Quality Of Service and MObility driven cognitive radio Systems

White Paper

Cognitive Radio Resource Management

ABSTRACT

This white paper presents an overview of cognitive radio resource management studied in the European Union (EU) FP7 Integrated Project (IP) called QoSMOS.
The work reported includes the design of a Cognitive Manager for Resource Management (CM-RM) to manage an opportunistic use of the spectrum whitespaces, tools for design and performance evaluation for cognitive radio networks (CRNs), and resource management solutions for CRNs in all the three main target scenarios of QoSMOS, i.e., cognitive femtocells, cellular extension in the TV white spaces, and cognitive ad hoc networks.

INTRODUCTION

The deployment of cognitive radio technology raises new challenges to manage the radio resources while the protection of the incumbents must be addressed as a matter of priority. Incumbent users should not be faced with service degradation due to interference caused by the presence of cognitive radios, and this puts limitations on the provision of cognitive services. Available whitespaces may not necessarily offer the bandwidth needed to provide a given service for the cognitive users and the protection of incumbent users from interference restricts the service level offered so that the required QoS has to be optimized.

The design of the QoSMOS system and of its functional blocks depends on the requirements and constraints set by both the applicable regulations and the exploitability conditions. One side of those requirements comes from the flexibility imposed by the project on its system architecture, which must be able to cope with the target scenarios identified within the project and should also be able to cover the possible needs. Another set of constraints comes from the system requirements that have been identified.

Indeed, the QoSMOS project identified, after a rationalisation process, six scenarios [D1.2] [MacEtal2011]. These scenarios have undergone an additional analysis as potential business cases [LehEtal2012] and resulted in the three key target scenarios summarised in Figure 1.

While fuller details are available from the above references, the scenarios are briefly outlined in the following.

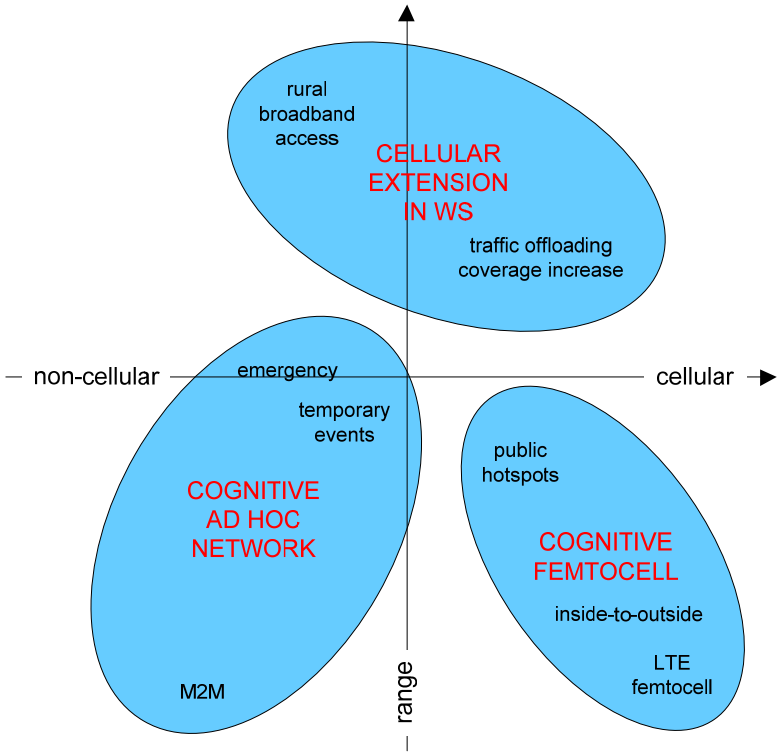

Figure 1: The final QoSMOS scenarios

Cellular extension in the whitespace

The cellular extension in whitespace scenario allows mobile telecommunication operators to improve coverage and/or capacity of their networks by using whitespace spectrum in addition to their own licensed spectrum. This scenario allows improving link quality and offering more flexible services, and therefore not only covers LTE-like business cases, but also rural broadband access.

Cognitive femtocells

The cognitive femtocell scenario makes use of small access points, for example to distribute broadband access in the home or its neighbourhoods, or to provide internet access in public areas, e.g., by so-called hot-spots. This scenario covers extensions of both concepts: femtocells in cellular networks and WLAN-type deployments. Example deployments include WLAN extension, indoor-to-outdoor coverage extension and public hot-spots.

Cognitive ad hoc networks

In the cognitive ad hoc networks scenario, whitespace is used to connect terminals as the operation of these networks is limited in both time and space. In order to comply with regulatory requirements, cognitive ad hoc networks are likely to require access to relevant repositories, whether directly or indirectly, with a static or a temporary connection. Without such a connection, the regulatory requirements may impose much stricter spectrum sensing capabilities. The cognitive ad hoc network scenario covers emergency operations, service during temporary events and machine-to-machine communication (M2M).

Constraints in terms of system requirements are given in the following.

First, the QoSMOS system shall be capable of adaptation in order to comply with regulations. To be able to do that, the QoSMOS system shall be able to collect *environmental information* depending on the QoS requirements and shall enable access to regulation information and policies. In particular, it shall allow collecting information from a *geolocation database* according to the requirements and shall allow updating it as required. In addition, it should support *spectrum sensing* for incumbent detection. Anyway, when spectrum sensing is needed, the system shall be capable of scheduling quiet periods for spectrum sensing purpose without QoS degradations for the opportunistic system below acceptable levels.
Then, the QoSMOS system shall be able to *react to the changes* in the environment. In particular, it shall avoid interference to incumbent communications. This may imply *vacating* the operating channel upon appearance of an incumbent user; alternatively, when this is authorised by regulations and policies, the system shall define a limitation on the *transmit power* in order to avoid interfering with simultaneous incumbent transmissions. In addition, it also shall coexist with other opportunistic systems. Moreover, it shall be able to detect *attacks of malicious users* and be robust to those misbehaviours.
As an implication to its design, the QoSMOS system shall be *flexible* enough to comprise different architectures which can support a variety of diverse use cases. In particular, it shall support multiple radio access technologies and be able to select the most appropriate. Moreover, it shall support different frequency bands for opportunistic use.
The performance of the QoSMOS system should be good enough to meet *expectations of the users* about the delivered service, even in presence of variations in the available spectrum resources. As a consequence, the system should maintain the agreed level of QoS and should be able to re-establish a disrupted service within an agreed time. This implies that an appropriate number of *reserve channels* shall be maintained based on the QoS needs. In any case, it shall provide data rates and latencies needed to satisfy QoS needs of the supported services in order to provide quality of experience (QoE) comparable to the one offered by other access technologies.
The QoSMOS system also shall support mobile users. However, the level of *mobility* varies among the target scenarios. The coverage increase and traffic offloading cases for the cellular extension possess high levels of mobility, together with the cognitive ad hoc network, whereas the rural broadband access case has virtually no mobility at all. The mobility for the femtocell cases somehow fall in the middle.

QoSMOS FUNCTIONAL ARCHITECTURE

In order to respond to the requirements and constraints outlined above, the QoSMOS system architecture (Figure 2), as documented and specified in [D1.2] [D2.1] [D2.2] [D2.3] and also presented in [CelEtal2011] [MacEtal2011] [LevEtal2012], defines a two-fold cognitive manager at its core: the cognitive manager for resource management (CM-RM), developed in WP5, and the cognitive manager for spectrum management (CM-SM), developed in WP6. In addition to those, a spectrum sensing (SS) block developed in WP3, a flexible transceiver (TRX) developed in WP4, and an adaptation layer (AL), developed as a cross-WP activity.

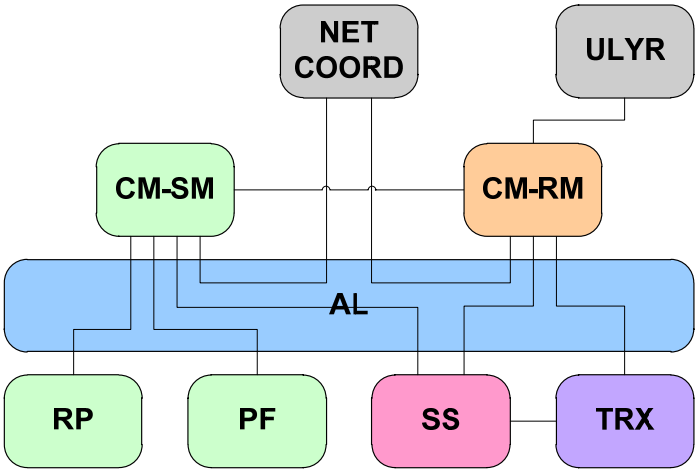

Figure 2: The QoSMOS reference model

The spectrum resources are opportunistically used by the TRX and exploited for serving the needs of the upper layers (ULYR), with the SS providing radio context information. The AL facilitates communication among all the remote entities, but it is not involved in the interaction between the CM-RM and the CM-SM.

Related to the activities of CM-RM and CM-SM is the external block providing network coordination (NET COORD). This block is optional and for the example case of the cellular scenario, it is part of the core network (CN).

At the user equipment, or in case of missing core network at any network device, the ULYR is for example the application, whereas in case of presence of a core network, the ULYR is at the transport layer. The split of SS functionalities depends on the spectrum sensing topologies [D3.4] and is out of scope here. The split of CM-RM functionalities is addressed later in this section.

The CM-SM is responsible for the management of the frequency spectrum allocated to the QoSMOS entities for dedicated use. To this end, the CM-SM first acquires the relevant context information, including environment information obtained from spectrum sensing results provided by the spectrum sensing block and performance reports of current spectrum usage provided by the CM-RM, which may include filtered status information such as average supported load levels or average interference levels experienced in the system. Based on this information and on external constraints such as regulatory policies, operator policies and operator frequency planning, the CM-SM then builds up the spectrum portfolio containing spectrum usage information and spectrum usage policies and putting constraints on the decisions that can be taken by other entities of the QoSMOS system. To this end, the CM-SM accesses the regulatory repository (RP), which includes constraints and requirements about the spectrum use, and the common portfolio repository (PF)used to store and exchange context information.

The CM-RM is the main user of the spectrum portfolios generated by the CM-SM and allocates radio resources from the assigned spectrum portfolio to the end-users in order to provide service to the application layer according to an agreed level of QoS. The CM-RM is also responsible for the management of the user mobility as well as the implementation of functionalities needed to protect the incumbent users, relying in a close cooperation with the CM-SM, which in turn implements incumbent protection on a spectrum management level.

In brief, the CM-RM provides the CM-SM with updated network status information and spectrum usage reports, and this information is exploited by the CM-SM in order to decide which parts of the spectrum can be used by the QoSMOS entities and under which conditions/constraints, based on the information collected from the CM-RM and other QoSMOS entities. The CM-SM thus relies upon context information provided by the CM-RM and responds to requests of the CM-RM to adjust portfolio allocations in accordance with the current radio resource management needs.

CM-RM functional architecture

The functionalities required by the CM-RM [LevEtal2012] are divided among the CM-RM-internal functional blocks, see Figure 3, and are described in the following.

Functional blocks

The QoS maintenance and mobility management functions of the CM-RM are assigned to the access control (AC) and mobility control (MC) blocks. The resource allocation (RA) block is in charge of the allocation of the resources, which are then made available to the resource exploitation (RE) block that offers the communication services to the upper layers, optimising the use of the lower layers. In this, for topological reasons explained shortly below, the resource control support (RS) block acts as an intermediate block. Similarly, gathering of cognitive information to be used for system reconfiguration is split between two blocks: the networking domain cognition (NC) and the terminating domain cognition (TC) blocks, which manage performance measurements, sensing results and inputs from repositories.

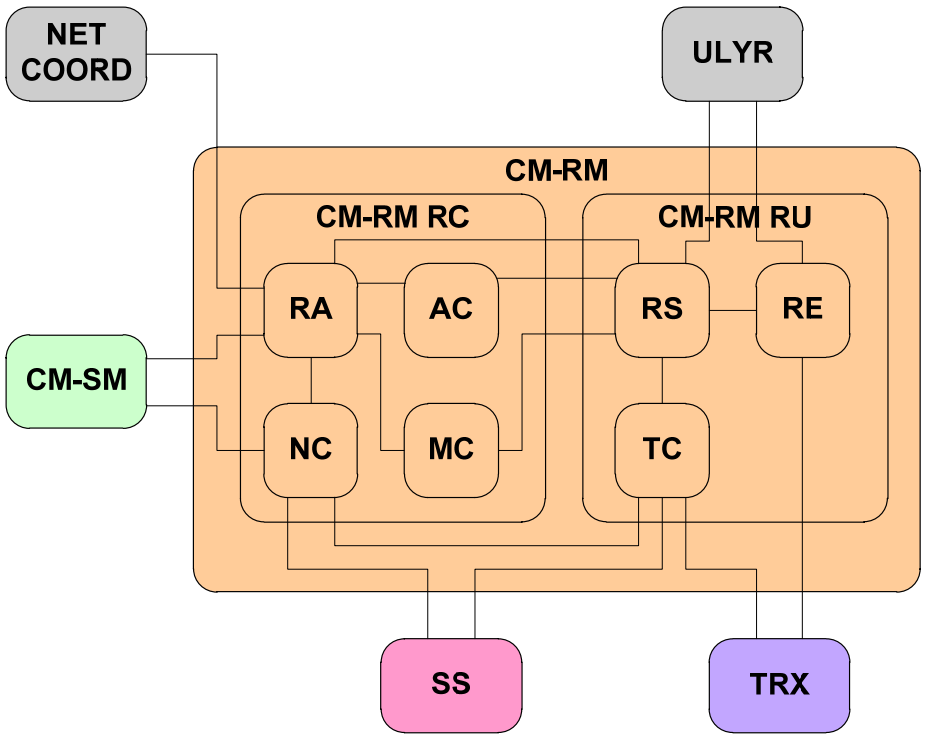

Figure 3: The functional architecture of the CM-RM

Topology mapping

The CM-RM is designed to be applicable to a range of diverse scenarios The various architectural options corresponding to spectrum sensing and resource control topologies are discussed in [D2.2] [D2.3]. In particular, from the resource control perspective, a QoSMOS system, and therefore the CM-RM, supports a centralised or a distributed resource control and may exploit the aid of a core network or not. To this end, the functional blocks of the CM-RM are further grouped. A first grouping of the functions into a resource control (RC) and a resource use (RU) group and making use of the four topological domains introduced by [CelEtal2011] is explained below.

The *terminating domain* pertains to the wireless border of the system, thus including those parts of the UEs as well as of the network nodes they are attached to, for example a base station, an access point or any other central controller. The *networking domain* covers the functions related to

the control of interconnected network devices, and hence included in a central controller as the above or alternatively in all nodes of a network with distributed control. The coordination domain is dedicated to the coordination with neighbouring and related networks, while the coexistence domain concerns larger-scale coexistence.
The resource control group includes the functions belonging to the networking domain. The RC is therefore present in a base station, an access point, or a cluster head in the case of centralised resource control, while it is found in any peer node of a network with distributed resource control. The resource use is by its nature always found in any QoSMOS wireless node. Both RC and RU groups are shown in Figure 3.

TOOLS FOR DESIGN AND PERFORMANCE EVALUATION

System design and its performance assessment rely on suitable tools. A set of such tools covering the protocol modelling, design, analysis and evaluation is presented in this section.

ADAPTATION LAYER FOR COMPONENTS' COMMUNICATION

The adaptation layer (AL) has a remarkable role in the QoSMOS architecture; its functionalities allow enhancing overall system performance as it is monitoring the status of each entity connected to it, thus triggering the needed alarms in case of misbehaviour of any piece of the system.
The AL comprises a set of components responsible for carrying out the different functions of the entity. [D2.3] presents the different activities carried out by the AL and also a detailed description of all its components. Figure 4 depicts the internal AL architecture. Next, a brief description of its components presented:

- AL_CORE: it is the module in charge of performing the most critical activities in the AL. It also has a database, called contactable entities DB, where all the information about registered QoSMOS entities is stored.
- AL_END: the interfaces between the AL_CORE and the QoSMOS entity they are connected to.

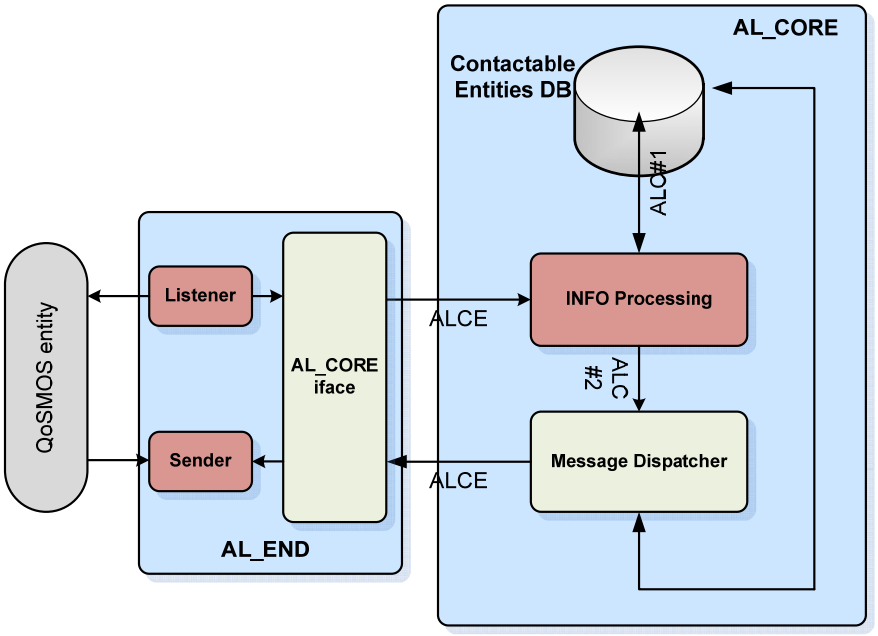

Figure 4: Internal AL architecture

The AL presents an architecture which allows many different communication paradigms and technologies. Considering the interactions with other blocks in the QoSMOS system, two of these technologies have been chosen due to the fact that they are the most widely used, namely XML-RPC and CORBA.

XML-RPC is a remote procedure call that uses HTTP as the transport protocol and XML to encode its calls. It allows transmitting, processing and returning complex data structures, but it has been designed to be as simple as possible. XML-RPC owns a specification [XML99] and a set of implementations that enable software to run in different operating systems and environments to make procedure calls over the Internet.

CORBA is a middleware solution that enables the exchange of information, independent of hardware platforms, programming languages and operating systems [COR11].

PHYSICAL LAYER ABSTRACTION FOR FAST SYSTEM-LEVEL PERFORMANCE PREDICTION

The main purpose of physical layer abstraction is to predict the link performance of the communication system based on a small number of measurable metrics. It can be applied for simplified system performance evaluation and also for dynamic adaptation of the parameters in order to match the predefined performance limits. In this way, a fast system level evaluation can be performed without the need for exhaustive search or detailed, extremely time consuming link-level simulations within the system-level simulator.). In our case, the system level performance will be investigated based on the block error rate (BLER).
The following abstraction methods described in [KliEtal2009] for OFDM based systems have been investigated:

- exponential effective SINR mapping (EESM);
- mutual information based effective SINR mapping – received bit mutual information (RBIR);
- mutual information based effective SINR mapping – mean mutual information per bit (MMIB).

The EESM technique is the simplest one as it only requires the knowledge of a per-subcarrier SNR for performance prediction. On the other hand, the RBIR and MMIB techniques require soft information which makes the computation and algorithm complexity higher.
Recent results of WP4 [DatEtal2011] show that in case of filter bank multicarrier modulation (FBMC) the inter-symbol interference and inter-carrier interference caused by the multipath channel can strongly degrade the performance of the system and soft decision calculations of the received bits can be rather complicated. As a result the simplest technique, which is suitable for FBMC, the EESM was selected for further investigations. In the case of the EESM the per-subcarrier SNR values are mapped using an exponential function and a weighting constant β as:

$$SINR_{eff} = -\beta \ln\left(\frac{1}{N}\sum_{n=1}^{N} e^{\left(-\frac{SINR_n}{\beta}\right)}\right) \qquad (0\text{-}1)$$

The goal is to determine the optimal β, which is a non-linear curve-fitting problem.

The basic steps of the parameter calculation and optimisation can be seen in Figure 5 below. First, based on the channel profile, a random channel realisation is generated. Subsequently, Monte Carlo simulations are performed for the given set of modulation/coding parameters in order to determine the BLER versus SNR values. Then, based on the SNR of each subcarrier and the simulated BLER curves, a curve fitting is performed in order to find the optimal β parameter to fit the curves to the AWGN curves.

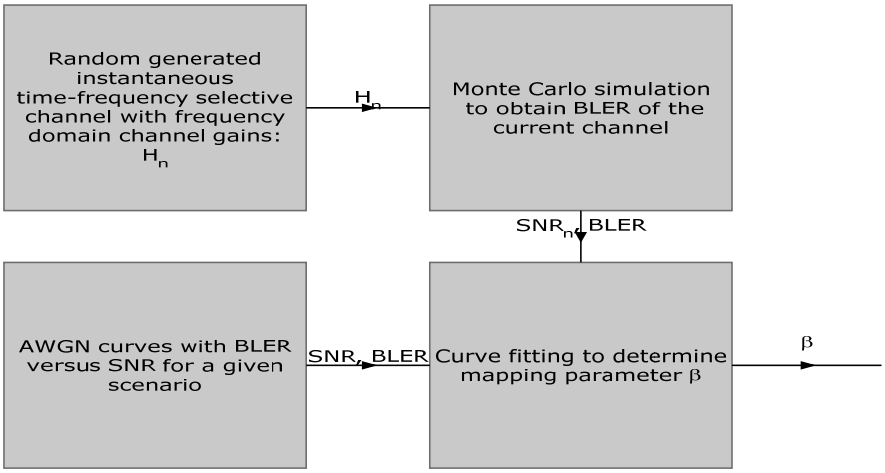

Figure 5: Parameter optimisation for PHY abstraction

IMPACT OF SENSING ACCURACY ON QOS

One of the common problems associated with opportunistic radio access based on spectrum sensing is the spectrum sensing accuracy. Collision will occur if an existing opportunistic user could not detect the arrival of an incumbent user or a newly arriving opportunistic user could not detect the presence of the incumbent user on a channel. Different types of spectrum sensing mechanisms have been proposed for detecting the presence and absence of incumbent users. The most widely used sensing mechanism is the energy detector.

In energy detection, the detector measures the energy of the received signal during some time period and in some frequency channel. The measured value of energy is compared with a threshold. If the threshold is exceeded, the detector decides that a signal was present. The probability of correctly detecting the signal is called the probability of detection P_D. If just noise or other interfering signals cause the threshold to be exceeded, this is called a false alarm. False alarms are generated by internal receiver noise and/or external interference. The false alarm probability P_{FA} refers to the probability that a free channel is classified as being occupied. If the threshold is not exceeded when the incumbent user is really present, this is called a missed detection P_M (i.e. the probability that an occupied channel is classified as vacant). Another factor influencing the performance of cognitive radios is spectrum handoff capability that enables opportunistic users who have to vacate their current channel due to the arrival of incumbent users in order to perform spectrum handoff to other unoccupied channels.

Network model

A continuous-time Markov chain (CTMC) model is used to analyse the performance of a cognitive radio network. The model supports multi-channel multi-user cognitive radio network with imperfect sensing. We consider a cognitive radio network as illustrated in Figure 6 with N . The network provides wireless access over a geographical area. These channels can be shared between incumbent and opportunistic users in an opportunistic manner with incumbent users having priority over opportunistic ones. Opportunistic users are allowed to access the channels that are not occupied by incumbent users. We assume that incumbent and opportunistic users have distinct arrival rates ($\square_1$, $\square_2$) and distinct service rates (μ_1, μ_2). The arrival and service rates are modelled by a Poisson process. New incumbent user call requests will be blocked if all channels are occupied by incumbent users while new opportunistic user call requests will be blocked if all channels are occupied by incumbent and/or opportunistic users

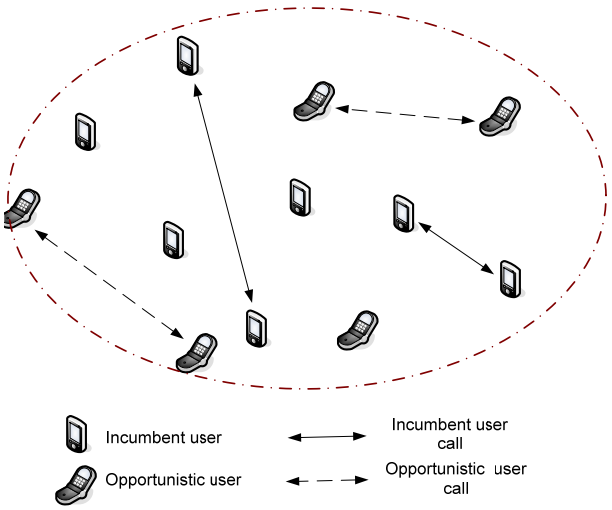

Figure 6: Cognitive radio network

A two-dimensional Markov chain is used to model the cognitive radio network system. The system states are given by two-tuples (i,j) where i is number of channels used for incumbent users' calls and j is number of channels used for opportunistic users' calls. The total number of channel occupied by incumbent and opportunistic users cannot exceed N. Therefore, the following restrictions appear: $0 \le i \le N$, $0 \le j \le N$, $i+j \le N$. *Let* $Q_{(i,j)}$ denote the steady state probability that the system is in state (i,j), which can be interpreted as the proportion of time that the system spends in state (i,j).

During the channel searching process, the opportunistic user searches for a free channel by randomly selecting one channel to detect whether it is free or not using the specified false alarm and detection probabilities. If the selected channel is found to be occupied by an incumbent user, the opportunistic user performs detection on the remaining channels with random order until it finds a free channel or all channels are determined to be busy. The time it takes to find a free channel (i.e. channel acquisition time) is assumed to be negligible.

By using the Markov chain and state transitions, formulas for different performance metrics are derived. The following performance metrics are used to evaluate the performance of the cognitive radio network.

Incumbent user termination probability - The term incumbent termination probability is used to refer to the probability that an incumbent user call, which has not been blocked initially, is terminated due to collisions with opportunistic users because of misdetections. There are two cases in which the incumbent user calls can be terminated. First, when an opportunistic user arrives at a channel occupied by incumbent users and it could detect the presence of the incumbent user ending up colliding with the incumbent user. The second case for collision is when an incumbent user arrives at a channel occupied by an opportunistic user, the opportunistic user has to leave the channel and move to a new free channel. In this case, the opportunistic user ends up colliding with another incumbent user.

Opportunistic forced termination probability - The opportunistic forced termination probability is the probability of dropping an active opportunistic user call due to the arrival of an incumbent user to a channel occupied by an opportunistic user. When a new incumbent user call arrives at a channel occupied by opportunistic user, the opportunistic user leaves that channel and starts the channel searching process. If the opportunistic user could not find a free channel, its call will be terminated.

Opportunistic successful probability - The opportunistic successful probability denotes the probability that an opportunistic user call is normally terminated (successful call completion).

Opportunistic blocking probability - The opportunistic blocking probability is the probability that a newly arrived opportunistic user call cannot be accepted due to insufficient radio resources, collision with an already existing incumbent user, and inability of the opportunistic user to find free channels. Opportunistic user's calls can be blocked for several reasons depending on the state of the system: when all channels are occupied by incumbent users, state (*N*,0), or due to miss detection (in such case the incoming opportunistic user collides with an existing incumbent user and the call will be completely lost). In the case where all channels are occupied by opportunistic users, state (0,*N*), an incoming opportunistic user will immediately be denied service since it knows about existence of other opportunistic by the opportunistic user controller/access point. An opportunistic user call can also be blocked even though all channels are free, state (0,0), if the opportunistic user could not classify any one of them as being free due to a certain P_{FA}.

Results

Extensive simulations using an event-based approach and Poisson arrival processes are performed to validate the analytical model. Results from the analysis and from the simulation are compared and they match very well validating the analysis. Figure 7 illustrates the degradation of the opportunistic successful probability (i.e. the probability that an opportunistic call is started and terminated normally) due to the increase in the incumbent arrival rate λ_1. This indicates that at high incumbent arrival rate the channels are more often occupied by incumbent users reducing opportunities for opportunistic users to access the network. It is clear that the opportunistic successful probability degrades quickly for small number of channels (e.g. *N*=3). It can be seen that as expected the success probability goes down when λ_1 increases.

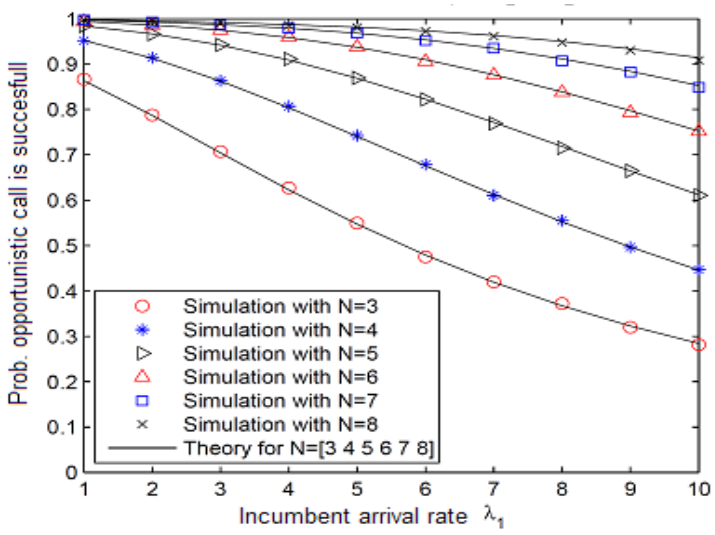

Figure 7: Opportunistic successful probability (normally terminated)

Figure 8 presents the opportunistic forced termination probability against the probability of detection for different number of channels. As the number of channels increases, the opportunistic forced termination declines. This is because more radio resources are available to handle incumbent calls. Hence the probability that new incumbent calls assigned to channels occupied by opportunistic users is reduced. On the other hand, those opportunistic users who force to handoff their call because they detected arrived incumbent users will more likely find new empty channels. However, as the probability of detection increases, incoming opportunistic detect the presence of incumbent users more accurately, and with P_D=1 opportunistic users will never access the network in the first place and therefore there would be no opportunistic users' force terminated calls.

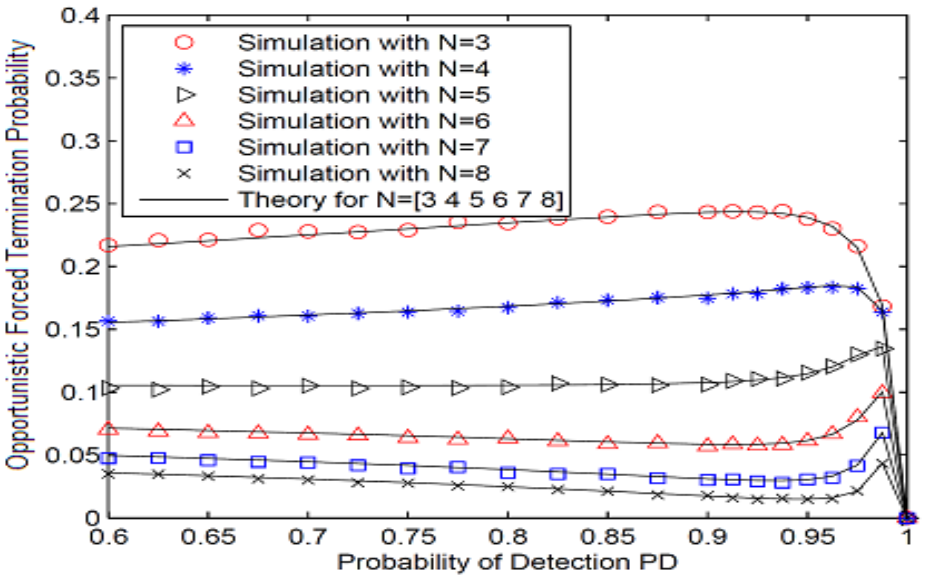

Figure 8: Opportunistic termination probability versus probability of detection

RESOURCE MANAGEMENT SOLUTIONS FOR THE TARGET SCENARIOS

This section presents resource management solutions for the three main target scenarios of QoSMOS: the cellular extension, the cognitive femtocell and the cognitive ad hoc network.

COGNITIVE ACCESS CONTROL FOR THE CELLULAR EXTENSION SCENARIO

Access control (AC) is a key element in the provision of QoS in conventional networks, as it aims at avoiding network congestion while preserving the committed QoS of already accepted calls. It can even restrict the number of ongoing connection in the system or degrade some user's QoS to satisfy a majority of ongoing user's requirements. However, the decision process is not simple as many factors, sometimes contradictory, have to be taken in consideration, and it becomes even more complex in a context of cognitive radio.

CR is the technical answer from the wireless community to solve the problems resulting from the spectrum underutilisation and the dearth of spectrum bands: an opportunistic system is authorised to transmit in the same frequencies than an incumbent system if minimal interferences are guaranteed. One possible orientation for AC may consist in developing schemes that defines the interference generated onto the incumbent system as the admission criterion. Another one could focus on schemes that are charged to maximise the number of admitted users, taking benefits from the presence of opportunistic resources. Because it addresses both QoS and mobility aspects, the second approach has been privileged in this study.

The literature provides then a plethora of solutions and [Hos05] brings an interesting illustration of the different schemes that could be implemented in a network.

Solution for optimising the access control in opportunistic cellular system

The proposed solution consists in enhancing the access control mechanism deployed in conventional network with cognitive abilities in order to control the impacts of the incumbent's apparition. Thus, the decision-making algorithm will take, in addition to the admission decisions, a set of evictions measures that will be motivated by its observation of the network environment and driven by policies adapted to the context. These measures can be classified, as following, depending on their impact on the QoS:

-(1) forcing the handover of UEs to neighbour cells;

-(2) forcing the handover of UEs to another band (licensed, for instance);

-(3) reconfiguring the base station to operate in a backup channel;

-(4) excluding pre-empted resources from resources allocation patterns;

-(5) reducing the QoS of the connected UEs by allocated less radio resources;

-(6) dropping UE connections.

The main objective of this solution is then to take jointly and in the most efficient way admission and evictions decisions. This process will be done in reactive mode, or in preventive mode depending on the availability of the incumbent detection information.
In the example illustrated in Figure 9, the estimation of the additional forced handovers triggered by the incumbent presence (done in BS#1) should benefit to the admission control (in BS#2) which may be able to adapt its guard band to minimise or cancel the degradation of the system QoS and guarantee mobility support.

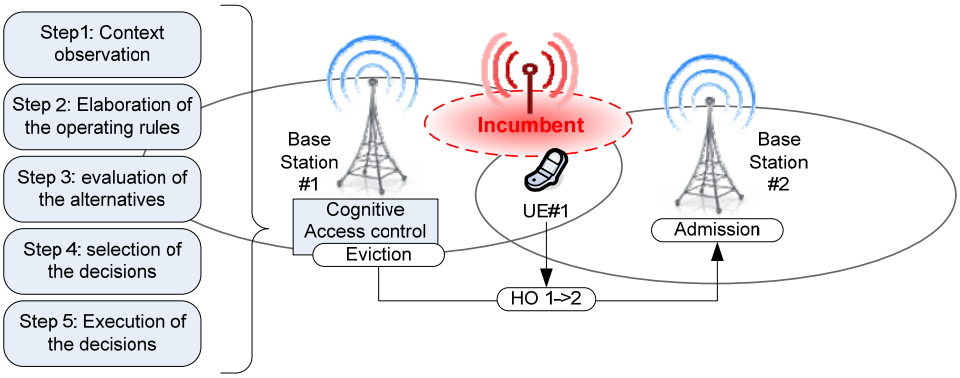

Figure 9: Illustration of the "cognitive access control" concept

To assess the solution, the two following network-relative performance metrics shall be considered.

-The connection blocking rate (CBR), which measures the rate of rejected service requests within the system. This metric considers the number of events that occurs in the whole system and is expressed in percentage:

$$CBR = 100 \times \frac{\sum_i NB\_COMM\_REJ}{\sum_i NB\_COMM\_REQ} \quad (0\text{-}2)$$

-The connection dropping rate (CDR) measures the rate of established communications that have been prematurely interrupted, whatever the cause:

$$CDR = 100 \times \frac{\sum_i NB\_COMM\_DROPPED}{\sum_i NB\_COMM\_ACCEPTED} \quad (0\text{-}3)$$

Algorithm description

The cognitive access control (CAC) algorithm firstly collects context information from a local source (e.g. spectrum measurements results provided by sensing sensors) and from a global database such as the common portfolio database. In parallel, the algorithm monitors the UE status as well as the base stations' metrics.

This information is then analysed and any incumbent apparition is logged in order to identify afterwards an eventual periodicity in the incumbent operations (through learning techniques). This input is used by the solution to orientate the action(s) to be taken: preventive action trigs the planning of eviction measures while reactive action forces the system to take decisions for responding immediately to the apparition of the incumbent.

The decision-making algorithm characterises the detected incumbent and lists the different possibilities it can apply to mitigate the impacts. These alternatives are evaluated based on their impacts on the QoS which are pondered depending on the observed context and potentially refined with learning techniques. This problem can be simplified as follows.

- A base station allocates a number of physical resources blocks w_j to a list of connected users u_i (with $i \in [1, \ldots, N]$).
- When an incumbent appears, it pre-empts a spectrum bandwidth W_G from the initial capacity of the cell/sector, managed by the base station, which corresponds to W_N physical resources blocks (W_G encompasses the guard bands, as required by the regulation).
- To compensate the impact of the incumbent presence, the base station has to take a series of eviction decisions D_k (with $k \in [1, \ldots, M]$) on the users u_i , each of them releasing w_j resources and generating a QoS preservation value $V(u,k)$.
- Decisions D_k are prioritised with a weight p_k according to the environment context, the operator policy and the appeared incumbent parameters. Moreover, a condition $c_k \in \{0, 1\}$ is applied to each decision D_k for each user u_i in order to characterise its validity.
- Then, the objective of the problem consists in choosing the set of users u_i that releases at least W_N physical resources blocks, such that the group of eviction decisions D_k applied to these users generates the maximum QoS preservation $Z(u,k)$.

Figure 10 illustrates the design of the solution, which can be divided in three steps: the elaboration of the operating rules, the execution of these rules to prioritise both UEs and eviction decisions and the selection of the decisions' set.

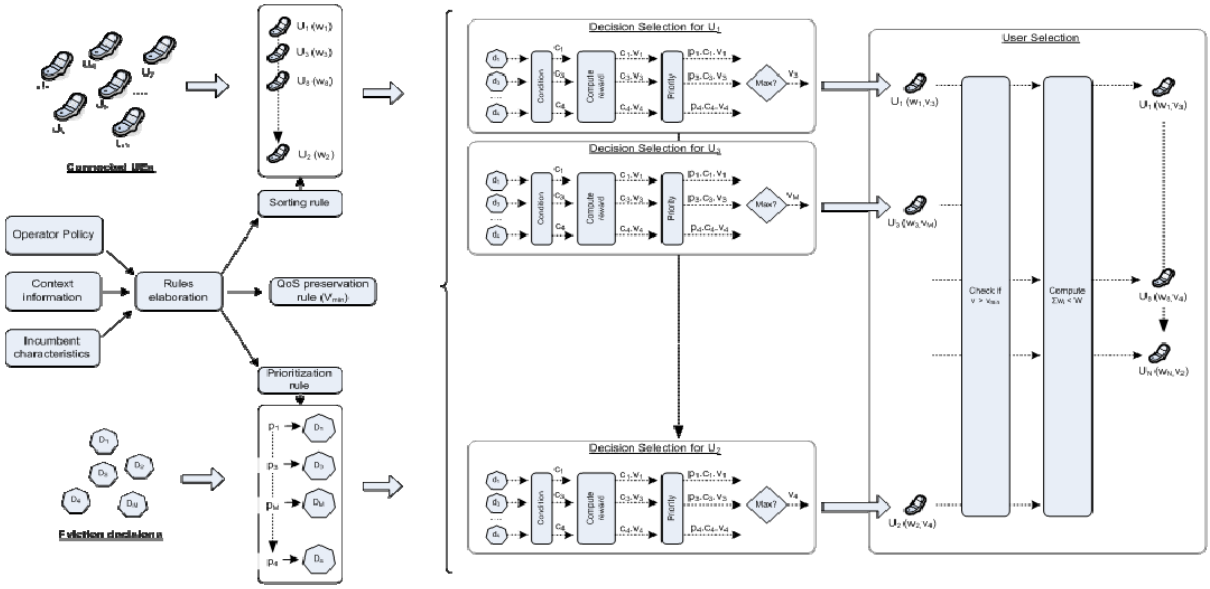

Figure 10: Overview of the access control algorithm

System model

The system model encompasses several base stations operating in an urban area and controlling for each of them three different sectors.
A set of user equipments is deployed uniformly in the simulated region, moving at 5 km/h according to a straightaway direction, randomly defined.
These user equipments connect to the base station which provides the best quality signal and initiate data communication requests according to a Poisson statistical distribution. These requests are then analysed by the admission control algorithm implemented in each sector of the base station which takes the decision to accept or reject the connection depending on the cell load and other cognitive information. These decisions are measured with two performance metrics previously introduced: the CBR and the CDR.
Three cases have been considered: in the first one, no incumbent is present and the system operates as any conventional LTE network. In the second use case, an incumbent appears and covers one sector of cell 5. In the third one, this incumbent impacts seven sectors as illustrated in Figure 11.

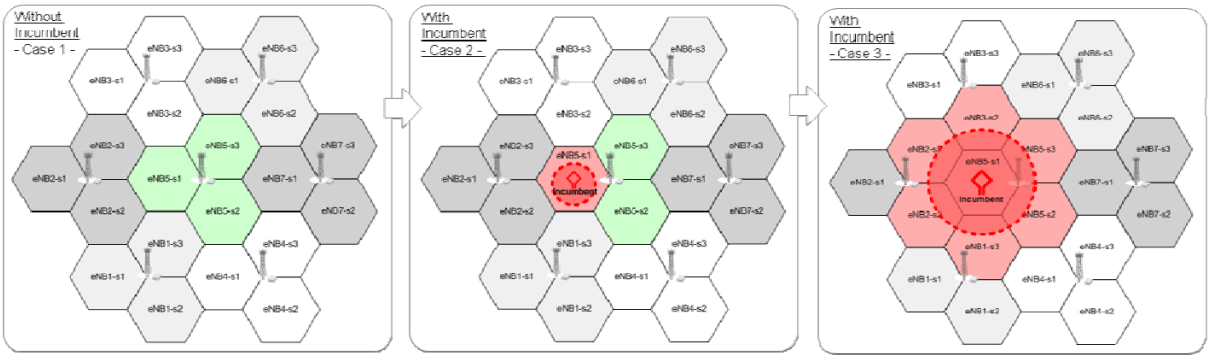

Figure 11: System model cases

Simulation results

The objective of this analysis is to characterise the impact of the incumbent apparition on the system performance and to quantify the benefits of the CAC algorithm. The two metrics CBR and CDR have been observed during the simulation time and the following figures illustrate the obtained results for the different cases.

-The CDR and CBR are expressed in percentage;

-The time is expressed in units of 10^5 ms;

-At T_{INC} = T0 + 9 minutes, the incumbent appears (its presence is highlighted by the usage of a grey background). It covers seven sectors (case 3) and has a bandwidth size of 3 MHz.

Figure 12 illustrates the case where no incumbent is present and corresponds more or less to the behaviour of a conventional network. This figure represents in consequence the reference to be used to assess the impacts of the incumbent, and also the objective to achieve by the cognitive AC algorithm.
The figure shows that the CDR is quite stable (with a mean value of 5%) while the CBR progresses according to the system load. This demonstrates the behaviour of the admission control which prioritises the handover requests at the expense of the new connection requests, and ensures a dynamic support of the physical mobility within the opportunistic system.

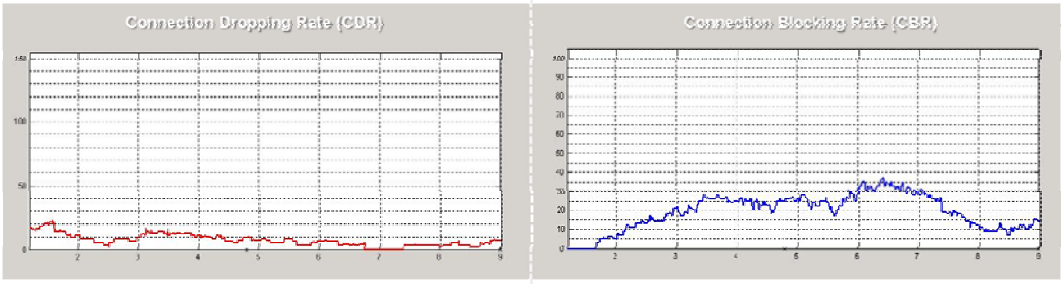

Figure 12: CDR/CBR vs time – No incumbent

The apparition of the incumbent is activated in Figure 13, and its impacts are perceptible on both graphs. For CDR, the system has to drop connections to release the radio resources pre-empted by the incumbent: this is materialised by the high peak present at T_{INC} (+ 55% in this context). In parallel, it shall also reject any new connection requests to avoid degrading the QoS even more. This is represented by an amplification of the CBR just after the incumbent apparition.
Moreover, the CDR peak shape seems to indicate that even if connections have been dropped, the system it is still over-loaded and has no other choice than rejecting handover requests (CDR continues augmenting after the incumbent apparition), which challenges the capacity of the network to support mobility in the impacted cells.

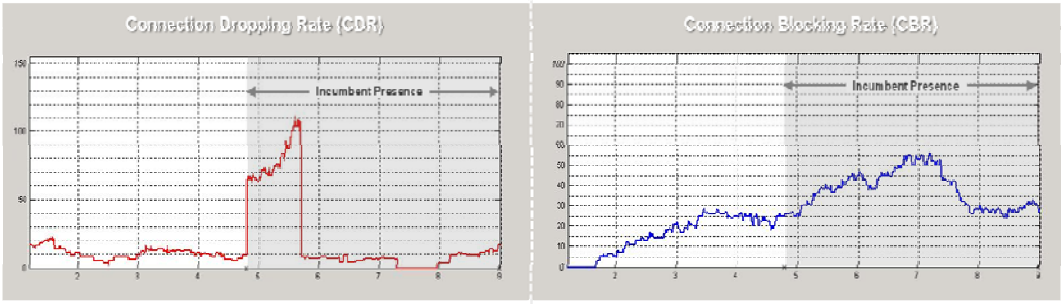

Figure 13: : CDR/CBR vs time – With incumbent

The cognitive AC algorithm is then activated in Figure 14 in order to mitigate the incumbent's impacts. In comparison to Figure 13, some improvements can be observed: the system has dropped fewer connections thanks to the eviction control algorithm which has taken "QoS-safe" decisions (for example, intra-cell handover). This has released additional radio resources that have been used by the system to improve the support of mobility in the impacted cells.
Furthermore, a CBR improvement is also noticeable: the decisions taken by the algorithm has facilitated a better distribution of the load among the sectors, which enables the acceptation of additional connections.

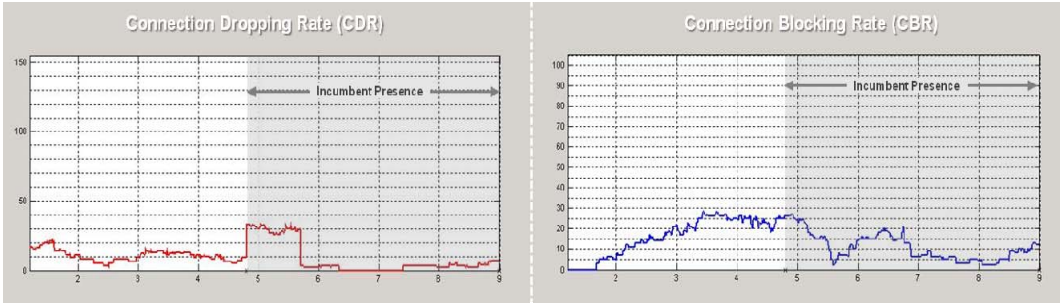

Figure 14: CDR/CBR vs time – Activation of the cognitive AC algorithm in reactive mode

Figure 15 represents the evolution of CDR/CBR when the cognitive AC algorithm is configured in preventive mode. This mode consists in predicting the presence of the incumbent for enabling the execution of preventive "QoS-safe" measures before the incumbent appears. In this simulation, the algorithm is aware of the predicting information six minutes before the incumbent apparition, which allows the system to plan five preventive operations triggered every minutes.
Figure 15 demonstrates that this mode cancels entirely the impacts of the incumbent apparition, contrary to the reactive mode. Nevertheless, a limited degradation of the CBR/CDR can be expected during the timing period when preventive measures are taken: this degradation is not perceptible for the configuration of this simulation, as the system has found enough candidate UEs to be moved to the neighbour cells.

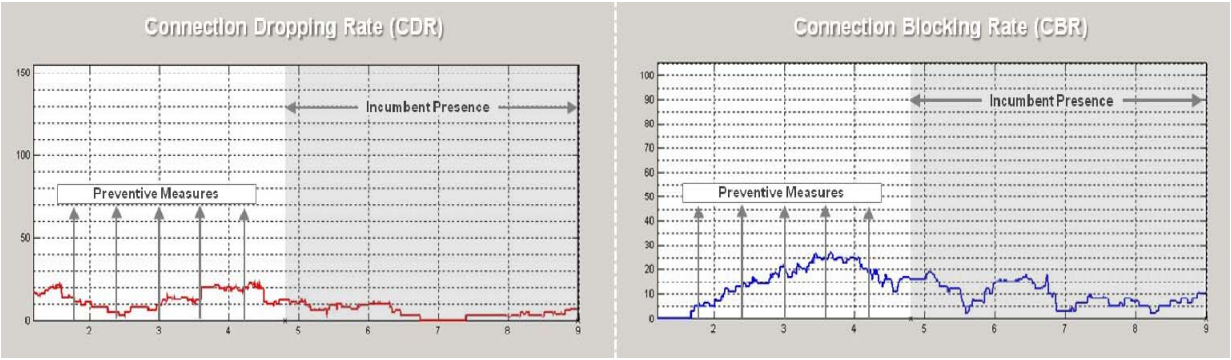

Figure 15: CDR/CBR vs time – Activation of the cognitive AC algorithm in preventive mode

This analysis has characterised the effects of the incumbent apparition on both the CDR and the CBR. But it has principally proved the capacity of the algorithm to cancel these impacts and to contribute to the preservation of the user mobility within the opportunistic system.

INTERFERENCE MANAGEMENT FOR FEMTOCELLS

Over the past decade, the demand for higher capacity and data rates has been on the increase. A number of technologies and standards have been developed to cope with this increasing demand i.e. high speed packet access (HSPA), LTE, LTE advanced and WiMAX. These technologies and others have been developed to provide speedy communications to end users. However, with the increasing demand for indoor cellular service, mobile operators simply cannot effectively provide good quality coverage to indoor users given the high in-building penetration loss. A survey [ABI2007] shows that in the near future more than 50% of voice and 70% of data traffic is expected to originate from indoor users. The need for providing good quality indoor voice and data services can therefore not be overemphasised.
With the growing demand of innovative 3G services, most industrial critics see significant potential for the use of technology, so called "femtocells" [Chan2008]. Femtocells, also known as home base station, are small, low power access points and visually look like an ordinary wireless router. These access points are installed by users indoor, which creates a small wireless coverage area and connect user equipment (UE) to the cellular core network through subscribers broadband internet access. The access points known as femtocell access point (FAP) work as BS, enabling high quality voice, data and multimedia services to be delivered to mobile devices in indoor settings without changing the underlining UE radio access font end configuration. Femtocells would require some portion of spectrum from the operators for its operation. This can be a separate portion of spectrum allocated by the operator or the same portion of spectrum as used by macro-cell. The case of same spectrum being used for femtocells (co-channel femtocell deployment) offers the best spectral efficiency, however, with serious interference concerns. This interference can be

between neighbouring femtocells (co-tier interference) as well as between femtocells and macrocell (cross layer interference). The main challenge faced by femtocells is interference management. The key techniques that can be used for avoiding and mitigating interference in femtocells are well presented [Chan2008] [Zah2012]. The work herein presented is a power control scheme for interference management in femtocell networks with a focus on reducing the cross tier interference caused by femtocells to macrocell users.

Femtocell system model and problem formulation

A co-existence scenario in which a number of femtocells coexist within a macrocell as shown in Figure 16 is investigated. The interference caused by the femtocell downlink to any nearby macrocell user is thus investigated. The system model of Figure 16 shows a random deployment of femtocells within a macrocell. The macrocell contains certain number of macrocell users called macrocell user equipments (MUE) communicating with their microcell base station (MBS) while every femtocell has only one femtocell (opportunistic) user equipment (FUE) communicating with its corresponding FAP. One FUE is considered for simplicity and it is assumed that each femtocell allocates all of its available resources to this one active FUE. On the other hand, the MBS allocates its resources to MUEs by dividing the resources equally among all active MUEs.

It is also assumed that there is a unidirectional common channel between macrocell base station and FAP. This channel is a broadcast channel and the FAP can use this channel only to receive any information from the macrocell base station. On the other hand, MBS-FAP control communication can be achieved through a femtocell gateway (FGW) located in MBS core network. Through this channel, the FAP is able to know the location of any MUEs around it and thus can find the distance to a specific MUE. Due to this information, the FAP is able to predict its interference impact on the MUE. The femtocell has geo location capabilities as well and hence they can also be aware of their own location within the macrocell.

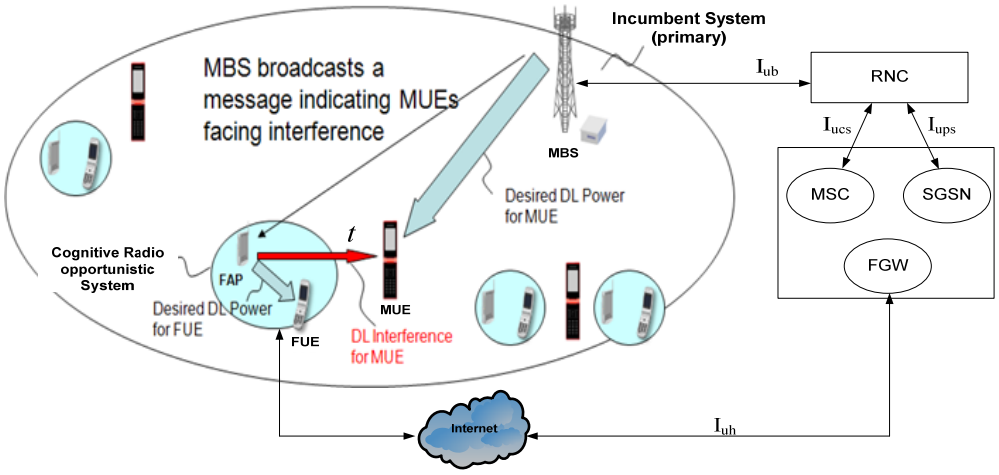

Figure 16: System model for femtocell network

Assumptions

The algorithm considers a number of assumptions and there it is necessary to summarise them separately. The main assumptions are given as follows.

- The cognitive femtocell is aware of its location and it is also also assumed that it has a geo location capability and can find its location.
- The femtocell is also aware of the location of the MUEs within its range. This information is given to the femtocell by the macrocell BS through the unidirectional broadcast channel.
- It is assumed that whenever a MUE faces interference from nearby femtocells, higher than a predefined threshold, it informs its base station about the higher interference.
- The model is based on path loss only.

Proposed downlink power control algorithm for femtocells

The main purpose of the downlink power control algorithm is to reduce the level of interference a femtocell causes to a nearby MUE in co-channel femtocell deployment and works as follows:
The MUEs in a macrocell containing femtocells would face interference from nearby femtocells. The impact of each femtocell on the MUE depends on the channel between MUE and FAP. When the MUE faces an interference level from the surrounding femtocells that is greater than a pre-defined threshold the MUE informs its base station about the increased level of interference. This predefined threshold is the level of interference that an MUE can handle. The MBS similarly receives one bit interference information from any active MUEs under interference. The one bit information only describes if the particular MUE is facing high interference or not. The one bit information is used to make sure there is no communication overhead.
The MSC for this process is shown in Figure 17. After receiving this information, the base station uses the unidirectional broadcast channel to inform the femtocells about the MUEs that are facing interference. The femtocell then, first checks if it is one of the "main aggressors" to any of the MUEs that are under interference. If the distance between the FAP and an MUE is less than or equal to the aggressor distance threshold t_{th} the particular FAP is then one of the main aggressors to that MUE. The aggressor distance specifies a circular region around the FAP with radius equal to t; any MUE within this area would be counted as a possible victim of interference from the femtocell. If an MUE resides within the aggressor distance, the FAP will then reduce its power; in the case where an MUE is at a distance greater than t, the FAP will ignore the message from MBS.
The concept behind the aggressor distance is simple and only those femtocells that are near to the MUE will decrease their power, as the nearby femtocells are the ones causing most of the interference to the MUE. This technique makes sure any unnecessary power reduction in faraway FAPs is avoided without degrading the quality of service to FUEs and also causing unnecessary FUE-FAP processing overhead. The aggressor distance t needs to be selected carefully as large values of t would cause unnecessary reduction in power (QoS) of femtocells that are faraway thereby increasing processing overhead while a smaller values will result in an underestimation of MUEs and cause high interference to MUEs thereby degrading overall performance. The value of t_{th} for the proposed algorithm has been selected based on best performance via simulation and is explained in the sequel.

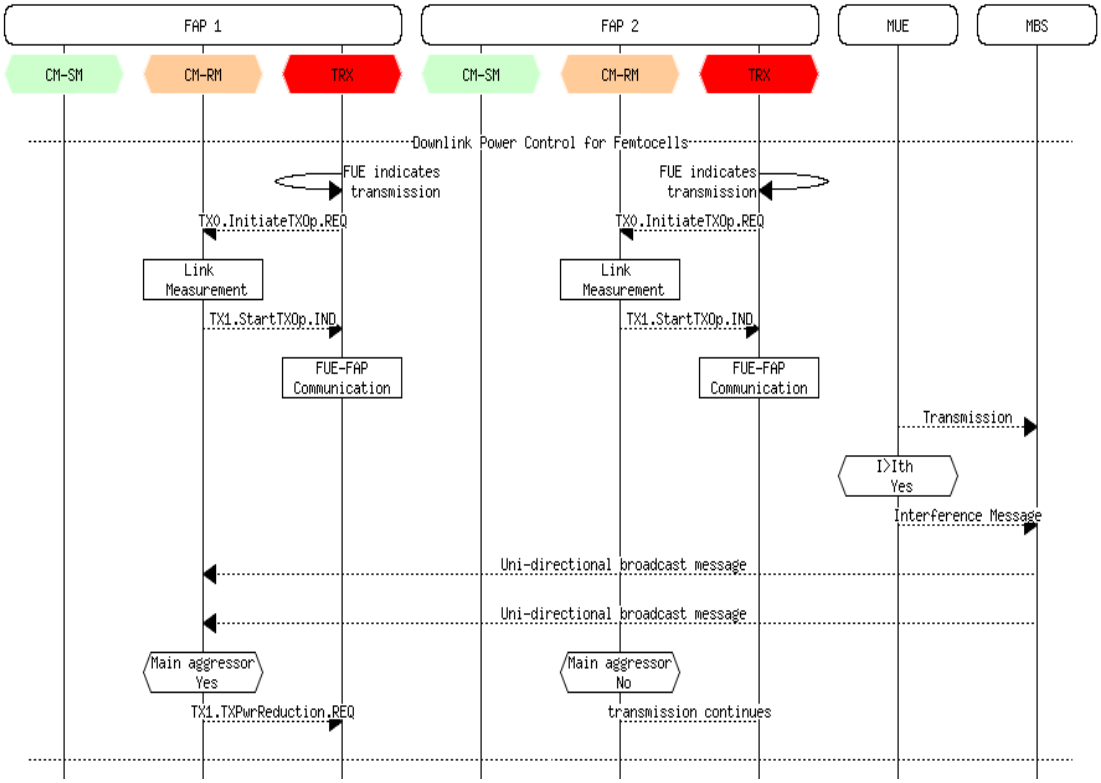

Figure 17: Message sequence chart for femtocell downlink power control

Normally, the FUE sends a transmit operation request to its FAP using a `TX0.InitiateTXop.REQ` command as seen in Figure 17. This command is processed at the CM-RM module of the FAP where inferences on the link measurements (channel) and power control configurations are made and passed to the FUE through a `TX1.StartTXOP.IND` indicator. FUE therefore starts transmission based on configuration parameters (power level) received from its FAP. Whenever a FAP have to reduce its power as a result of information from the MBS, it reduces its power by a fixed step size Δ and correspondingly re-calculates configuration parameters which are conveyed to its active FUE. This reduction in power is to make sure the FAP reduces the amount of interference to an MUE. Both the value of aggressor distance t and Δ can affect the performance of the algorithm. The algorithm after reduction of power operates normally until it receives another message from the MBS to reduce its power.

Femtocell simulation results and discussion

Simulations are carried out in order to evaluate the performance of the algorithm. The simulation parameters are given in Table 1.

Table 1: Femtocell simulation parameters

parameter name	Value
number of MUEs	20
number of femtocells	0 – 200
number of channels	20
macro-cell radius	500m

femtocell transmit power	-20dBm
MUE interference threshold	-100dBm
wall losses L_{wall}	15dB
aggressor distant t	50m

The simulation is carried out with 20 MUEs in a macrocells with different number of femtocells. The locations of MUEs and femtocells are taken randomly and interference faced by MUEs with increasing number of femtocell is calculated. The results are shown with the total interference in system (I_T), which is the sum of aggregate interference faced by all MUEs and given as (0-4):

$$I_T = \sum_{n=1}^{20} I_n^{fm} \qquad (0\text{-}4)$$

where I_n^{fm} is the interference faced by each MUE in the n^{th} channel. The result in Figure 18 shows that the total interference in the system is reduced with the proposed power control algorithm. Notice that for any given number of femtocells, the algorithm makes sure all the MUEs are interference free. This algorithm gives higher priority to MUEs and therefore, the transmit power is reduced whenever an MUE is under interference due to a nearby femtocell. The number of MUEs within the macrocell also has an impact on the overall performance as shown in Figure 19.
Increasing in the number of MUEs increases the total interference in the system as seen in Figure 19. It can also be inferred that increasing the number of MUEs would also increase the processing overhead, as the femtocells would then have many MUEs in its main aggressor list.

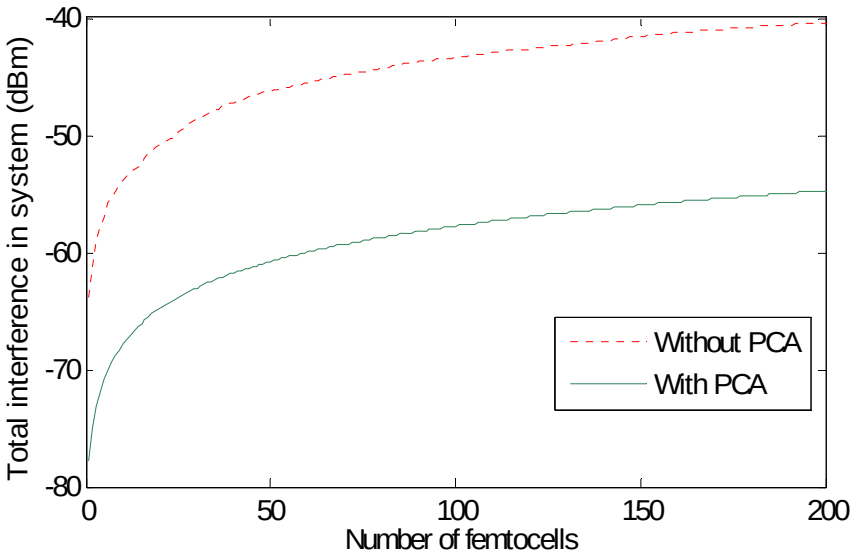

Figure 18: Performance of the downlink power control algorithm

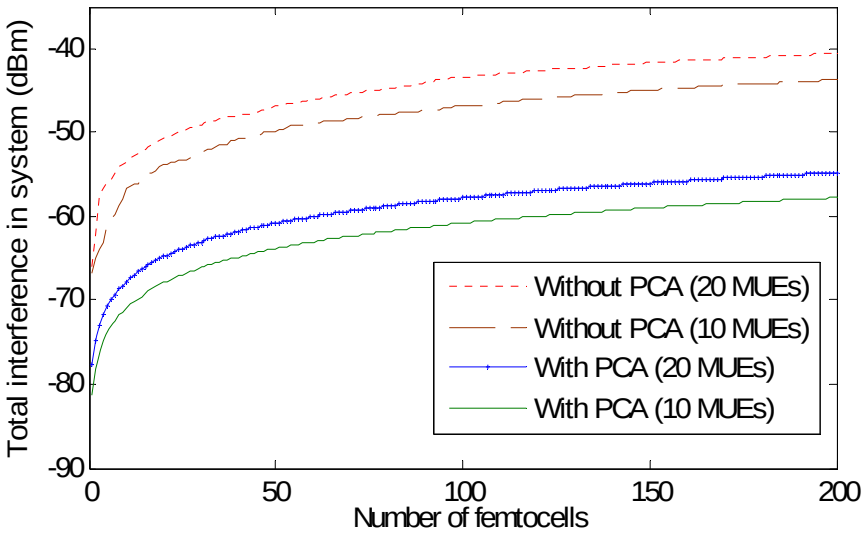

Figure 19: Comparison of PCA with different number of MUEs

The aggressor distance has an impact on the overall performance, which can be seen in Figure 20. Decreasing the aggressor distance reduces the overall performance. It is worthwhile to note here that the increase in distance does not increase the performance after a certain value, which in this case is 50 metres. The performance at an aggressor distance 50 metres and 70 metres is almost the same. Therefore, the aggressor distance of 50 metres has been used in this algorithm. The algorithm is a simple one and thus suitable for implementation in low powered FAP devices. It also makes sure the far away FAPs do not need to arbitrarily reduce their power if they are not causing interference to MUEs.

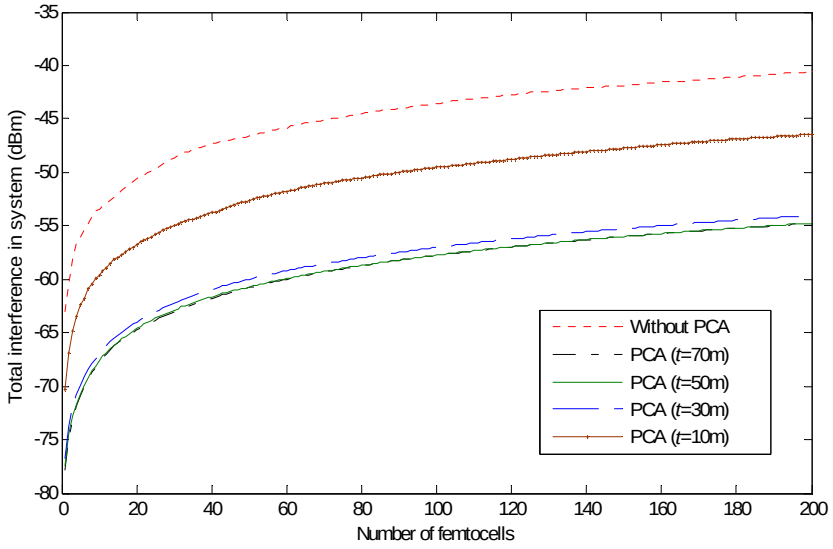

Figure 20: Impact of aggressor distance on the overall performance

Ad hoc networks scenario

Cognitive ad hoc networks can be set up by different types of nodes which may be static, nomadic or mobile depending on the use cases envisaged. Their existence is limited in time (like for emergency or big event) and they allow the operating frequency band to be adapted to the specific needs in bandwidth, range and QoS.

The case of multiple cognitive ad hoc networks sharing the same portfolio of available channels in a given area is considered. Each cluster-based single ad hoc network has a star topology as depicted in Figure 21. The nodes/UEs are grouped into one cluster with one node/UE having the additional functionality of cluster head (CH). It is assumed that the management of the resources is centralised and implemented in the CH providing routing, resource allocation and power control functionalities whereby communication flows are exchanged directly between nodes when possible.

In this scenario, the focus is on finding necessary algorithms for sharing efficiently the available channels in the CM-RM portfolio among different clusterized mobile ad hoc networks employing scheduled access protocol and not random access ones.

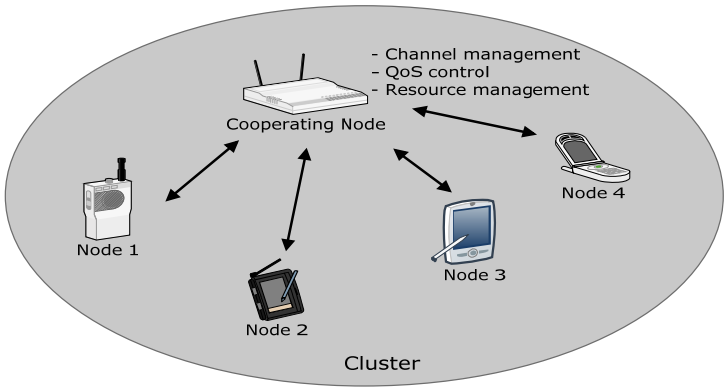

Figure 21: Cluster based ad hoc network with star topology

System description

Time-division multiple access (TDMA) communications in a time-division duplexing (TDD) mode using OFDM transmission technique is considered. Since the nodes inside a cluster share the same band, both for transmitting and receiving, then the nodes must transmit and receive on separate slots. The switch from transmitting state to receiving state can be handled during the guard time which is present at the beginning of any slot (beacon, random access and data). The corresponding TDMA frame structure is illustrated in Figure 22 and it is divided into signalling, incumbent detection, and communication phases.

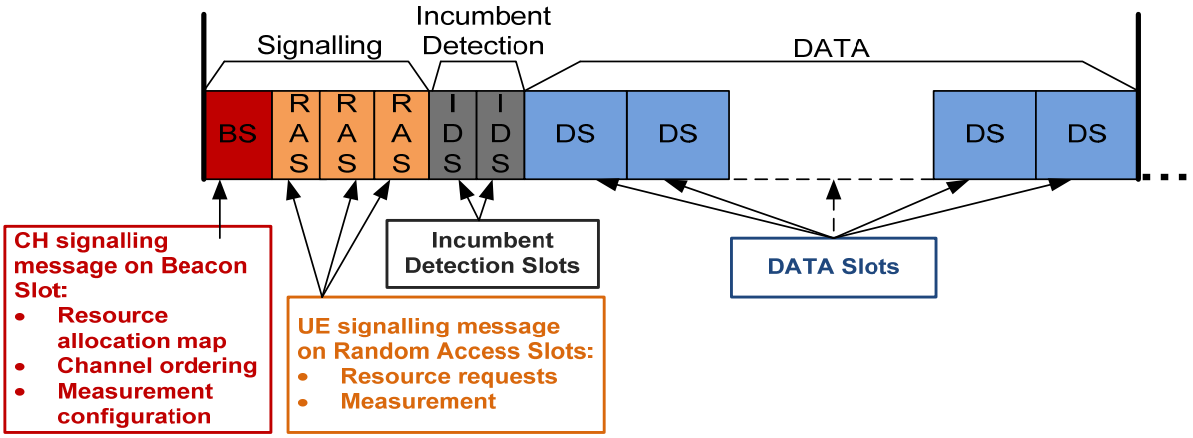

Figure 22: TDMA frame structure with the signalling, incumbent detection, and the communication phases

Signalling phase

The beacon slot is used by the CHs to send CH signalling message that indicates to the nodes the use map of the data slots in the communication phase, and serves also for time and frequency synchronisation purposes. The map allows the members of the cluster to know on which time/frequency resources the communication links are scheduled.
The beacon indicates also information about available channels in the portfolio and sensing directives.
The random access slots (RAS) have three main purposes:

- the resource allocation requests sent by each node to its cluster head;
- the network synchronisation messages are transmitted and detected during these slots and are used for neighbouring discovery and topology control;
- the sensing measurement reporting by the nodes to their CH.

Incumbent detection phase

One or several random access slots are dedicated to incumbent users' detection on the operating channel. It is chosen to rather dedicate for this purpose RAS than data slots as signalling messages are exchanged on each frame, which is not the case of data protocol data units (PDU). The RAS slots being much shorter than the data slots, this choice permits also to preserve the network useful throughput.

Resources allocation and QoS support

QoS management is performed at link level for peer-to-peer communications. We consider two QoS classes:

1. best effort (BE) for data (files, images, etc.);
2. real-time (RT) for voice and urgent traffic that is needed in emergency situations.

The resource allocation proposed in the QoSMOS context is split into two stages. The first stage referred to as demand adaptation (DA) consists in pre-processing the brute demand of the queues by taking into account the QoS classes, then a recursive per-slot allocation is performed taking as inputs the list of candidate links elaborated by the DA. Detailed description of the algorithm is given in [D5.2]

Sensing control

The sensing operation of the cognitive ad hoc network is monitored by the CH. The sensing control directives are part of the beacon message. These directives are given in terms of the list of available channels listed from the best to the worst (channel sorting algorithm is given thereafter), and the target number of measurement to be done on each channel.
Each node performs then the sensing in a distributed and opportunistic manner in order to best fulfil the directives of the CH. In doing so, the need of having the CH sending explicit sensing commands to the nodes is avoided and thus we save signalling bandwidth. Moreover, there is no guaranty that a network is able to sense all available channels unless it dedicates some slots for sensing on every channel.

Incumbent user protection

Upon the detection of an incumbent user on the operating channel, the nodes stop immediately transmitting data. If a node detects the incumbent presence on a given channel then it informs its CH in its signalling message. The CH marks the channel where incumbent users are detected as

not available and excludes it from the channel selection process until it is sensed again as free from incumbent users. If an incumbent is detected on the operating channel, the CH selects another one immediately and informs the nodes in its cluster.

Sensing procedure

The sensing operation is done by each node in the network in a distributed and opportunistic way, driven by sensing directives of the CH.
Indeed, let C={C1,…,Cn} be the list of sorted available channels, T={T1,…,Tn} be the list of the corresponding target number of measurement asked by the CH, and M={M1,…,Mn} be the number of corresponding performed measurements. Then, when a node is not transmitting and has no data to receive on a given slot, it selects to listen to the channel of the portfolio that maximises the cost function:

$$F(C_i) = \frac{T_i - M_i}{i} \qquad (0\text{-}5)$$

The measurement process is of moving average type. The sliding window size is a multiple of the frame duration

Channel selection algorithm

The role of the channel selection algorithm (CSA) is to provide a list of active channels sorted out from the best (ranked #1) to the worst, the best being taken as the operating channel. The remaining channels are kept to serve as reserve channels in case the operating channel needs to be freed, and are selected in the decreasing quality order. The CSA process is performed at the CHs based on local measurements by the CH itself and reported measurement from the UEs
A metric that reflects the channel quality needs then to be chosen in order to sort out the available channels. It is assumed that at a ggiven time in the ad hoc network all the links that need to be served (called “links in operation” in the sequel) are identified and for each of them also the corresponding doublet (data rate demand (queue size), priority). The metric considered here is then the maximum data rate that the cluster can achieve for the set of links in operation, and for the highest priority. This metric allows fulfilling the QoS since the highest priority will be served first and the maximum data rate ensures the efficient use of the radio resources.
The first approach to select the channel that maximises the above metric is to run the resource allocation algorithm (RAA) for all the available channels. This will guarantee that the channels order will be in accordance with respect to the RAA capabilities. The possible issue with this approach is the computation complexity since the RAA is rather demanding, and this method would need to run the RAA as many times as the number of candidate channels.
To overcome the issue of the direct approach, it is here proposed to use as metric the weighted sum of the link capacity (over the set of operating links) computed using the Shannon capacity as a function of the SINR and is referred to as WSLA (weighted sum link approach). The weight applied to each link in the metrics computation is the rate demand normalised by the total rate demand. This normalisation is for fairness issue between links of the same priority.
The metric is given as follows

$$SR(c, p) = \frac{1}{\sum_{i=1}^{N}\sum_{j=1}^{N} R_{i,j}(p)} \sum_{i=1}^{N}\sum_{j=1}^{N} R_{i,j}(p)\log(1 + SINR_{i,j}^{c}) \qquad (0\text{-}6)$$

Where $SINR^{c}_{i,j}$ is the signal to noise-plus- interference ratio of the link between source *i* and destination *j* on channel *c* of the portfolio, and $R_{i,j}(p)$ is the asked rate of the flow demand on this link having priority *P*.

This metric requires little computation effort to the expense of eventual performance degradation. In the following, we compute performance results of both approaches to evaluate the degradation of the SLA compared to the RAA.

Both approaches have been compared through simulations. The simulation settings are: $N = 10, 20, 30$ nodes in the cluster, Rayleigh fading, and fixed transmit power. The number of candidate channels in the portfolio provided by the CM-SM is 15.

Results are reported in Figure 23 which presents the probability that the *k*-th channel identified by WSLA is equal to the operating channel (#1) chosen by the RAA f It can be seen that the WSLA performs well and the performance is improved as the number of nodes increases. The probabilities that the two methods choose the same operating channel are equal to 0.68, 0.92, 0.99 for $N = 10, 20, 30$ respectively. This can be explained by the average effect since the number of operating links increases with the number of nodes. Thus from the simulations it can be concluded that, when the number of nodes is large enough (e.g. $N \geq 20$), the SLA can be a good alternative to the RAA by achieving comparable performance at a lower computational cost.

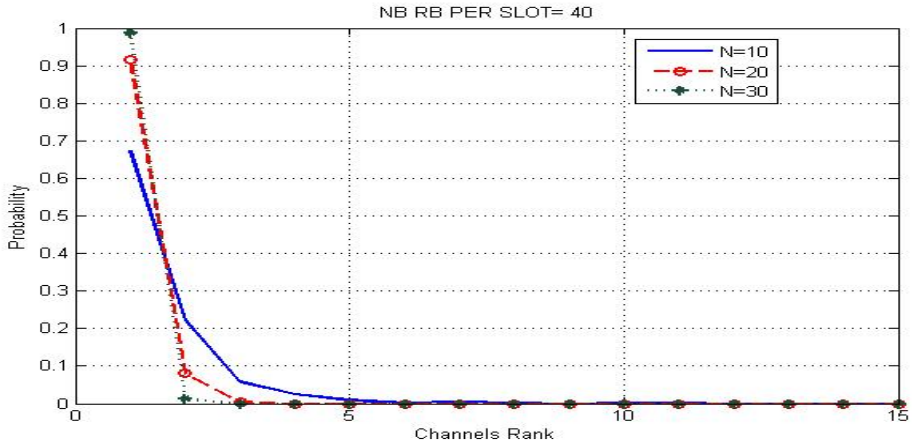

Figure 23: Channel selection algorithm performance vs network size

Channel acquisition protocol

Once the CH has identified the best operating channel to use using the channel selection algorithm, it notifies to the nodes in its cluster to switch to the selected channel.

The change of the operating channel may occur due to the detection of incumbent users or due to mutual interference caused by co-localised cognitive ad hoc networks sharing all the same portfolio of available channels. In the two cases, the decision of CHs to change their operating channels will occur somehow synchronously in time and will lead to a conflicting use of the radio channels in the first case, or will not resolve the conflicting use of the radio channels in the second one.

In order to reduce the probability of conflicting use of the operating channel among the cognitive ad hoc networks, the CHs will follow a channel acquisition protocol. The protocol is of the family of random access protocols and imposes to each CH that decides to change its operating channel to wait a random amount of time before the effective change (local change and notification to the nodes in its cluster).

During this random wait (multiple of frame time), the CH keeps updating its measurement about the available channels (local and remote measurements), and calling the channel selection algorithm on each frame. If the CSA detects that the current operating channel is again the best one then it cancels the channel change procedure and reset the channel change counter, otherwise it decrements the change counter. Once the counter is zero the change is performed and notified to the nodes in the cluster.

Simulation results

The simulation framework is based on the event-driven discrete time simulation tool Omnet++ [Var]. The simulation considers complete mobile ad hoc network simulation from protocol layer L1 to L7 [MAS10].

Incumbent users protection scenario

In this scenario we are interested in the coexistence behaviour of cognitive ad hoc networks and incumbent networks. one mobile CAN and one fixed incumbent network are considered. At the beginning of the scenario, the CAN uses as operating channel the one of the incumbent network. The CAN then moves to cross the incumbent network area and to finish at the other side of it. In both networks, every node has one TX/RX flow to/from another node in its network. All the flows have the same throughput and are of best effort class of QoS. Figure 24 illustrates the scenario.

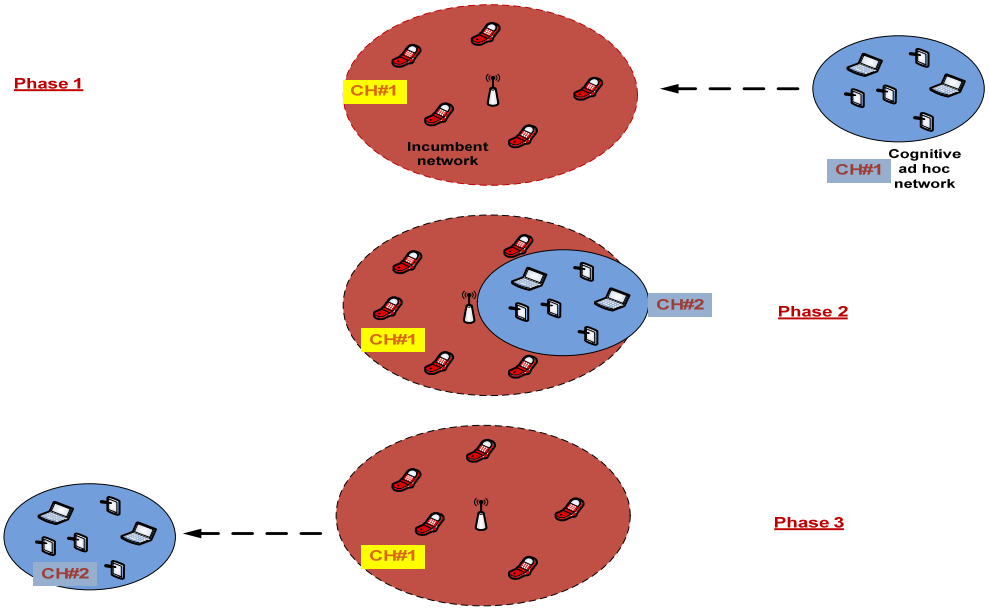

Figure 24: Incumbent users protection scenario

Figure 25 shows the achieved sum throughput of each network during the simulation time. The physical interference between the two networks lasts approximately 40 seconds from t=30s to t=70s.
It can be observed that immediately at the beginning of the mutual interference the throughput of the cognitive networks deeply decreases, while the throughput of the incumbent network remains unchanged. The decrease is due to the fact that as soon as the nodes of the CAN sense the presence of the incumbent users they stop transmitting data to not interfere the incumbent network. The CAN changes then the operating channel and restores the data transfers. The CAN takes approximately three seconds only to change the operating channel and to retrieve the same level of data throughput as before the detection of the incumbent network.

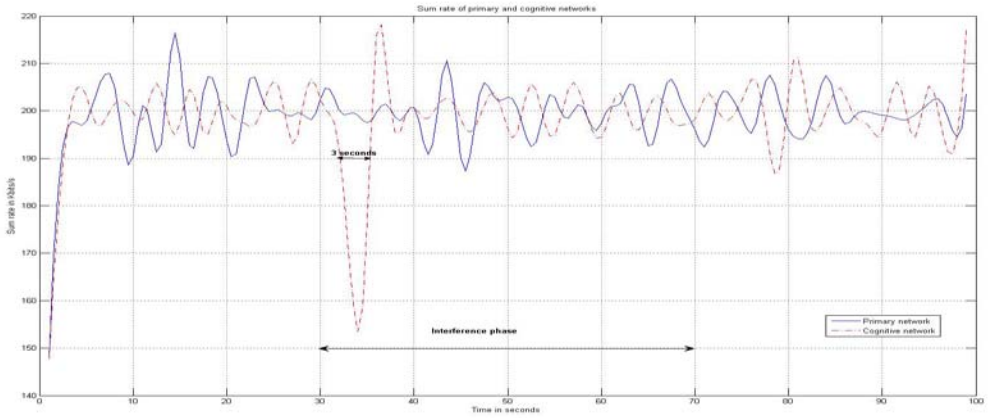

Figure 25: Sum rate of incumbent and cognitive networks

Co-localised cognitive ad hoc networks scenario

Let us focus on now the coexistence behaviour of these cognitive ad hoc networks and two mobile CANs are therefore considered. At the beginning of the scenario the CANs use the same operating channel. The CANs then moves toward each other and exchange their initial position at the end of the scenario.

In both networks, every node has one TX/RX flow to/from another node in its network. All the flows have the same throughput and are of best effort class of QoS. Figure 26 illustrates the scenario.

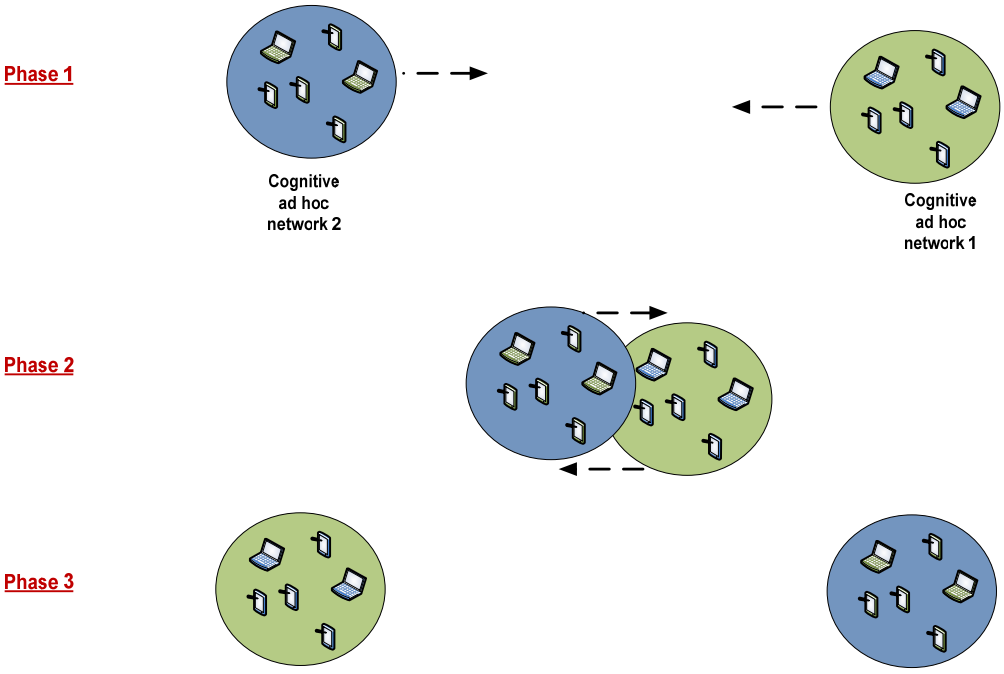

Figure 26: Co-localised cognitive ad hoc networks scenario

Figure 27 depicts the achieved sum throughput of each network during the simulation time. The physical interference between the two networks lasts approximately 40 seconds from t=30s to t=70s.
It can be again observed that immediately at the beginning of the mutual interference, the throughput of both networks decreases, but slightly this time as the CANs do not stop transmitting data. The decrease is due to interference and to operating channel change but last only four seconds approximately.

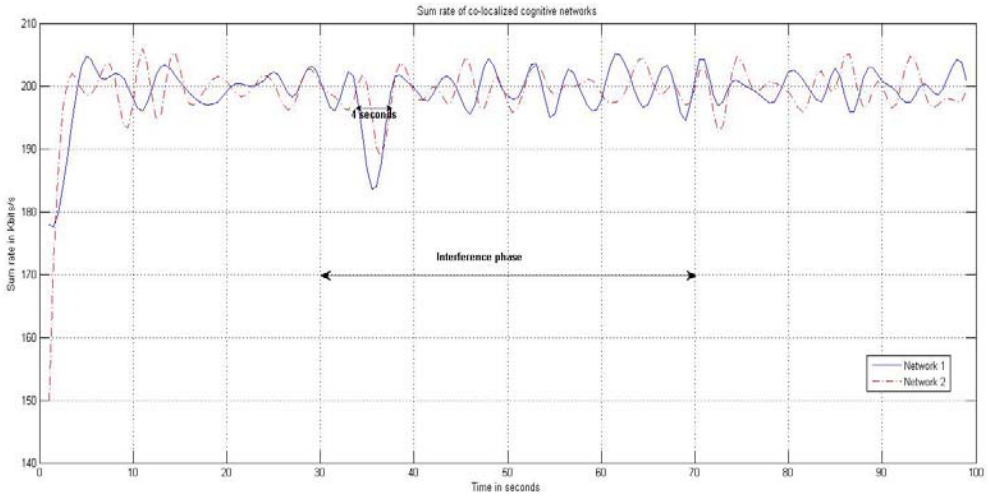

Figure 27: Sum rate of co-localised cognitive networks

AUTHORS

Hicham Anouar, Thalès Communications & Security, FR
Péter Bakki, University of Budapest, HU
János Bitó, University of Budapest, HU
Keith Briggs, British Telecom Research, UK
Ulrico Celentano, University of Oulu, FI
Olasunkanmi Durowoju, University of Surrey, UK
Martina Fuentevilla, TST Sistemas, SP
Tao Guo, University of Surrey, UK
Péter Horváth, University of Budapest, HU
Ingo Karla, Alcatel-Lucent Bell Labs, GE
Zsolt Kollár, University of Budapest, HU
Stéphanie Leveil, Thalès Communications & Security, FR
Miguel López-Benítez, University od Surrey, UK
Richard MacKenzie, British Telecom Research, UK
Geneviève Mange, Alcatel-Lucent Bell Labs, GE
Arturo Medela, TST Sistemas, SP
Juan Rico, TST Sistemas, SP
Christophe Rosik, NEC Technologies UK, FR
Isameldin Suliman, University of Oulu, FI
Johanna Vartiainen, University of Oulu, FI

ACKNOWLEDGMENTS

This work has been performed in the framework of the EC funded project QoSMOS, FP7-ICT-2009/248454.

REFERENCES

[D1.2] R. MacKenzie, P. H. Lehne, U. Celentano, M. Ariyoshi, B. Cendón, A. Medela, “QoSMOS consolidated scenarios”, Deliverable D1.2 (PU), 31 p., 23 Dec 2010.

[D2.1] M. Ariyoshi, K. Arshad, B. Bochow, U. Celentano, B. Cendón, R. Datta, P. Delahaye, J. Gebert, O. Grøndalen, P. H. Lehne, P. Marchand, K. Moessner, D. Noguet, G. Yuming, “Initial description of system architecture options for the QoSMOS system”, Deliverable D2.1 (RE), 79 p., 7 May 2010.

[D2.2] S. Leveil, C. Le Martret, O. Grøndalen, B. Bochow, C. Rosik, V. Mérat, B. Cendón, J. Herrero, A. Medela, U. Celentano, R. Datta, F. Noack, C. Lange, J. Gebert, K. Moessner, H.Sugahara, K. Muraoka, M. Ariyoshi, “System architecture options for the QoSMOS system”, Deliverable D2.2 (PU), 106 p., 24 Dec 2010.

[D2.3] G. Mange, P. Horváth, V. Berg, B. Bochow, R. Robles, M. Ariyoshi, C. Rosik, O. Grøndalen, P. H. Lehne, J. Rico, A. Medela, R. Datta, U. Celentano, “System specification and evaluation criteria”, Deliverable D2.3 (PU), 95 p., 30 Nov 2011.

[D3.4] U. Celentano, K. Muraoka, M. Ariyoshi, A. Bagayoko, D. Panaitopol, P. Delahaye, X. Yu, P. Navaratnam, K. Moessner, A. Gameiro, F. Kemeth, R. Wansch, D. Noguet, V. Berg, “Reference protocol stack for QoSMOS”, Deliverable D3.4 (PU), 56 p., 2 Apr 2012.

[D5.2] G. Mange, P. Horváth, R. MacKenzie, K. Briggs, M. Fitch, C. Rosik, S. Leveil, C. Le Martret, R. Massin, P. Fouillot, A. Sanz, B. Cendón, A. Medela, J. Rico, K. Arshad, T. Guo, U. Celentano, ”Final framework description, preliminary cognitive manager structure and first mechanisms for QoS support”, Deliverable D5.2 (RE), 109 p., 13 Jul 2011.

[ABI2007] ABI Research, Picochip, Airvana, IP access, Gartner, Telefonica Espana, 2nd Intl. Conf. Home Access Points and Femtocells; available on line at: http://www.avrenevents.com/dallasfemto2007/purchase presentations.htm.

[CelEtal2011] U. Celentano, B. Bochow, C. Lange, F. Noack, J. Herrero, B. Cendón, O. Grøndalen, V. Mérat, C. Rosik, “Flexible architecture for spectrum and resource management in the whitespace”, Proc. Int. Symp. Wireless Personal Multimedia Commun. (WPMC 2011), Brest, France, 3-7 Oct 2011.

[Chan2008] V. Chandrasekhar, J. Andrews, “Femtocell networks: A survey”, IEEE Commun. Mag., vol. 46, no .9, pp. 59-67, Sep. 2008.

[COR11] Common Object Request Broker Architecture (CORBA/IIOP) v3.2 Nov 2011.

[DatEtal2011] R. Datta, G. Fettweis, Zs. Kollár and P. Horváth, “FBMC and GFDM interference cancellation schemes for flexible digital radio PHY design”, Proceedings of the 14th EUROMICRO Conference (Euromicro'11), Oulu, Finland, 2011.

[Hos05] M. Hossam Ahmed, “Call admission control in wireless networks: A comprehensive survey”, IEEE Communications Magazine, Jan 2005.

[KliEtal2009] A. Kliks, A. Zalonis, I. Dagres, A. Polydoros, H. Bogucka, “PHY abstraction methods for OFDM and NOFDM systems”, Journal of Telecommunications and Information Technology (JTIT), 3/2009.

[LehEtal2012] P. H. Lehne, R. MacKenzie, O. Grøndalen, P. Grønsund, K. Briggs, “Business opportunities and scenarios for cognitive radio systems”, QoSMOS whitepaper, Apr 2012. http://www.ict-qosmos.eu/

[LevEtal2012] S. Leveil, C. Martret, H. Anouar, K. Arshad, T. Zahir, J. Bito, U. Celentano, G. Mange, J. Rico And A. Medela, “Resource management of centrally controlled cognitive radio networks”, Proc. Future Network & Mobile Summit (FuNeMS 2012), Berlin, Germany, 6-8 Jul 2012.
[MacEtal2011] R. MacKenzie, P. H. Lehne, U. Celentano, “Identifying scenarios with high potential for future cognitive radio networks”, Proc. Future Network & Mobile Summit (FuNeMS 2011), Warsaw, Poland, 15-17 Jun 2011.
[Mas10] R.Massin, C. Lamy-Bergot, C. J. LeMartret, and R. Fracchia, “OMNeT++-based cross-layer simulator for content transmission over wireless ad hoc networks”, EURASIP Journal on Wireless Communications and Networking, vol. 2010, article ID 502549.
[Var] A. Varga, “OMNeT++ discrete event simulation system”, http://www.omnetpp.org/
[XML99] XML-RPC Specification, D. Winer, Jun, 1999.
[Zah2012] T. Zahir, K. Arshad, A. Nakata, K.Moessner,”Interference management in femtocells”, IEEE Communications Surveys & Tutorials, vol. 99, pp.1-19, 2012