of uncertainty of parameters – Positioning devices (position, position accuracy and position trustworthiness), geolocation database query (accuracy of propagation path model, trustworthiness of database), spectrum sensor (position, position accuracy, position trustworthiness, sensor accuracy, accuracy of propagation path model , sensor trustworthiness).

Identify models describing the effect on the risk factors – A linear error on a signal strength estimate will result in a linear error on the derived threshold estimate. A positioning error will cause an error on the threshold as given by the path loss model. Inaccuracy of the

path loss model will cause random errors. All errors are sequentially accumulating as random variables.

Evaluate relevance of parameters – Assuming that system optimization goal is to minimize safety margins and thus to calculate thresholds as precise as possible, position of victim device and incumbent transmitter's signal strength at this location are most relevant. Signal strength can be obtained either by a database query or by a sensor reading. These are redundant parameters potentially having different levels of accuracy and trustworthiness.

Evaluate effect on risk factor – Calculate probability density function (pdf) of outcomes for both database query and sensor reading considering the error factor chain for both alternatives. Estimate pdf of the resulting threshold estimate. **Select most suitable subset of parameters** – If error pdfs of sensor reading and database query are in a similar range then select both to evaluate threshold. If there is a significant difference, chose that with higher trustworthiness, or chose the parameter providing the most narrow error pdf (i.e. providing higher accuracy).

5.3.3 QoSMOS approach for decision-making under risk

The QoSMOS approach for increasing robustness in decision-making is experimental. It relies on reasoning on context (see sect. 5.2.2), concurrent reasoning (see sect. 5.2.3) and on reasoning on a potential impact of a decision (see sect. 5.2.1). Currently, the main focus is on concurrent reasoning and dependencies between 'modules' are studied.

Reasoning on context is integrated with context filtering by balancing accuracy, trust and relevance levels of context when assigning context parameters to reasoning engines. Assuming that each concurrent decision engine has a dedicated goal (e.g. expressed by different top-level rules), may operate on different or on the same input facts. Inferred facts are again handled as context and are evaluated on relevance, trust and accuracy (considering the corresponding attributes of the input facts) and are filtered before forwarding them to decision-making.

For example, two identical inference engines may operate on different (but partially congruent) sets of input facts and may produce the same inference. This may allow concluding that the current rule-set is robust to some uncertainty of input facts. If they provide a different inference, it may be concluded that there exist input facts of unexpectedly high relevance to a decision.

In the course of balancing accuracy, trust and relevance attributes for input parameter selections, concurrent reasoning engines may operate on a complete set of input facts in parallel to a narrowed set of input facts. Inferred facts than may complement each other or may narrow a decision. The latter is relevant for QoSMOS since it may allow 'exchanging accuracy with area

For example, by spatial narrowing (e.g. matching the space of higher accuracy of a path loss function) a wider decision may bear high risk to obtain a potentially harmful decision, but a higher certainty of decisions may be obtained for a closer space lowering the risk of a harmful decision. This approach potentially could be applied to some white space / grey space decisions if path loss functions or terrain models may bear areas of higher uncertainty to avoid.

Redundancy of input context is a key element for robust decision making. In particular a QoSMOS CM-SM may benefit from spatial or temporal redundancy of input context (e.g.

utilizing context information obtained from multiple CM-RM instances or from distributed sensing even if not mandated by the optimization goal. In addition, Context parameters of high relevance but below a certain threshold of accuracy and trustworthiness may be replaced by computed or surrogate context sources.

For example, a certain spectrum sensor showing insufficient accuracy may be replaced by multiple surrounding sensors and by applying a suitable propagation model to sensor readings. The QoSMOS approach is considering redundancy in its context reasoning stage and may decide to schedule the inaccurate sensor to a different reasoning engine than its surrounding sensors. Comparing outcomes may lead to a decision to exclude the inaccurate sensor from further generating input facts.

5.4 Examples for robust decision-making on spectrum portfolio composition

Composition of spectrum portfolios in QoSMOS mainly relies upon decision-making for the following cases:

1. Decision to include a certain frequency band with a portfolio.
2. Decision to remove a certain frequency band from a portfolio.
3. Decision to modify (narrow or extend) a certain frequency band in a portfolio.
4. Decision to deploy a portfolio towards a certain spectrum user.
5. Decision to withdraw a portfolio from usage by a certain spectrum user.

Clearly, those cases rely upon ancillary decisions such as which frequency band to consider for inclusion, modification or removal from a portfolio, or which portfolio to deploy towards (or revoke from) which spectrum user. [D2.2] section 6.5 lined out the framework implemented for the purpose of portfolio exchange between CM-RM, CM-SM and portfolio repositories. The protocols given there are the basis for implementing decisions.

The rule set for decision-making currently is subject to ongoing studies, which does not allow for the time being to provide an unmitigated overall description of the decision-making process. Instead, a number of examples will be given next having a focus on robustness in decision-making, outlining the process of portfolio composition by discussion of some of the ancillary decisions required.

5.4.1 Enhancing robustness of portfolio composition relying on database queries

Querying a geolocation database is one of the most prominent use cases in portfolio composition. The database here is considered a context provider for one or more CM-SMs. A portfolio is composed from the fact that certain frequency bands are unused for the location queried, which involves context provided by a database as well as context obtained from collaborating CM-SMs querying the same database and from spectrum sensors available to the CM-SM (either direct or via requesting a CM-RM). The flow of basic actions is given below:

- Trigger condition: A CM-RM requests an amount of spectrum from a CM-SM.
  CM-SM selection criteria for CM-RM: A CM-SM responsible for a certain frequency band (e.g. TV bands) and for a certain area (e.g. nation, state, city).

Mandatory context to be provided by CM-RM when requesting spectrum: Amount of spectrum requested, upper and lower frequency limits to consider, minimum amount of contiguous frequency spectrum required, geographical extent of intended use.

- Context acquisition and filtering: Queried CM-SM acquiring context from collaborating CM-SM and co-located sensors to increase robustness.
  Context related to coexistence: Spectral map composed from portfolios already deployed to neighboring areas. Spectrum utilization (or interference) observed by sensors for this spectral map.
  Context related to robustness: Incumbent activity observed by sensors for this spectral map including adjacent frequency bands.
  Context related to resource allocation: User population (or temporal activity) for frequency bands of the spectral map.

- Reasoning done by CM-SM: Creating a suitable interference map and spectrum utilization map.
  Facts regarding spectrum utilization: Relative metrics comparing adjacent resources (spatial, temporal or spectral for frequency band utilization, user population and interference level produced) expressed in form of logical inference.
  Facts regarding robustness: Facts upon uncertainty of facts, derived from relevance, accuracy and trust level of a logical inference based on relevance, accuracy and trust of context and context source contributing.

- Decisions taken by CM-SM: Decision to include a certain frequency band into a portfolio and to deploy that portfolio to the requesting CM-RM (preferences of frequency bands are given by facts).
  Decision on choice of context source: Considering relevance and accuracy of context provided in relation to trust of context source selected, to query CM-RM or database with significant trust level first.
  Decisions on algorithms to involve: Linking algorithmic procedures with inference rules relying on comparisons, sorting or iterations in a selection process, potentially including ancillary reasoning (probabilistic, non-monotonic, symbolic …) to avoid extensive rule sets.
  Decision on optimization goal: Preference of optimization goal to consider (e.g. minimizing interference, maximizing use of contiguous bands, maximizing number of spectrum users, increasing safety margins and minimizing potential harm to incumbents …).
  Decisions on deployment of portfolio: Verifying composed portfolio against spectrum map estimating impact of dependent parameters by algorithmic means (i.e. estimating parameters not considered by primary optimization goal, such as interference if optimized for maximum number of users). Reject deployment if boundaries (e.g. regulatory) are violated and rerun optimization based on a different optimization goal.

Basic context information required to construct an initial spectrum portfolio (for later optimization by reasoning and decision-making) is obtained from a geolocation database which is the sole context source when robustness is not of major interest. From the perspective of increasing robustness by suitable selection of context sources, multiple databases or complementary spectrum sensing might be considered. **Figure 5-5** depicts the flow of ancillary decisions in case a single database is queried as well as having available

multiple databases or spectrum sensors. The decision flow shown results from judging risk factors related to trustworthiness of context sources as an example.

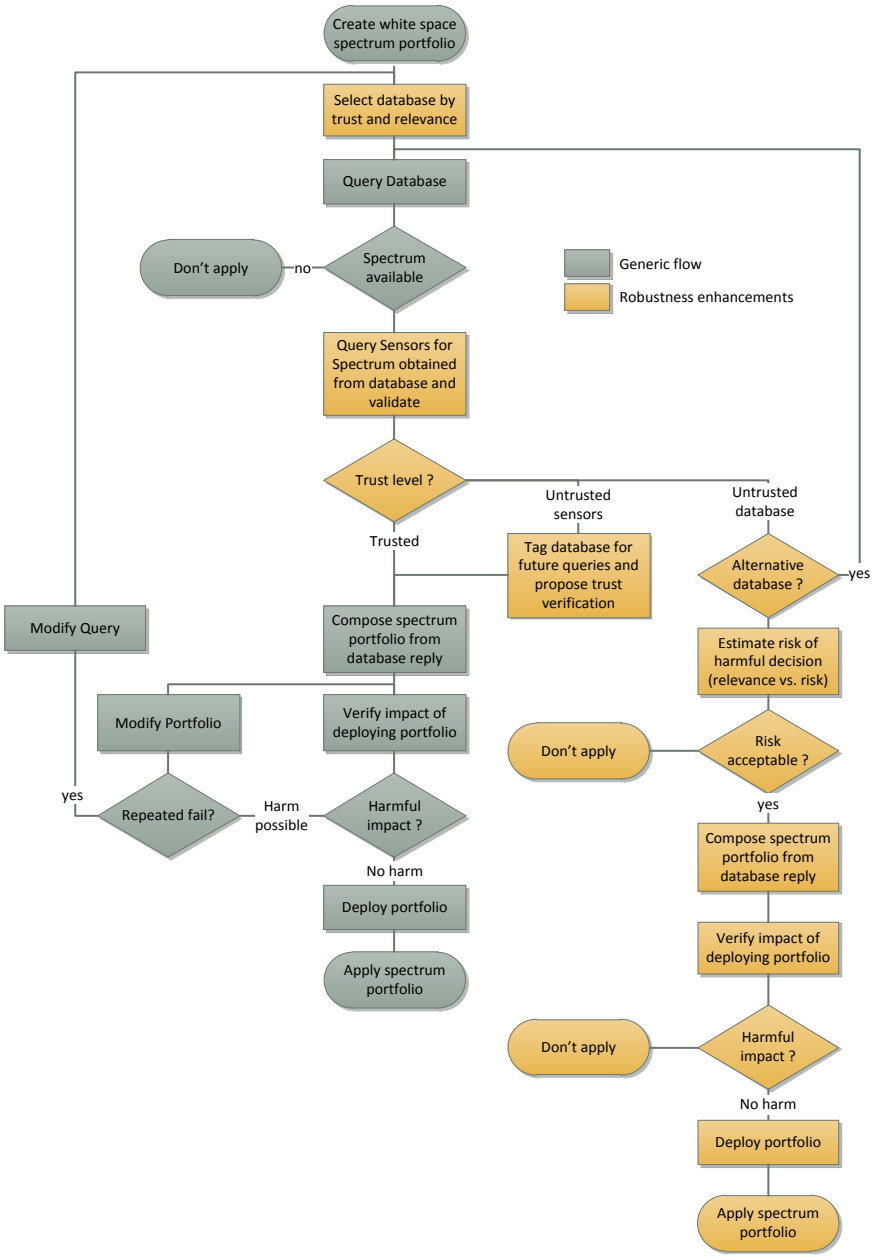

Figure 5-5: Sample decision flow for robust database queries

5.5 References

[Wald45] A. Wald, "Statistical decision functions which minimize the maximum risk", The Annals of Mathematics, 46(2), 1945, 265-280.

[Ben06] Y. Ben-Haim, "Info-gap decision theory: decisions under severe

uncertainty", Academic Press, 2006

[Aamodt94] A. Aamodt, E. Plaza, "Case-Based Reasoning: Foundational Issues, Methodological Variations, and System Approaches", Artificial Intelligence Communications 7 (1994): 1, 39-52.

[Sar96] T. Saracevic, "Relevance reconsidered", Proceedings of the second conference on conceptions of library and information science (CoLIS 2), 1996, 201-218

[Wos92] L. Wos; R. Overbeek; E. Lusk; J. Boyle, "Automated reasoning: Introduction and Applications", McGraw Hill 1992.

[Reas11] "Journal of Automated Reasoning", Volume 1 / 1985 - Volume 47 / 2011, ISSN 0168-7433 (Print) 1573-0670 (Online), Springer Netherlands

[D2.2] QoSMOS Deliverable D2.2

[D2.3] QoSMOS Deliverable D2.3

[D6.3] QoSMOS Deliverable D6.3

[D7.2] QoSMOS Deliverable D7.2

[D6.1] QoSMOS Deliverable D6.1

6 Cognitive Spectrum Utilization for Stable, Dense Indoor Femtocells

6.1 Introduction

In this chapter, we consider the context of orthogonal frequency division multiplexing access (OFDMA) based indoor femtocells, overlaid to the existing macrocell by spectrum sharing. For given sub–channels available at the OFDMA femtocells, we propose a cognitive spectrum management functionality to enhance reliability of the spectrum management operation from the femtocell perspective by investigating a joint energy and spectrum (i.e., sub–channels) utilization for dense indoor femtocell networks. This aims not only for sharing the spectrum with the conventional macrocell, but also for robust spectrum and energy resource management to the finite, random sub-channels available at the dense femtocells.

To this end, overall energy and spectrum management among the femtocells is studied in this section. In particular, we aim at

(i) Mathematically formulating the spectrum and energy usage by indoor femtocells for the control and data transmissions,

(ii) Evaluating the outage capacity of each femtocell under the requirement of overall interference towards the incumbent macrocell receiver,

(iii) Developing a cognitive functionality of self–organizing the number of active sub-channels (spectrum) and their energy usage in a distributed manner.

From an information-theoretic perspective, characterization of the maximum achievable rates of the dense indoor femtocell downlink fading channels is provided for in the allowance for the outage rate. The performance of the proposed scheme is analyzed by deriving an accurate and closed-form expression for the outage capacity at the femtocells, each of which limits its energy usage for the protection of licensed users and thereby co-exists with the macrocell. Unlike the conventional approaches [Ashraf wcnc10][Lopez CM09], this work takes into account the energy and spectrum management for the control and the data. We also provide the numerical results that illustrate the presence of opportunities that the achievable outage capacity per femtocell is maximized under realistic constraints by properly finding the energy usage and the number of active sub–channels per femtocell.

6.2 Dense Indoor Femtocells case and problem formulation

As shown in Figure 8-1, we consider L femtocells, each of which serves Nl femtocell user equipments (FUEs) in a radius (r) and, for the *downlink*, L femtocells cognitively access the radio spectrum, licensed to the under-laid macrocell network. Let each femtocell coordinate to each other and orthogonally operate over the available incumbent channels in the frequency domain while avoiding the co–tier interference among neighbouring femtocells.

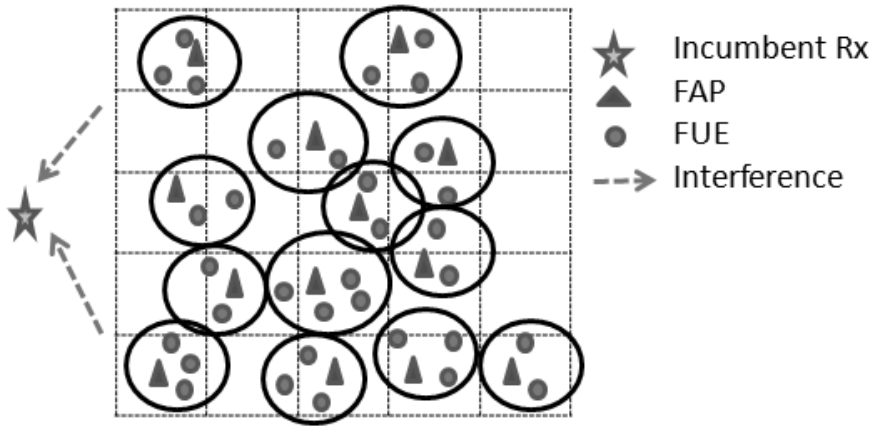

Figure 8-1 Multiple OFDM femtocells deployment in a 5x5 grid enterprise environment layout.

For the downlink of each femtocell, we employ orthogonal frequency division multiplexing (OFDM, e.g., 3GPP's LTE). Particularly, let each FUE in a certain femtocell be allocated to $\overline{n}$ sub–channels (or, equivalently, sub–carriers) for given *m* incumbent radio channels, where it is assumed that *m* channels are originally licensed to a macrocell UE near the femtocells and for the simple analysis and without loss of the generality, the value of *m* is given to be equivalent to the sum of all sub-channels available among FUEs in the *L* femtocells.

For given *m* inactive channels, we are aware of the energy usage at two planes inherent in the networked femtocells: there exists the energy usage at the control and the data planes on every time slot.

Firstly, in the control plane, exchange of control signaling between FAPs and FUEs happens. In particular, for given $\overline{n}$ sub–channels per FUE, the FAP *l* can communicates with the local spectrum control module in the network controller and is informed to randomly activates only a subset of n_l ($\leq \overline{n}$) sub–channels per FUE according to the Uniform distribution at every time slot. This random activation enables that each entry (i.e., each sub–channel) in the subset is equally likely activated. Then, among N_l FUEs at femtocell *l*, $N_l n_l$ sub–channels result in active at a given time slot. For given such $N_l n_l$ active sub–channels, therefore, the exchange of signalling occurs for the purpose of the CM-RM functionality (e.g., radio resource scheduling.) Here, let the average power control be applied to each active sub–channel *i* so that the desired power level P_c at each sub-channel is received on average [D6.3 Ch4.5].

Secondly, for given $N_l n_l$ active sub–channels per femtocell, the opportunistic radio spectrum scheduling scheme [Q.Ma Jul05], [D.Tse 05] is applied to the data plane. That is, only the best among $N_l n_l$ active sub–channels is allocated for the data transmission at femtocell *l*, $\forall l$ at each time slot. The selection criterion of the best sub–channel is to select the best whose SINR is defined as the maximum among the SINRs of sub-channels. Let the data transmission by the chosen best be also made by the average power control, similar to the control plane, so that P_d is the desired receiving power for the data.

Based on the above proposed methods, the resulting sum rate at each femtocell can be given by

$$C_l = \log_2(1+\rho_l) = \log_2(1+\bar{\rho}_l x_l P_d) \text{ for } l \in \{1,...,L\},$$

where $x_l = \max_i x_{li}$ and $\bar{\rho}_l$ denotes the average normalized SINR, i.e., $\bar{\rho}_l = \Theta/(I^{mf} + \sigma^2)$.

6.3 Overall Energy Usage by Networked Femtocells

We address the aggregate energy usage between all the FUEs and the networked femtocells at both the control and the data planes from the signal processing perspective. For simplicity in analysis and without loss of the generality, we consider hereafter the worst case interference, where all the FUEs are located at the cell-edge of each femtocell and thus the resulting downlink energy usage per femtocell is largest. This leads to an asymptotic situation where the interference I_{fm} caused by the femtocells results in highest.

For the mathematical treatment of the energy usage between FUEs and femtocells, it is first referred to the energy usage by multiple users in a single cellular environment [Y.Ko Aug10]. When extending such energy usage to those of the multiple femtocells, we can formulate that the energy usage at each femtocell, comprising multiple femtocell UEs, is decomposed into two energy usage terms; energy usage at the control plane, that at the data plane. This can be represented for a given n_l ($\leq \bar{n}$) as

$$E_a = \sum_{l=1}^{L} N_l n_l \psi_l T_f (P_c + P_d).$$

where ψ_l is the propagation-loss compensation between FUEs and the FAP *l*. Notice that this sum energy can be obtained as the sum of individual energy usage at each femtocell.

6.4 Outage Sum Capacity Analysis

Based on the above energy usage model, it is now aimed at analyzing the outage sum capacity of a femtocell ofinterest. Particularly, notice that the amount of the above energy usage is causing the interference I_{fm} at the incumbent receiver. As per [D6.3 Ch4.5], when limiting I_{fm} to $I_{fm} = I_o$, we can have that

$$P_c = \frac{\mathrm{I}_o}{\sum_{\mathrm{l}} \left(N_l \bar{n} + \eta^{-1}\right) \left(\frac{d_l}{r_l}\right)^{-L_f}}.$$

Also, when for a given n_l ($\leq \bar{n}$), fixing the sum energy to the energy usage in the case when $n_l = \bar{n}$, P_d in a given E_a can be given when $n_l \leq \bar{n}$ by

$$P_d = N_l\left(\bar{n} - n_l + \eta^{-1}\right)P_c.$$

By inserting this into C_l, the sum capacity per femtocell can be represented accordingly. Then, let the outage probability be defined as the probability that C_l is less than $C_{out,l}$ and let this outage probability be very low such that $\Pr\left(C_l \le C_{out,l}\right) \le \varepsilon$. According to the above expression for C_l and by using the cumulative density function of $x_l \sim \chi^2_{2k}$, the expression for $C_{out,l}$ can be achievable as

$$C_{out,l} = \log\left(1 + \bar{\rho}_l P_c N_l (\bar{n} - n_l + \eta^{-1}) F_x^{-1}(\varepsilon)\right),$$

and namely, it is the outage capacity of a femtocell.

6.5 Simulation Results

For simulation results, we consider a femtocells deployment in a 5x5 grid layout of geographical environment such as, for example, enterprise environments. Here, both penetration and propagation losses are in line with 3GPP deployment parameters [3GPP ts36.211]. On this layout, the co–channel deployment of $L \in \{8,16\}$ femtocells is considered, where each is randomly deployed and intends to access the radio spectrum licensed to the macrocell.

Let $\bar{n}$ inactive sub-channels be given to each FUE. Here, the ratio of the energy usage between control and data planes at each sub–channel is fixed to $\eta = 3/4$ that is referred to the case when transmitting 3 and 4 OFDM symbols for the control and the data, respectively, at every frame in 3GPP LTE Femtocells. Due to the downlink communications between L femtocells and their FUEs, the incumbent macrocell user deployed near the femtocells should experience the interference from the femtocells and this should be no greater than $I_o = -30$dB.

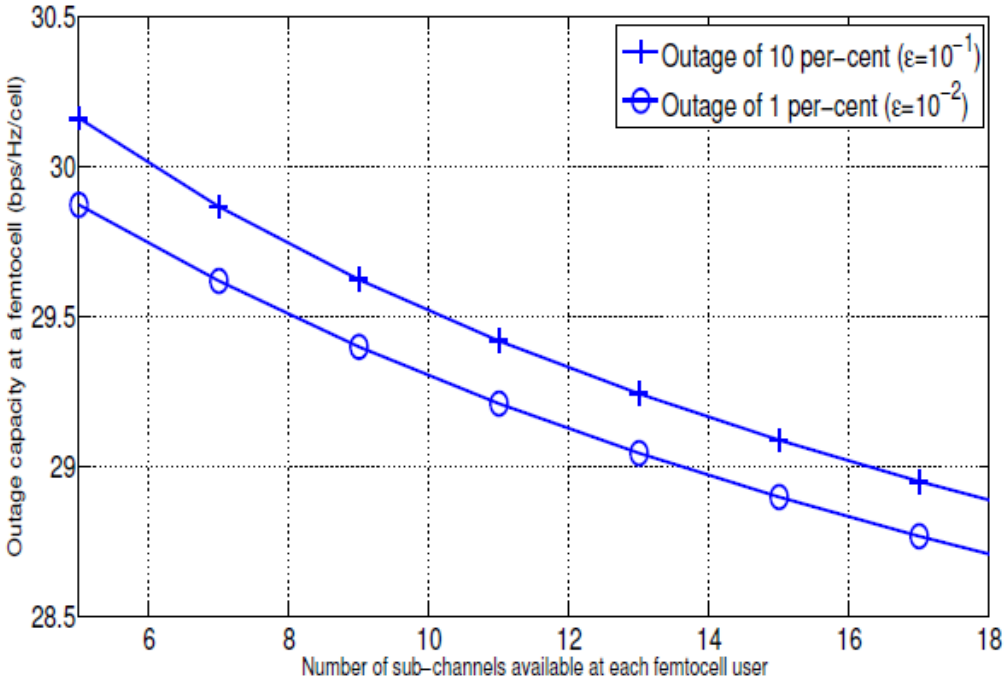

Figure 8-2 Outage capacity at a femtocell versus the number of sub-channels available at various values of the target outage probability (i.e., $\varepsilon \in \{0.01, 0.001\}$).

As illustrated in Figure 8-2, the outage capacity of a femtocell is shown to decrease with the number of sub-channels available at various values of the given target outage probability when 16 femtocells each having 4 femtocell users are deployed. For the illustrations in this figure, it is assumed that all sub-channels are active at every time slot (i.e., $n = \bar{n}$). Intuitively, more the number of sub-channels, less the energy usage by femtocells are. The latter is in order not to cause too much interference towards the incumbent receiver and thus protect the licensed users.

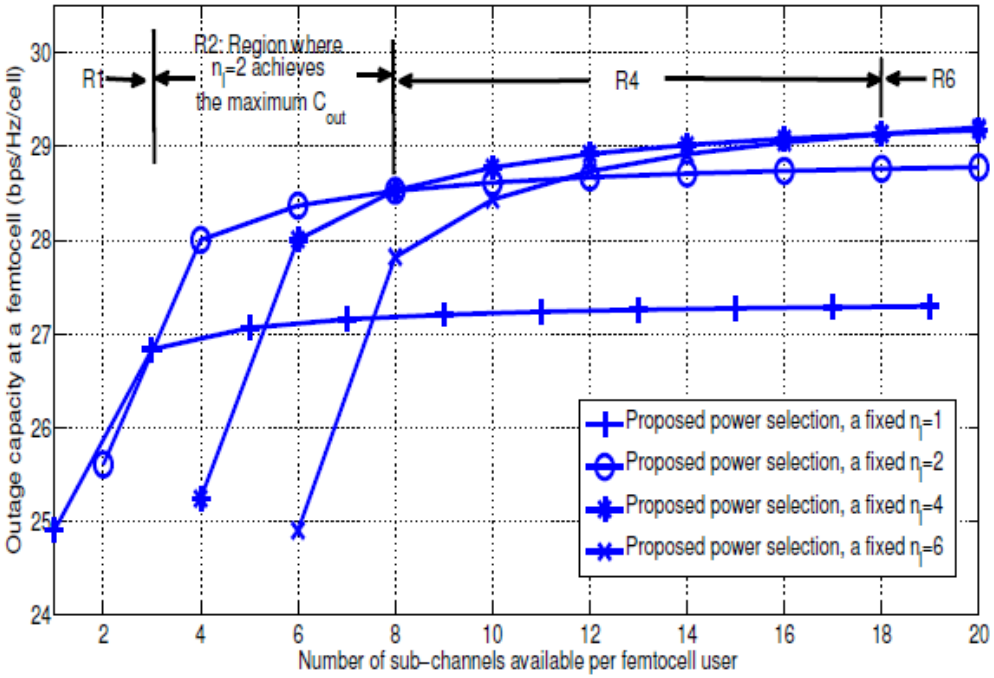

Figure 8-3 Impact of activating a subset of all sub-channels on the outage capacity is illustrated.

Furthermore, it can be found in Figure 8-3 that for a given number of sub-channels, activating only a subset of $n_l \leq \bar{n}$ sub-channels and adjusting their energy usage levels benefit higher outage capacity without requesting an extra energy usage in a femtocell. Therefore, it is shown in this figure that using the proposed scheme results in the outage capacity as an increasing function of the number of sub-channels available. Also, it is illustrated in this figure that there can exist the presence of opportunistic, discrete regions of n_l, maximizing the outage capacity.

6.6 Conclusions

This section considered the CM-SM opportunistic functionality: the cognitive management of power and spectrum resources for the networked co-channel femtocells, overlaid to the

macrocell. It was aimed at cognitively managing the spectrum resources among the femtocells by investigating the opportunities for the spectrum and energy usage balance between the control and the data planes per femtocell. Formulating the practical energy and spectrum usage model at the networked co–channel femtocells, the proposed CM-SM functionality showed that the proper management of both the power levels and the size of the subset of active spectrums alongside the CM-RM functionality (i.e., radio resource scheduling) can improve the stability of the femtocell in terms of the outage capacity, while co-existing with the licensed macrocell receiver.

6.7 References

[Ashraf wcnc10] I. Ashraf, L. T. W. Ho, and H. Claussen, “Improving energy efficiency of femtocell base stations via user activity detection,” in *Proc. IEEE Wireless Communications and Networking Conference (WCNC)*, 2010, pp. 1–5.

[Lopez CM09] D. Lopez-Perez, A. Valcarce, G. de la Roche, and J. Zhang, “OFDMA femtocells: A roadmap on interference avoidance,” *IEEE Commun. Mag.*, vol. 46, no. 9, pp. 59–67, Jun. 2009.

[D6.3 Ch4.5] QoSMOS D6.3, `` Initial description of cognitive and opportunistic functions of the spectrum management framework’’, at *http://www.ict-qosmos.eu,* Jan. 2012.

[Q.Ma Jul05] Q. Ma and C. Tepedelenlioglu, “Practical Multiuser Diversity With Outdated Channel Feedback,” *IEEE Trans. Veh. Technol.*, vol. 54, pp. 1334–1345, Jul. 2005.

[D.Tse 05] D. Tse and P. Viswanath, *Fundamentals of wireless communication*, 1st ed. Cambridge University Press, 2005.

[Y.Ko Aug10] Y. Ko, S. A. Vorobyov, and M. Ardakani, “How much multiuser diversity is required for energy-limited multiuser systems?” *IEEE Trans. Signal Process.*, vol. 58, no. 8, pp. 4367–4378, Aug. 2010.

[3GPP ts36.211] The 3rd Generation Partnership Project TS 36.211, “Evolved universal terrestrial radio access (E-UTRAN); physical channels and modulation (release 9),” vol. 9.1.0, Mar. 2010.

7 Robustness of interference management

In this chapter we consider the mathematical steps required for robust calculation of interference caused by white-space devices to TV reception.

7.1 Wanted DTT signal

The dB power of the wanted DTT signal received in a particular pixel is defined to be $\mathbf{P_{RW}}$ and it is generally accepted that this can be modelled as a normal random variable with mean and variance values represented by $\mu_{\mathbf{RW}}$ and $\sigma^2_{\mathbf{RW}}$, respectively, which usually have to be derived using numerical analysis techniques.

7.2 Unwanted DTT Signal

The sum of the powers of the unwanted DTT signals received in the same pixel as the wanted DTT signal, in dB, is defined to be $\mathbf{P_{RU}}$ and it is generally accepted that this can be approximated as a normal random variable with mean and variance values, represented by $\mu_{\mathbf{RU}}$ and $\sigma^2_{\mathbf{RU}}$, respectively, which usually have to be derived using numerical analysis techniques.

7.3 Unwanted White Space Interferer Signal

The sum of the powers of the white space interference signals received in the same pixel as the wanted DTT signal, in dB, is defined to be $\mathbf{P_{RI}}$ and it is generally accepted that this can be approximated as a log-normal random variable with mean and variance values, represented by $\mu_{\mathbf{RI}}$ and $\sigma^2_{\mathbf{RI}}$, respectively, which usually have to be derived using numerical analysis techniques.

7.4 Location Probability

To derive the location probability the difference between the wanted DTT signal power and the sum of the unwanted DTT signal powers is used, and in the liner domain this can be expressed as

$$10^{\frac{P_R}{10}} = 10^{\frac{P_{RW}}{10}} - \sum_{1}^{Nu} 10^{\frac{P_{Un}}{10}} = 10^{\frac{P_{RW}}{10}} - 10^{\frac{P_{RU}}{10}} \quad \ldots..(1)$$

where N_U is the number of unwanted DTT interferers, random variable P_{Un} is the n^{th} unwanted DTT's signal power in dB. P_{RW} and P_{RU} are as defined earlier and are also in dB.

It follows from (1) that in the dB domain

$$P_R = P_{RW} - P_{RU} \text{ .....(2)}$$

Because P_{RW} and P_{RU} are being assumed to be normally distributed, then P_R will also be normally distributed and it follows from the rules of subtracting random variables that its mean and variance values will be given by

$$\mu_R = \mu_{RW} - \mu_{RU} \text{ .....(3)}$$

$$\sigma_R^2 = \sigma_{RW}^2 + \sigma_{RU}^2 \text{ .....(4)}$$

Substituting (3) and (4) into (A10) it is easily shown that the location probability, q_1, is given by

$$q_1 = P(P_R > P_{RW\min}) = \frac{1}{2} erfc\left(\frac{1}{\sqrt{2}} \cdot \frac{P_{RW\min} + \mu_{RU} - \mu_{RW}}{\sqrt{\sigma_{RW}^2 + \sigma_{RU}^2}} \right) \text{.....(5)}$$

where P_{RWmin} is the noise limited DTT receiver sensitivity in dB.

Because P_R is dependent on subtracting random variables, it can be shown that there is an alternative expression for (5), and that this is given by

$$q_1 = P(P_R > P_{RW\min}) = 1 - \frac{1}{2} erfc\left(-\frac{1}{\sqrt{2}} \cdot \frac{P_{RW\min} + \mu_{RU} - \mu_{RW}}{\sqrt{\sigma_{RW}^2 + \sigma_{RU}^2}} \right) \text{.....(6)}$$

7.5 Degraded Location Probability

To derive the degraded location probability the difference between the wanted DTT signal power and the sum of the unwanted DTT and white space signal powers is used, and in the linear domain this can be expressed as

$$10^{\frac{P_{RD}}{10}} = 10^{\frac{P_{RW}}{10}} - \left(\sum_{1}^{Nu} \left(10^{\frac{P_{Un}}{10}} \right) + \sum_{1}^{Nw} \left(10^{\frac{P_{In}}{10}} \right) \right) = 10^{\frac{P_{RW}}{10}} - 10^{\frac{P_{RU}}{10}} - 10^{\frac{P_{RI}}{10}} \text{.....(7)}$$

where N_W is the number of white space interferers, random variable P_{In} is the n^{th} interferer's signal power in dB. P_{RW}, P_{RU} and P_{RI} are as defined earlier and are also in dB.

Therefore, it follows from (7) that in the dB domain

$$P_{RD} = P_{RW} - P_{RU} - P_{RI} \text{ .....(8)}$$

Because P_{RW}, P_{RU} and P_{RI} are being assumed to be normally distributed, then P_{RD} will also be normally distributed and it follows from the rules of subtracting random variables that its mean and variance values will be given by

$$\mu_{RD} = \mu_{RW} - \mu_{RU} - \mu_{RI} \text{ .....(9)}$$

$$\sigma^2_{RD} = \sigma^2_{RW} + \sigma^2_{RU} + \sigma^2_{RI} \text{ .....(10)}$$

which for convenience will be expressed as

$$\mu_{RD} = \mu_{RWU} - \mu_{RI} \text{ .....(11)}$$

$$\sigma^2_{RD} = \sigma^2_{RWU} + \sigma^2_{RI} \text{ .....(12)}$$

where

$$\mu_{RWU} = \mu_{RW} - \mu_{RU} \text{ .....(13)}$$

$$\sigma^2_{RWU} = \sigma^2_{RW} + \sigma^2_{RU} \text{ .....(14)}$$

Substituting (11), (12), (13) and (14) into (A10) it is easily shown that the degraded location probability, q_2, is given by

$$q_2 = P(x > P_{RW\min} + k_I) = \frac{1}{2} erfc\left(\frac{1}{\sqrt{2}} \cdot \frac{P_{RW\min} + k_I - (\mu_{RWU} - \mu_{RI})}{\sqrt{\sigma^2_{RWU} + \sigma^2_{RI}}} \right) \text{.....(15)}$$

where K_I is the interference margin in dB.

Because P_{RD} is dependent on subtracting random variables, it can be shown that there is an alternative expression for (15), and that this is given by

$$q_2 = P(x > P_{RW\min} + k_I) = 1 - \frac{1}{2} erfc\left(-\frac{1}{\sqrt{2}} \cdot \frac{P_{RW\min} + k_I - (\mu_{RWU} - \mu_{RI})}{\sqrt{\sigma^2_{RWU} + \sigma^2_{RI}}} \right) \text{.....(16)}$$

7.6 Special Case of a Single White Space Interferer

For the special case of a single interferer P_{RI} can be expressed as

$$10^{\frac{P_{RI}}{10}} = 10^{\frac{P_{TI}K_W G}{10}} \quad \text{.....(17)}$$

where P_{TI} is the transmit power in dB of the white space interferer, k_W is the fraction of P_{TI} in dB that appears at the output of the DTT receiver's filter and G is the effective path loss in dB.

It follows from (17) that in the dB domain

$$P_{RI} = P_{TI} + k_W + G \quad \text{.....(18)}$$

Therefore, knowing that it is generally accepted that G is a normally distributed random variable in the dB domain, then it follows from the rules of adding constants to a random variable that

$$\mu_{RI} = P_{TI} + k_W + \mu_G \text{.....(19)}$$

$$\sigma_{RI}^2 = \sigma_G^2 \text{.....(20)}$$

Substituting (13), (12), (19) and (20) into (15) and (16) it will be found that they can be expressed as

$$q_2 = P(x > P_{RW\min} + k_I) = \frac{1}{2} erfc\left(\frac{1}{\sqrt{2}} \cdot \frac{P_{RW\min} + k_I - \left(\mu_{RWU} - \left(P_{TI} + k_W + \mu_G\right)\right)}{\sqrt{\sigma_{RWU}^2 + \sigma_G^2}} \right) \text{.....(21)}$$

$$q_2 = P(x > P_{RW\min} + k_I) = 1 - \frac{1}{2} erfc\left(-\frac{1}{\sqrt{2}} \cdot \frac{P_{RW\min} + k_I - \left(\mu_{RWU} - \left(P_{TI} + k_W + \mu_G\right)\right)}{\sqrt{\sigma_{RWU}^2 + \sigma_G^2}} \right) \text{.....(22)}$$

The value of k_W depends upon whether the interference is co-channel or adjacent channel interference.

For co-channel interference

$$k_W = k_{CO} \text{.....(23)}$$

where k_{CO} is the co-channel interference margin in dB.

For adjacent-channel interference

$$k_W = 10\log\left\{\frac{1}{ACIR}\right\} = -ACIR_{(dB)} \text{.....(24)}$$

where $ACIR_{(dB)}$ is the adjacent channel interference ratio in dB (see Appendix B for the derivation of (24))

7.7 Expression for P_{IT} Given a Single White Space Interferer

Because it will be useful for comparison with Karimi's work, (22) will be expressed as

$$q_2 = 1 - \frac{1}{2} erfc\left(-\frac{Z}{\sqrt{2}} \right) \text{.....(25)}$$

where, after substituting for μ_{RI} using the relationship from (19), Z can be shown to be

$$Z = \frac{P_{RW\min} + k_I - \left(\mu_{RWU} - \left(P_{TI} + k_W + \mu_G\right)\right)}{\sqrt{\sigma_{RWU}^2 + \sigma_G^2}} \text{.....(26)}$$

After rearranging (25) it can be shown that Z can also be expressed as

$$Z = -\sqrt{2}erfc^{-1}\{2(1-q_2)\}\text{.....(27)}$$

Equating (26) and (27) and then rearranging for P_{TI}, it is easily shown that

$$P_{TI} = \mu_{RWU} - (\mu_G + P_{RW\min} + k_I + k_W) - \sqrt{2}erfc^{-1}\{2(1-q_2)\}\sqrt{\sigma_{RWU}^2 + \sigma_G^2} \text{.....(28)}$$

Unfortunately, (28) is a transcendental equation because $erfc^{-1}\{2(1-q_2)\}$ is a function of P_{TI}. However, if q_2 is defined to be

$$q_2 = q_1 - \Delta q \text{.....(29)}$$

where Δq is the reduction in DTT location probability caused by any interference terms.

Substituted (29) into (28) it will be found that (28) can be expressed as

$$P_{TI} = \mu_{RWU} - (\mu_G + P_{RW\min} + k_I + k_W) - \sqrt{2}erfc^{-1}\{2(1+\Delta q - q_1)\}\sqrt{\sigma_{RWU}^2 + \sigma_G^2} \text{.....(30)}$$

The advantage of using (30) instead of (28) is that q_1 is independent of P_{TI} and if Δq is specified then (30) is no longer a transcendental equation and, therefore, is easily solved provided q_1 is specified.

Again, because P_{RD} is dependent on subtracting random variables, it can be shown by repeating the above analysis using (21) instead of (22), that there is an alternative expression for (30) and that it is given by

$$P_{TI} = \mu_{RWU} - (\mu_G + P_{RW\min} + k_I + k_W) + \sqrt{2}erfc^{-1}\{2(1+\Delta q - q_1)\}\sqrt{\sigma_{RWU}^2 + \sigma_G^2} \text{.....(31)}$$

7.8 Comparison of derived equations with those from Karimi's Study

If the definition of the parameters used in this analysis are compared with those used by Karimi it will be found that

$$P_{RW\min} = P_{S\min(dBm)}$$
$$P_{RWU} - P_{RW\min} = Z_{(dBm)}$$
$$P_{TI} = P_{IB(dBm)}^{WSD}$$
$$P_{ACLR} = P_{OOB(dBm)}^{WSD}$$
$$\mu_{RW} = m_{S(dBm)}$$
$$\mu_G = m_{G(dBm)}$$
$$\sigma_{RW}^2 = \sigma_S^2$$
$$\sigma_{RU}^2 = \sigma_U^2$$
$$\sigma_{RWU}^2 = \sigma_Z^2$$
$$\sigma_{RI}^2 = \sigma_G^2$$
$$k_I = IM_{(dB)}$$
$$k_W = r(\Delta f_{dB})$$
$$k_{CO} = r(0)$$
$$P(x > P_{RW\min}) = q_1$$
$$P(x > P_{RW\min} + k_I) = q_2$$
$$\sqrt{2}erfc^{-1}\{2(1-q_2)\} = \mu(q_2)$$

and it will be assumed that the definitions of Karimi's remaining parameters are such that

$$\mu_{RU} + P_{RW\min} = m_{U(dBm)}$$
$$\mu_{RWU} - P_{RW\min} = m_{Z(dBm)}$$

Using the above relationships it is easily shown that in terms of Karimi's parameters (8) and (28) become

$$q_1 = 1 - \frac{1}{2}erfc\left(\frac{1}{\sqrt{2}} \cdot \frac{m_{S(dBm)} - m_{U(dBm)}}{\sqrt{\sigma_S^2 + \sigma_U^2}}\right) \text{.....(32)}$$

and

$$P_{IB(dBm)}^{WSD} = m_{Z(dBm)} - \left(m_{G(dBm)} + r(\Delta f_{dB}) + IM_{(dB)}\right) - \mu(q_2)\sqrt{\sigma_Z^2 + \sigma_G^2} \text{ .....(33)}$$

If (32) and (33) are compared with equations (2) and (5) in Karimi's paper it will be found that they are identical.

7.9 Appendix : Background Statistical Information

a) Normally distributed random variable

The probability function for a normally distributed random variable is

$$f(x) = \frac{1}{\sqrt{2\pi\sigma_X^2}} \exp\left\{-\frac{1}{2}\left(\frac{x-\mu_X}{\sigma_X}\right)^2\right\} \qquad \text{.....(A1)}$$

where μ_X is the mean value and σ_X is the standard deviation.

By definition

$$\frac{1}{\sqrt{2\pi\sigma_X^2}} \int_{-\infty}^{\infty} \exp\left\{-\frac{1}{2}\left(\frac{x-\mu_X}{\sigma_X}\right)^2\right\} dx = 1 \qquad \text{.....(A2)}$$

and

$$P(x < X) + P(x > X) = 1 \qquad \text{.....(A3)}$$

where the first term is the probability that x is less than value X and the second is the probability that x is greater than value X.

Therefore from (A2) and (A3) it follows that

$$P(x > X) = \int_X^{\infty} f(x)dx = \frac{1}{\sqrt{2\pi\sigma_X^2}} \int_X^{\infty} \exp\left\{-\frac{1}{2}\left(\frac{x-\mu_X}{\sigma_X}\right)^2\right\} dx \qquad \text{.....(A4)}$$

and

$$P(x < X) = \frac{1}{\sqrt{2\pi\sigma_X^2}} \int_{-\infty}^{X} \exp\left\{-\frac{1}{2}\left(\frac{x-\mu_X}{\sigma_X}\right)^2\right\} dx \qquad \text{.....(A5)}$$

Using the substitution

$$t = \frac{1}{\sqrt{2}} \cdot \frac{x - \mu_X}{\sigma_X} \qquad dx = \sigma\sqrt{2}dt \qquad \text{.....(A6)}$$

in (2) gives

$$P(x > X) = \frac{1}{\sqrt{\pi}} \int_T^{\infty} \exp\{-t^2\} dt \quad \text{.....(A7)}$$

where T, the value of t when x is set equal to X, is equal to

$$T = \frac{1}{\sqrt{2}} \cdot \frac{X - \mu_X}{\sigma_X} \qquad \text{.....(A8)}$$

Given the complementary error function, erfc(T), is defined as

$$erfc(T) = \frac{2}{\sqrt{\pi}} \int_T^{\infty} \exp\{-t^2\} dt \qquad \text{.....(A9)}$$

it follows from (A8) that

$$P(x > X) = \frac{1}{2} erfc\left(\frac{1}{\sqrt{2}} \cdot \frac{x - \mu_X}{\sigma_X} \right) \qquad \text{.....(A10)}$$

and from (A4) that

$$P(x < X) = 1 - \frac{1}{2} erfc\left(\frac{1}{\sqrt{2}} \cdot \frac{x - \mu_X}{\sigma_X} \right) \text{.....(A11)}$$

b) Log-Normally distributed random variable

If random variable X is in the dB domain and normally distributed, its probability density is as given by (A4) provided that μ_X and σ_X are in dB. To transform (A4) so that the variable is in the linear rather than dB domain, the following relationships are needed

$$x = 10\log(y) = 10\ln(y)\log(e) \quad \mu_x = \mu_{dB} \quad \sigma_x = \sigma_{dB} \text{.....(A12)}$$

$$dx = \frac{10\log(e)}{y} dy \text{.....(A13)}$$

Using these relationships it can be shown that (A4) can be expressed as

$$P(x > X) = P(y > Y) = \frac{10\log(e)}{y\sqrt{2\pi\sigma_{dB}^2}} \int_Y^\infty \exp\left\{-\frac{1}{2}\left(\frac{10\log(e)\ln(y) - \mu_{dB}}{\sigma_{dB}}\right)^2\right\} dy \quad \text{.....(A14)}$$

which can then be re-arranged to give

$$P(x > X) = P(y > Y) = \frac{1}{y\dfrac{\sigma_{dB}}{10\log(e)}\sqrt{2\pi}} \int_Y^\infty \exp\left\{-\frac{1}{2}\left(\frac{\ln(y) - \dfrac{\mu_{dB}}{10\log(e)}}{\dfrac{\sigma_{dB}}{10\log(e)}}\right)^2\right\} dy \quad \text{.....(A15)}$$

Knowing that μ_e and σ_e, the natural logarithm values of μ_x and σ_x in (A4), have the following relationships with the dB values

$$\mu_e = \frac{\mu_{dB}}{10\log(e)} \qquad \sigma_e = \frac{\sigma_{dB}}{10\log(e)} \quad \text{.....(A16)}$$

then (A15) can be expressed as

$$P(x > X) = P(y > Y) = \frac{1}{y\sigma_e\sqrt{2\pi}} \int_Y^\infty \exp\left\{-\frac{1}{2}\left(\frac{\ln(y) - \mu_e}{\sigma_e}\right)^2\right\} dy \quad \text{.....(A17)}$$

This is the probability density function for a random variable that has a log-normal distribution in the linear domain and a normal one in the logarithm domain for the specific case of using natural logarithms. Therefore, it follows that Y is a log-normal random variable in the linear domain and that if $-\infty \le X \le \infty$ then $0 \le Y \le \infty$.

7.9.1 Log-normal mean and variance

The mean and variance for a log-normal distribution that uses natural logarithms in the logarithm domain are given by

$$mean = e^{\mu_e + \frac{\sigma_e^2}{2}} \quad \text{.....(A18)}$$

$$\text{var}\,iance = \left(e^{\sigma_e^2} - 1\right) \cdot e^{\left\{2\mu_e + \sigma_e^2\right\}} \quad \text{.....(A19)}$$

So,

$$mean_e = \ln(mean) = \mu_e + \frac{\sigma_e^2}{2} \text{ .....(A20)}$$

$$\text{var}\,iance_e = \ln(\text{var}\,iance) = \ln\left(e^{\sigma_e^2} - 1\right) + 2\mu_e + \sigma_e^2 \text{ .....(A21)}$$

Using the relationship between logs that have different bases in conjunction with (A16), (A20) and (A21), it can be shown that the mean and variance in the dB domain are given by

$$mean_{dB} = 10\log(mean) = \mu_{dB} + \frac{\sigma_{dB}^2}{20\log(e)} \text{ .....(A22)}$$

$$\text{var}\,iance_{dB} = 10\log(\text{var}\,iance) = 10\log\left(e^{\left\{\frac{\sigma_{dB}}{10\log(e)}\right\}^2} - 1\right) + 2\mu_{dB} + \frac{\sigma_{dB}^2}{10\log(e)} \text{ .....(A23)}$$

7.9.2 Addition / subtraction of normal random variables and constants

Linear Domain

The result of adding / subtracting a number of normal random variables and / or constants produces a new normal random variable with mean (μ) and variance (σ^2) values given by

$$\mu = \sum_{\mu=1}^{N_\mu} \mu_n + \sum_{j=1}^{N_k} k_j \text{ .....(A24)}$$

$$\sigma^2 = \sum_{n=1}^{N_\mu} \sigma_n^2 \text{ .....(A25)}$$

where μ_n and σ^2_n represent the means and variances, respectively, of N_μ random variables and k_j represents the N_k constants. The algebraic sum should also take account of the fact that some of the means and constants could have negative values.

Log Domain

The addition of N independent, log-normally distributed random variables (Y_T) in the linear domain can be expressed as

$$Y_T = \sum_1^N Y_n = \sum_1^N 10^{\frac{X_n}{10}} \text{ …..(A26)}$$

Given it is also generally accepted that the outcome of adding a number of log-normal random variables can be approximated by a log-normal distribution, it follows that this distribution can be expressed as

$$Y_T = \sum_1^N 10^{\frac{X_n}{10}} = 10^{\frac{Z}{10}} \text{ …..(A27)}$$

Relation of X and Z derived using Wilkinson, Schwartz and Yeh paper or Monte Carlo numerical simulation (Statistics of the sum of lognormal variables in Wireless Communication P. Cardieri and T. Rappaport)

So in the dB domain

$$Z = 10\log(Y_T) \text{ …..(A28)}$$

Therefore, in the dB domain Z is a normally distributed random variable and its probability density is as given by (A4) and its mean and variance values, represented by μ_Z and σ^2_Z respectively, usually have to be derived using numerical analysis techniques. However, it may be possible to derive all of the mean and variance values for all pixel and interference source location combinations etc.

7.10 Appendix B: Adjacent Channel Interference Ratio

The fraction of the white space interference power that falls within the DTT receiver's bandwidth is determined by the value of transmitter's adjacent channel leakage ratio (ACLR) and the value of the DTT receiver's adjacent channel selectivity (ACS). The interference power at the output of the DTT receiver's filter due to these two effects are conventionally expressed as

$$P'_{ACLR} = \frac{G' P'_{TI}}{ACLR} \text{ …..(B1)}$$

$$P'_{ACS} = \frac{G' P'_{TI}}{ACS} \text{ …..(B2)}$$

where ACLR and ACS are the values for the transmitter's adjacent channel leakage ratio and the receiver's adjacent channel selectivity, respectively.

Consequently, in the dB domain, they are given by

$$P_{ACLR} = \log\left(P'_{ACLR}\right) = \log\left\{\frac{G' P'_{TI}}{ACLR}\right\} = G + P_{TI} - ACLR_{(dB)} \text{.....(B3)}$$

$$P_{ACS} = \log\left(P'_{ACS}\right) = \log\left\{\frac{G' P'_{TI}}{ACS}\right\} = G + P_{TI} - ACS_{(dB)} \text{.....(B4)}$$

The total adjacent channel interference power at the output of the DTT receiver's filter is derived by adding (B1) and (B2) which gives

$$P'_{RI} = P'_{ACLI} + P'_{ACS} = \frac{G' P'_{TI}}{ACLR} + \frac{G' P'_{TI}}{ACS} = G' P'_{TI}\left\{\frac{1}{ACLR} + \frac{1}{ACS}\right\} = \frac{G' P'_{TI}}{ACIR} \text{.....(B5)}$$

where ACIR is conventionally defined as the adjacent channel interference ratio

Comparing (B5) and (17) it will be seen that

$$k'_W = \frac{1}{ACIR} \text{.....(B6)}$$

So it follows from (18) that

$$k_W = \log\left(k'_W\right) = \log\left\{\frac{1}{ACIR}\right\} = -ACIR_{(dB)} \text{.....(B7)}$$

7.11 References

[Mit95] J. Mitola, "The software Radio Architecture", IEEE Communications Magazine, May 95, pp.26-38..