SDR and Cognitive Radio for Military Applications

Tricia J. Willink
Communications Research Centre
3701 Carling Ave., Box 11490, Station H
Ottawa, ON, K2H 8S2
CANADA

email: tricia.willink@crc.ca

ABSTRACT
The development of software-defined radios (SDRs) should provide a small, light and cost-efficient platform capable of supporting multiple waveforms over a large frequency range. While there are challenges in achieving the vision of rapidly portable waveforms, the SDR is a critical technology for future military communications, and is an enabling platform for cognitive radio. Cognitive radio is proposed as a technology for exploiting the EM spectrum more effectively. While the main frequency bands of interest are fully licenced to authorised users, they are often unoccupied over large geographic areas or for significant time intervals. Cognitive radios are envisioned as aware, adaptable and intelligent devices, capable of learning and operating autonomously in a wide range of scenarios. The key feature of cognitive radios is the capability to identify unused frequency bands, to jump to them and select appropriate radio parameters. These radios must be able to operate without causing unacceptable interference to authorised users of the frequency band, therefore they must monitor for the presence of the primary user, and take into account the possible location of receivers of its signals.

INTRODUCTION

The adoption of the network-centric warfare (NCW), or net-enabled operations (NEOps), philosophy by western and allied nations requires a similarly revolutionary approach to communications technology. The basis of NEOps is the sharing of information among front-line forces, decision makers, sensors, weapons, etc. This information sharing will result in improved situational awareness, faster command decisions, improved survivability and greater mission success. Essentially, NEOps places information at the centre of combat operations.

This massive increase in information must be transferred wirelessly among the combat participants. At the same time, civilian and commercial interests are placing a high economic value on the radio spectrum, pressuring military users to reduce, not increase, their allocated bands. While the VHF and UHF bands are fully allocated in most regulatory domains, measurements of this range of spectrum show that many

Willink, T.J. (2007) SDR and Cognitive Radio for Military Applications. In *Emerging Wireless Technologies* (pp. 8-1 – 8-20). Educational Notes RTO-EN-IST-070, Paper 8. Neuilly-sur-Seine, France: RTO. Available from: http://www.rto.nato.int.

allocations are unused, part or all of the time, as indicated in Fig. 1. This presents an opportunity for radios that are agile and smart enough to make use of allocated bands where and when they are unoccupied by the assigned users. This requires, at a minimum, adaptive capability: the ability to sense occupancy and to react by changing carrier frequency. With additional intelligence, the radio might 'figure out' suitable operating parameters based on sensing its environment, for example, altering its bandwidth and packet length to fit within unoccupied blocks of frequency at different times. Radios with this capability to reason, perhaps with higher levels of intelligence and memory, are referred to as **cognitive radios**.

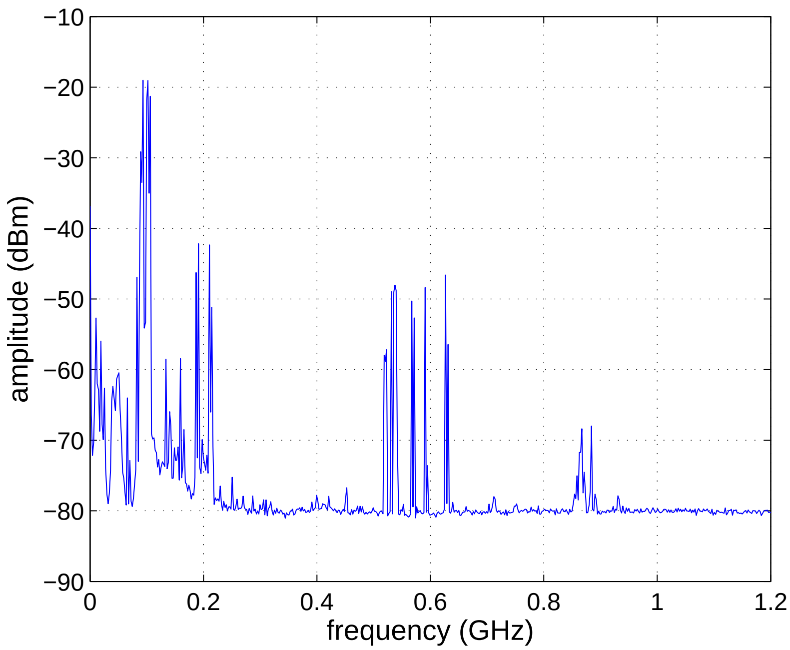


Figure 1: **Spectrum occupancy measured at the Communications Research Centre in rural Ottawa**

Cognitive radios can support the increased need for networked communications and situational awareness by observing and understanding their environment, applying appropriate policies and behaviours and learning from their experiences. Their primary objective is to make more efficient use of the spectrum, both in terms of accessing un- or under-utilised bands and also by effective resource management.

At the same time as cognitive radios provide new capabilities, they must support existing communications equipment. Legacy radios have multiple waveforms, operating with different radio parameters, which must be incorporated into new systems. Size and cost constraints motivated the use of **software-defined radios**, which are able to change waveforms and radio characteristics for interoperability, performance and adaptability. Ideally, over-the-air updates could provide platforms with new capabilities as they are required, for example, for coalition operations. In reality, the need for interoperability limits the achievability of the goal for small, light and cheap platforms.

There are many facets to the study of cognitive radio, from the 'bird's-eye' view assessing the interaction and network-wide impacts of different capabilities, through more conventional points-of-view such as adaptive waveform design and signal processing, to knowledge representation and ontologies (models of concepts and their relationships). The objective of this paper is to present the capabilities and challenges of cognitive radio technology from the perspective of military communications, and will focus on the 'engineering' rather than the 'computer science' aspects. In doing so, an idealised vision of cognitive radio will be assumed, which does not respect the hierarchy and boundaries imposed by the OSI layer model.

In the first part of this paper, a brief overview of SDR is given: details of specific SDR implementations can be found elsewhere. While the SDR technology is not necessary for the implementation of cognitive radios, it provides a natural platform due to its flexibility and programmability. Cognitive radio (CR) concepts are introduced in Part II, where a framework is developed to describe the levels of cognitive capability and some key challenges in CR technology are discussed.

Part I – Software-Defined Radio

The term "software-defined radio" (SDR) has different definitions within different organisations. Some examples are:

International Telecommunications Union (ITU): "A radio in which the RF operating parameters of frequency range, modulation type, and/or output power can be set or altered by software, or the technique by which this is achieved."

SDR Forum (SDRF): "A radio that provides software control of a variety of modulation techniques, wide-band or narrow-band operation, communication security functions (such as hopping), and waveform requirements of current and evolving standards over a broad frequency range."

US Federal Communications Commission (FCC): "A radio that includes a transmitter in which the operating parameters of frequency range, modulation type or maximum output power (either radiated or conducted), or the circumstances under which the transmitter operates in accordance with Commission rules, can be altered by making a change in software without making any changes to hardware components that affect the radio frequency emissions."

Note that the ITU definition includes both transmitters and receivers, while the FCC definition specifically excludes receivers alone. A survey of the R&D literature shows that the latter is not a widely accepted limitation of the definition. The common ground is that SDR is a radio platform in which certain operating parameters, such as frequency carrier and bandwidth, waveform and transmit power, can be modified in software without changes to the hardware itself.

I-1 SDR CONCEPTS

The SDR Forum has defined four tiers of software radios, as summarised in Table 1. Most commercial devices such as cell phones would fall into level 1.

The current state-of-the-art is level 2, which implements most of the physical layer in software, notably carrier frequency and bandwidth selection, waveform generation/detection and source coding, as well as functions such as cryptography. The supported frequency bands are limited by the RF front-end. Fig. 2 shows the typical architecture of a level 2 SDR.

The highest-level, the "ultimate software radio", is envisaged as being fully implemented in software, including the higher-layer OSI stack functions, with software-programmable filters and antenna tuning for

Table 1: Four tiers of software-defined radio (from SDR Forum)

Tier	Description
0 - Hardware radio	traditional radio implementation in hardware
1 - Software-controlled radio	control features for multiple hardware elements implemented in software, e.g., power level, but not modulation
2 - Software defined radio	control of modulation, bandwidth, security, waveform generation and detection implemented in software
3 - Ideal software radio	full programmability with A/D, D/A conversion at antennas
4 - Ultimate software radio	fully programmable traffic and control information, able to support a broad range of frequencies and functions concurrently, able to switch from one air interface to another in milliseconds

multi-frequency functioning. At this visionary level, the software radio would be able to switch almost instantaneously among applications and air-interfaces.

The key aspect of SDRs for military use is the portability of waveforms for interoperability. Within the NATO SDR User's Group **waveform** has been defined as:

> all aspects of a radio which are necessary to communicate interoperably over the air with another radio or radios employing the same standard. E.g. the "Waveform" is not only the air interface aspect of radio communication, but the entire function describing conversion of input data (bits or voice etc) to the output RF signal and vice versa, including transmission frequencies, modulation schemes, voice encoding, error protection, security etc. A waveform 'description' in this context may cover at least ISO layers 1-4 or even above.

For full interoperability, the hardware components of the SDR must be able to support a variety of **waveform definitions**, defined within the NATO SDR User's Group as:

> an exchangeable piece of software which contains all the information to implement a waveform upon a software defined radio platform. The "waveform definition" is all of the information which is required to be loaded into an SDR in order for it to be interoperable with another radio

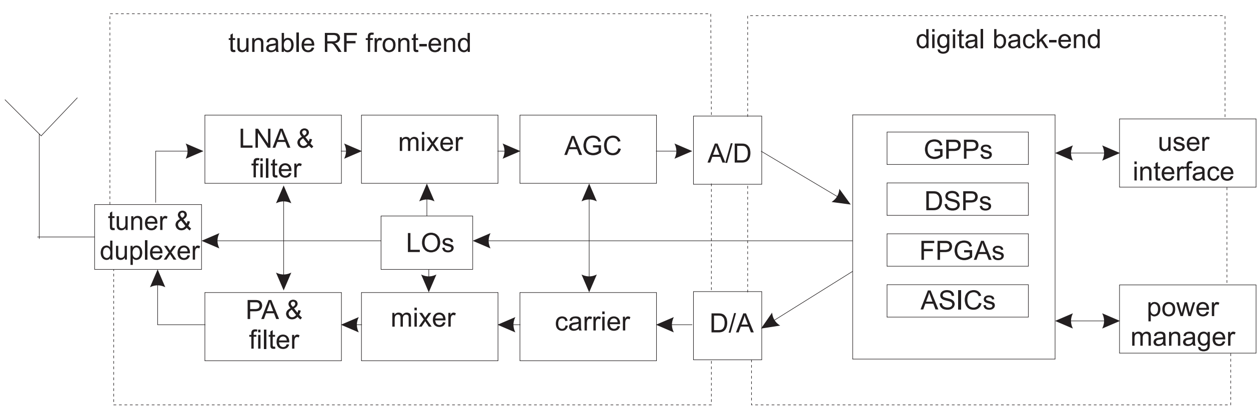


Figure 2: Typical architecture of an SDR [1, Ch. 1].

of a particular type.

Typical SDR hardware resources are general purpose processors (GPPs), digital signal processors (DSPs) and field-programmable gate arrays (FPGAs). The challenge for military communications is to achieve this flexibility at reasonable cost, as many commercial manufacturers opt for lower tier (level 1) implementations using system-on-a-chip (SoC) technology or application-specific integrated circuits (ASICs) that can be mass-produced cheaply. Consumer products tend to have a shorter life-span than is acceptable for military equipment, and models are continuously being upgraded with new features, such as cameras or MP3 players on cell phones, alleviating the requirement for upgradeable communications functionality.

SDR is an implementation concept: it is not specific to any standard, specification or application. However, the architecture of the SDR does influence its portability and interoperability. This is of primary concern for military and public safety users. The desire for a common architecture led to the development of the Software Communications Architecture (SCA) by the U.S. Department of Defense Joint Tactical Radio System (JTRS) project. The SCA provides specifications and software control commands for the interactions between different software and hardware components in the radio. It was adopted by the SDRF [2], and open source versions have been developed, notably the reference implementation SCARI-OPEN by the Communications Research Centre Canada [3], sponsored by the SDRF.

Note that the SCA itself is not sufficient to ensure true waveform definition portability. As noted in [4], “hardware technology is generally not sufficiently advanced to support the creation of truly portable waveforms”. Without some degree of hardware abstraction, the waveforms must be reconfigured for each SDR platform to accommodate different combinations and configurations of hardware resources. This can be a time-consuming task, and requires considerable expertise both in low-level programming and in signal processing. Abstractions of the interfaces to data transports, which connect the software and firmware components, and of the components will reduce the effort required to port waveform definitions from one platform to another, but they increase the complexity of the platforms themselves, resulting in larger, heavier systems that consume more power.

I-2 JOINT TACTICAL RADIO SYSTEM

The US Department of Defense (DoD) led the early effort in building software radios. The Air Force Rome Labs (AFRL) made a ‘programmable modem’, which laid the ground work for the SPEAKeasy program in conjunction with DARPA. SPEAKeasy was a programmable, multimode, multiband system, which took advantage of state-of-the-art technology to replace many analog radio components with programmable DSPs. The first phase, which was a large, full-rack device, was demonstrated to interoperate with fixed-frequency and frequency hopping radios from the HF to UHF bands [5]. This successful demonstration of the feasibility of a software radio was followed by the smaller, more portable SPEAKeasy II, which expanded the concept of modularity and reprogrammable architectures from user input/output to RF, and supported more waveforms operating from 2 MHz to 2 GHz [6]. These early technologies paved the way for the JTRS program, which will be used throughout the US military.

The JTRS program is currently organised by “domain” [7]:

Ground Domain	Ground Domain Ground Mobile Radio (GMR) support requirements for Army and Marine Corps Ground Vehicular platforms Handheld/ Manpack/Small Form Factor (HMS) support requirements for JTRS handheld and manpack units for platforms requiring a Small Form Fit radio
Airborne Domain	Airborne, Maritime and Fixed Site (AMF) support requirements for airborne (including rotary wing), maritime and fixed station platforms for all Services
Special Radios	JTRS Enhanced Multi-Band, Inter/Intra Team Radio (MBITR) support requirements for handheld radios for the Army, Navy, Marine Corps and Air Force Special Operations Forces

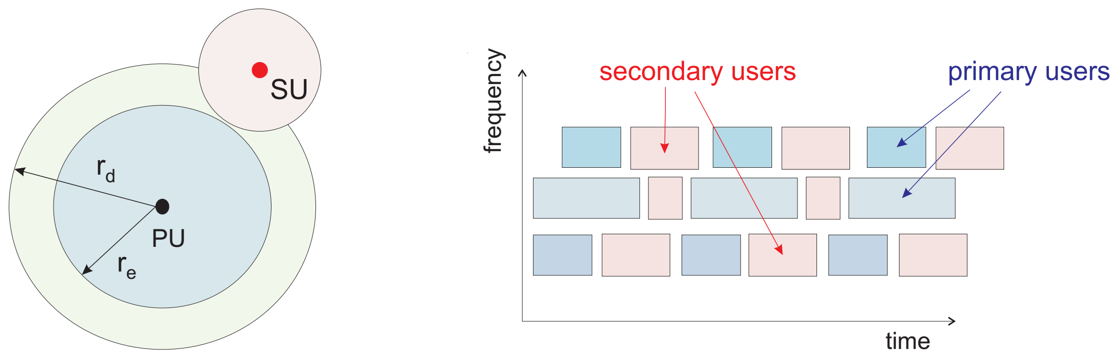
Part II – Cognitive Radio

Cognitive radios support the increased need for networked communications and situational awareness. Their capability to sense, learn, analyse and adapt autonomously will enable significantly more efficient use of the spectrum, both in time and in space. Awareness of other users and their requirements opens the possibility to use un- or under-utilised portions of the spectrum without disrupting existing military, government or civilian services.

The availability of regions of unused frequency bands in time and space provides the potential for increased spectrum access for opportunistic secondary users (SUs). In general (depending on the operational scenario and the rules of engagement), these SUs should not prevent the operation of primary receivers, that is, units that are listening to the primary users (PUs). Conceptually, this can be illustrated as in Fig. 3(a): when the PU is transmitting, SUs must not interfere with primary receivers within an exclusion zone, shown with radius r_e. This leaves primary receivers within the decodability radius, r_d, who could receive information from the PU *without* the presence of the SU, vulnerable to lose their connection when the SU is present. The allowable proximity of the SU to the PU is therefore dependent on the transmit power of the SU. This simple model is more complicated in practice: when there are multiple SUs, their combined interference must be considered; also, in the urban and complex terrain environments of main interest, the circular model does not adequately describe the true propagation conditions, hence distance alone is not adequate to determine operating region. Further complications arise when the PU is mobile. If the exclusion zone is established too conservatively, much opportunity for secondary use may be lost. In many systems, such as cellular networks, the central PU must also be able to detect and decode the low power signal from the remote primary node, therefore this model must be overlaid with equivalent versions for all remote nodes as PUs.

For PUs that transmit in predictable bursts, additional opportunities exist for SUs to occupy the quiet periods. The result of dynamic access in time might result in a spectral occupancy illustrated in Fig. 3(b). Rapid and accurate spectrum sensing is therefore of key importance in developing highly agile cognitive radios that can take full advantage of spectrum availability. Dynamic frequency access is discussed in Sec. II-3, following the conceptualisation of a cognitive radio framework in Sec. II-1 and an overview of the DARPA XG program in Sec. II-2.

In addition to spectrum sensing and frequency agility, the cognitive radio should be able to adapt its



(a) Spatial co-existence (b) Temporal co-existence

Figure 3: **Co-existence with primary users**

operating parameters, e.g., power, modulation, coding, spatial (MIMO) characteristics, to suit both the EM (propagation and interference) environment and the capabilities of the radio at the other end of the link. This may be a legacy radio, with less flexibility and no cognitive abilities, or it may be a more advanced device. A brief discussion of radio parameter selection is in Sec. II-4.

II-1 A FRAMEWORK FOR COGNITIVE RADIOS

The term 'cognitive radio' was proposed by Mitola in [8] to apply to a 'self-aware learning system'. Self-aware implies that the radio has a basic set of facts about its own operation and that it is able to communicate with other devices using these facts.

The cognition cycle can be described in terms of the OODA (Observe, Orient, Decide, Act) loop, as illustrated in Fig. 4. This was introduced by the military strategist John Boyd, who used it to formalise strategic decision-making strategies. This framework is helpful in understanding the operation of a cognitive radio, or network of CRs: in this context, the strategic goal is to achieve high-rate, robust communications everywhere, all the time.

There are four states:

- **OBSERVE**: information is collected such as interference and propagation conditions, signal monitoring, location and time, quality of service metrics.
- **ORIENT**: this state, illustrated in Fig. 5, is the most important from a cognition stand-point. It was originally conceived to incorporate characteristics such as cultural traditions and genetic heritage, as well as previous experience and new information, which are analysed and synthesised. From a CR perspective, the first two characteristics can be considered to be equivalent to *shared models* and *programmed models*. Shared models are traits, behaviours and policies that are shared among nodes: they can vary over time but the difference among nodes remains small. Programmed models would include imposed behaviours and operational policies such as radio capabilities and limitations on spectrum access affecting primary users: these are generally fixed over time, but may be different for different nodes.
- **DECIDE**: this state acts on the output of the orient phase to form a hypothesis, or plan, which is evaluated. A negative outcome results in a return to observe and thence to orient, while a positive plan results in moving to the act state.

- **ACT**: the plan is put into action, and the impact is used as an input in the observe state.

The "implicit guidance and control" connections between the **orient** state and the **observe** and **act** states are a key part of the cognitive cycle. The **decide** state represents explicit control of the **act** state: ideally, it is bypassed in favour of implicit guidance. A fast, effective OODA 'loop' would consist of the **observe** state passing relevant information to the **orient** state, which 'understands' the situation and 'knows' what to do, leading to the **act** state, where the required action is completed. In a command and control sense, the implicit guidance and control connection reflects the shared values and experiences, and a common understanding of intent. In essence, it makes the **observe** state focus on the most important features, based on increasing experience or understanding. Note that the 'implicit' nature of the guidance is important as it allows for mutating behaviour – the **observe** state may identify a significant input that was not requested, for example due to changes in the environment. The **decide** state is then activated only when no clear and effective action results from the **orient** state. This state delays completion of the goal, because it requires an experimental approach to finding the correct action. A key part of rapidly achieving successful actions is to have a good initial position, i.e., good situational awareness and good models (programmed or obtained through training), so the **decide** state can be bypassed.

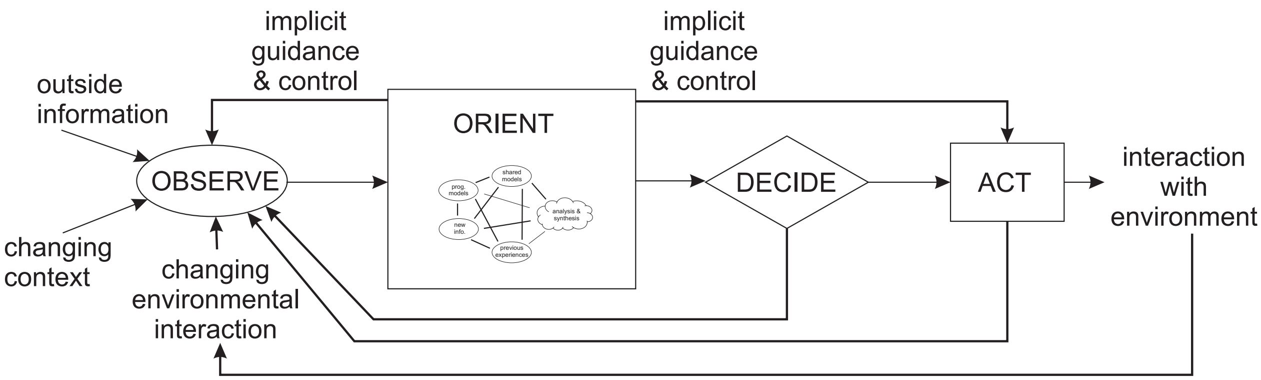


Figure 4: **OODA loop (modified from [9])**

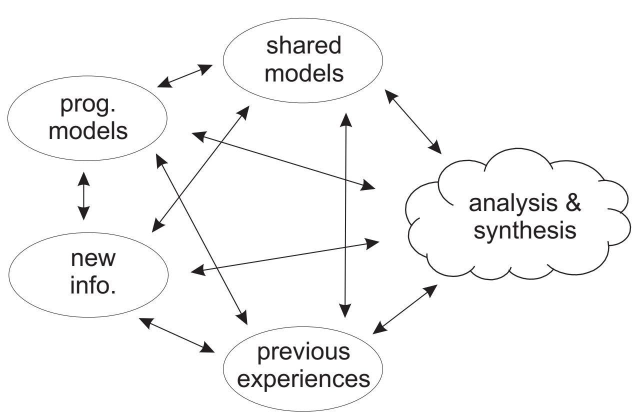


Figure 5: **Orient state of OODA loop (modified from [9])**

The degree of sophistication in the **orient** state, as well as in the capability to plan in the **decide** state,

Table 2: Levels of cognitive capabilities of radio

Level	Capability	Characteristics
-	User-operated	Operational modes selected by user
0	Adaptive	Autonomous selection of parameters (e.g., frequency, bandwidth, transmit power, waveform) to provide specified QoS
1	Reasoning	Determines suitable parameters based on context, e.g. application, propagation/interference environment
2	Planning	Evaluates programmed plans based on objectives, capabilities and reasoned information
3	Learning	Constructs models of capabilities, requirements, environment based on experience, and applies to decision making
4	Strategising	Modifies plans based on anticipated requirements, learned models, environment, capabilities etc.

determines the level of cognition of the device. Mitola suggested a nine-tier model of cognition in [8], but a simpler approach is proposed here. Table 2 gives a four-tier model in which each level adds a distinct type of behaviour. Note that this model specifically separates **adaptivity** from **cognition**; although the term 'cognitive radio' is becoming synonymous in the literature with 'dynamic spectrum' technology, in reality this capability is only *sensing*, which is part of the **observe** state in the OODA loop, and does not require any cognition. Thus, in this work, devices that simply sense the radio spectrum and select an unoccupied band for operation are labelled adaptive, not cognitive, radios.

For NEOps, the main case of interest is when the radio units form peer groups, or networks, that operate intelligently together to provide an improvement in end-to-end performance, for example by improving spectral efficiency, decreasing latent delays or reducing overall power consumption. For the purposes of this work, no assumptions are made about the type of network structure. In practice, typical operational structures might be mobile ad-hoc networks (MANETs) or autonomous sensor networks.

Level 0 - Adaptive

A number of existing systems exhibit a degree of adaptive behaviour. For example, the household cordless phone standard, digital European cordless telephone (DECT), senses the noise and interference on all the channels available to it, and selects the one with the lowest. IEEE 802.11 (WiFi) standards adapt the modulation and error correction schemes to provide acceptable quality of service. Within the NATO community, the 'HF House' concept, which includes fixed frequency (STANAGs 4539, 4285), frequency-hopping (STANAG 4444) and robust (STANAG 4415) waveforms along with an automatic radio control system (ARCS - STANAG 4538), provides adaptive radio capability, modifying carrier frequency, data rate and waveform based on user requirements and propagation and interference conditions.

For example, the definition of cognitive radio proposed by IEEE USA is "a radio frequency transmitter/receiver that is designed to *intelligently detect* whether a particular segment of the radio spectrum is currently in use, and to *jump* into (and out of, as necessary) the temporarily-unused spectrum very rapidly, without interfering with the transmissions of other authorized users".

Level 1 - Reasoning

At the **reasoning** level, the cognitive radio is capable of observing aspects of its performance, the environment and requirements; analysing these pieces of information along with internal policies, regulations, etc., and arriving at a course of action. Thus, this level operates in the **observe** and **orient** states of the OODA loop.

Level 2 - Planning

Planning in the cognitive radio context consists of evaluating possible solutions and selecting the one with the best expected outcome. As noted above, in the context of the OODA loop, this should be necessary only when the **reasoning** capability has failed to produce an effective action. Thus, part of this cognitive capability is to recognise this situation. In addition, the CR must be able to assess the effectiveness of the planned (or implemented) action, in order to improve the accuracy in the next OODA cycle.

Level 3 - Learning

In general, the **learning** ability in a cognitive radio deals with memory and model generation. Memory involves creating databases of experiences, for example, comprising the plans that were most successful in achieving their goals ("previous experiences" in the **orient** state). Over time, these experiences may lead to modified behaviours and policies, impacting the "shared model" in the **orient** state.

The impact of successful learning is in improving the actions selected in the **orient** state, thereby reducing the requirement to use the **decide** state and arriving at the desired goals more quickly, with fewer OODA cycles. The result is an improvement in overall performance (end-to-end spectral efficiency, power consumption, delay, etc.) of the cognitive system.

As with **reasoning** and **planning**, successful cooperative learning requires a greater benefit than cost; for example, an overall reduction in delay, power consumption and spectral occupancy when taking the overhead of information sharing and subsequent negotiation and adaptation into account.

Level 4 - Strategising

Strategising is the highest cognitive level, and requires a degree of sophistication and autonomy in the radio device that is unprecedented. It includes anticipating future requirements and conditions based on changes in context, environment, demands, etc., and modifying or innovating plans accordingly. A CR that is capable at Level 4 should be able to react effectively to unforeseen circumstances in a 'rational' way.

In terms of the OODA loop, this cognitive level can be thought of as identifying ambiguous situations in the **orient** state, and autonomously proposing intelligent plans, or hypotheses, in the **decide** state to determine an appropriate action. The difference between **strategising** and **planning** is in the autonomy that is applied to finding a solution: at Level 2, the CR proposes pre-selected options (possibly in order of likely success), while at Level 4, the plans are developed based on the information available at the **observe** and **orient** states.

An example of a CR capable of **strategising** is one that has learned models based in one environment, e.g., a fixed location, which now changes to a new environment, e.g., mobile. The CR would recognise that the change in observed behaviour is caused by the new context (mobility) and would adapt the plans and models it had been using.

Another example would be that the CR anticipates an increase in overhead information sharing, for example, resulting from new peer group members or a new activity, and re-prioritises its own data flow and clears its buffers, or perhaps goes into sleep mode to conserve battery power, in preparation.

II-2 THE DARPA NEXT GENERATION COMMUNICATIONS PROGRAM

The DARPA neXt Generation (XG) program was established to develop concepts and enabling technologies to achieve a dynamic redistribution of spectrum, providing assured communications for military operations. The objective is to increase the DoD spectrum access by a factor of ten for any networked radio. In Phase I (2002/03) it was determined that 94% of spectrum is unused, worldwide. The focus of Phase II was system and protocol design; currently Phase III, system development and demonstration, is in progress. In fact, a limited demonstration (six mobile nodes, six frequency channels, using WiMAX physical layer in the 225–600 MHz band) was undertaken in August 2006 [10]. This demonstration showed that the three core principles could be achieved, namely:

- no harm – the system causes no harmful interference to legacy systems by detecting other emitters, informing other nodes, adhering to spectrum use policies;
- works – dynamic connections are made and maintained among XG nodes in a non-XG environment (six node network formed in ≤ 30 s, re-establish time ≤ 0.5 s, net join time ≤ 5 s);
- adds value – spectrum management time is reduced and network capacity increased.

One of the most significant conclusions from the XG program so far is that there is a need for policy-based behaviour, in particular [11]: reasoning for controlling real-time processes; declarative language expression; and provable policy expression and implementation. Such policies might form part of the “Rules of Engagement”, for example, describing acceptable behaviours (protect, avoid interference, etc) for different primary users at different stages of a conflict.

The next steps in the XG program include integration into networked technology to enable different topologies, scalability development, incorporate greater selection of waveforms, and continue development of spectrum access behaviour to address DoD needs.

II-3 DYNAMIC FREQUENCY ACCESS

The fundamental purpose of the cognitive radio is to identify and exploit un- or under-used spectrum, such that there is no degrading interference to primary, or allocated, users of the frequency bands. In the literature, these are identified as white (un-used) and gray (low primary user energy) spectral holes. When the radio has identified a suitable spectral hole, it ‘jumps’ into the frequency band and establishes communications, while continuing to monitor other signals in the same band. When it senses that the primary user is occupying the band again, it should inform its peers and cease transmission.

II-3.1 Spectral sensing

Sensing the spectrum is the key challenge for cognitive radios. The objective is to determine whether or not a given bandwidth is occupied, but this is complicated by the effects of propagation, in particular shadowing and multipath fading. Furthermore, the decision must be made quickly, to enable sufficient frequency agility to exploit short spectral vacancies. The time taken to sense the spectrum and determine the location of usable holes also has an impact on the delay in link establishment.

There are different signal processing approaches depending on the *a priori* knowledge about the primary user, but the basic method is the same: measure the observed signal, $y(t)$, estimate a metric, γ, and assess whether this is below some predetermined threshold, γ_t. This is formulated as a hypothesis test:

$\mathcal{H}_0$:	$y(t) = n(t)$	no signal
$\mathcal{H}_1$:	$y(t) = s(t) + n(t)$	signal present

The null hypothesis $\mathcal{H}_0$ is rejected if $\gamma > \gamma_t$, i.e., if the measured metric exceeds the threshold. This is a statistical procedure: there is some probability α that $\mathcal{H}_0$ is falsely rejected (*type I error*) as well as a probability β that $\mathcal{H}_0$ is falsely accepted (*type II error*). It is generally more important not to falsely accept $\mathcal{H}_0$, as that would result in unacceptable interference, however, selecting a small value of β will make finding a usable spectrum hole more difficult.

With no knowledge of the PU's signal, the simplest sensing method is the energy detector, which just estimates the amount of energy within the bandwidth of interest. If the band is a legacy allocation to an analog TV band, for example, the signal features such as modulation format, pulse shape, etc., may be used for matched filter detection. Many transmitted signals exhibit cyclostationarity, i.e., they have periodic mean and autocorrelation signatures, which may be exploited in the detection method if the sensor can observe over a sufficiently long time, and can support the computational complexity required. For a given probability model (α, β), the simple, noncoherent method requires a measurement sample whose length is inversely proportional to the squared SNR, i.e., $N \sim O(1/SNR^2)$, while the coherent matched filter method requires $N \sim O(1/SNR)$ [12].

Theoretical models of spectrum sensing techniques generally assume that the receiver noise is Gaussian distributed with known noise. In practice, there is some degree of uncertainty about the noise variance and its distribution is likely only approximately Gaussian. It was shown in [12] that this uncertainty introduces a threshold below which the energy detector cannot detect the presence of a signal. For noise lying in the range $[\sigma_n^2, \kappa \cdot \sigma_n^2]$, the signal cannot be detected by the mean energy alone if the SNR is less than $\kappa - 1$. Furthermore, when quantisation is taken into account, [12] shows that the noise uncertainty creates an absolute limit on detectability for any detector method.

In addition to jumping *into* spectrum holes when they are available, the cognitive radio must detect when the primary user begins to use its allocated frequency, and must jump *out of* those bands. This requires that the CR sense while transmitting. This may be possible if technological advances provide the capability to measure the EM environment with sufficient accuracy by cancelling the transmitted signal at the antenna; in practice, periodic interruptions to the transmission are necessary to monitor the external signal levels. The combined length of the interruptions must be enough to provide an accurate determination within the maximum allowable window. A single, long interruption is undesirable as there is the potential for another device to detect the unused spectrum and begin to transmit.

A single cognitive radio sensing spectral use is exposed to the risk of what is called the "hidden node problem". This occurs when the CR is shadowed from the PU whose signal it is trying to sense, and therefore may incorrectly identify the spectrum as vacant. This can be avoided to some degree if there is additional knowledge about other spectral occupants operating near the PU of interest, because the shadowing that causes the hidden node problem is not frequency selective. Thus, lower than expected energy from other transmitters may be an indicator of this situation.

Cooperative sensing, in which multiple cognitive radio nodes sense the spectrum and share information, is one way to solve the hidden node problem. This is a 'diversity' approach, where it can generally be assumed that only a small portion of the CR nodes will suffer shadowing from a given PU simultaneously.

When the individual CRs do not have directional antennas, the multiple nodes may be able to operate as a 'virtual array' to provide the direction, or even location, of the primary transmitter. Sharing of the spectral characteristics also facilitates cooperative spectrum access, which will be discussed below.

A more problematic challenge is that interference from the CR at the primary receivers must be avoided, and the locations of those receivers may be completely unknown. For example, in the TV bands, the CR must not interfere with television sets, which may be anywhere within the coverage area of the transmitter; this was illustrated in Fig. 3(a). As the CR cannot know the interference environment of those receivers, they cannot guarantee that the additional interference they cause will not be detrimental. The FCC proposed an "interference temperature" approach to this problem, which placed a limit on the total additional interference that could be introduced by any operating devices to protect a minimum service range of the primary transmitter. This approach has been deemed unworkable, and the proposal was withdrawn by the FCC in May 2007. This leaves the "gray space" operation of cognitive radios in question.

II-3.2 Multiple cognitive radios

As noted in the introduction, the main consideration for using cognitive radios is in a networked environment. In this case, there are potentially many CRs searching for available spectrum at the same time, and some method must be devised to ensure that as high a proportion as possible are able to access spectrum for their respective needs.

There are two approaches to sharing the spectrum amongst many users. The first is cooperative, in which the nodes share their requirements and come to a common decision about the spectrum access, transmit power, etc. The alternative is a competitive approach, where each pair of nodes makes independent decisions.

II-3.2.1 Cooperative spectrum access

As noted above, individual nodes are prone to the "hidden node" problem whereby they are shadowed from a transmitter, for example by a building or hill. An improved picture of the spectrum can be obtained using multiple nodes, where it is assumed that one or more of the nodes is not shadowed, and therefore no primary user would be hidden from all CRs. The diversity provided by the cooperative sensing also provides the potential for shorter observation periods if the nodes are able to make independent observations. In the most challenging environments, urban and complex terrain, this is a reasonable assumption for the same reasons that MIMO systems are able to provide capacity gains: signal observations are generally uncorrelated at distances separated by a few wavelengths. The disadvantage of cooperation is in the amount of information (overhead) that must be passed around the network to arrive at, and communicate, a decision on spectrum access.

CORVUS (COgnitive Radio for usage of Virtual Unlicensed Spectrum) is a system conceived by researchers at UC Berkeley and TU Berlin [13] in which underlay control channels (see Sec. II-3.3 are formed among the nodes in the peer group. In that proposal, a universal control channel would be used by all networks to share access and other information. For military applications, such a common control channel would not be feasible due to the vast range of different users (belonging to civilian and government services, as well as coalition and unfriendly forces), radios and network structures.

While it would be expected that cooperative spectrum sensing would be more robust than single-node sensing, in fact it is a complex problem that may not lead to an optimal solution. In the formulation for distributed detection decision-making in [14], the ith CR quantises its observation, $y_i(t)$, and submits the result, $u_i(t)$, to a fusion centre which makes a decision (Fig. 6). For the networked CR case, the next step would be to assign appropriate segments of the spectrum to different nodes, and to inform them of those decisions. The quality of the decision must be traded-off with the amount of information transferred (the level of quantisation) from each node and the computation required to arrive at the decision. The decision itself is limited by the quality of the information used to reach it: the impact of untrustworthy information from individual CRs was investigated in [15].

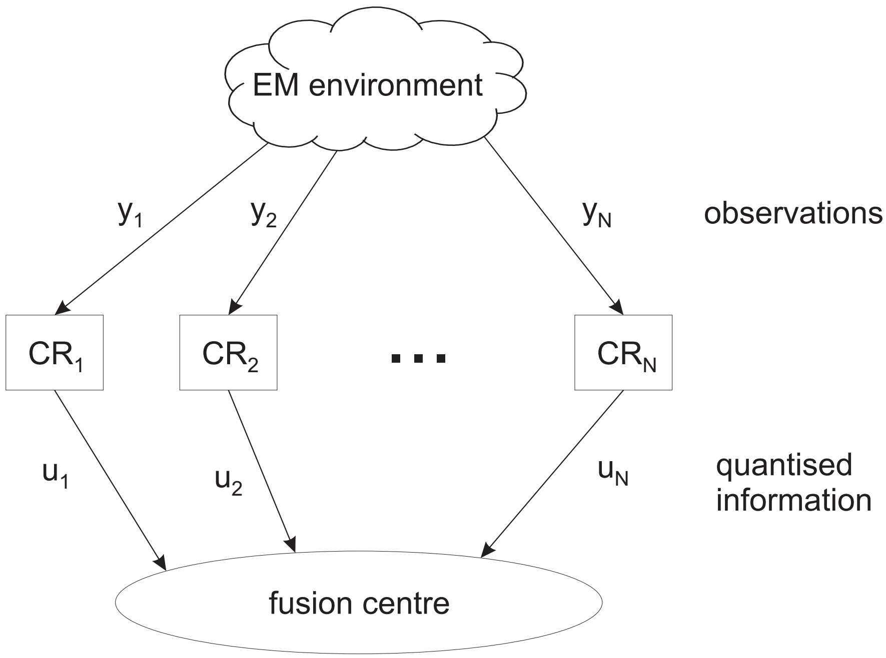


Figure 6: **Distributed detection decision-making [14]**

II-3.2.2 Noncooperative spectrum access

As indicated above, the cooperative approach to dynamic spectrum access requires a significant overhead in information sharing, which reduces overall spectral efficiency and increases link establishment delays. This overhead can be avoided if the individual pairs of nodes operate completely opportunistically, ignoring the needs of other CRs, or if the nodes adapt their operating parameters taking into account their observations of the behaviour of the other CRs. This is typically modelled and analysed using game theoretic concepts, see for example [16]–[19], [1, Ch. 15].

The normal game theory framework consists of N players, where the nth player, $n = 1, \ldots, N$ selects an action A_n, with the selfish objective of maximising its own utility function, u_n. The 'playing' of the game consists of several rounds in which the combined action set of the previous round forms part of the set of observations on which each player bases its updated decisions. The outcome is thus a result of all the actions taken. The game theory analysis should determine the steady state achieved by the adaptations of the CRs, if any, as well as to identify the restrictions on the decisions made by each CR in order to achieve the steady state.

Although there has been quite a lot of attention paid to normal game theory for the analysis of cognitive radio networks, it has some significant limitations: in particular, it assumes that the nodes have perfect state knowledge and does not model learning behaviour. This results in unnecessarily long delays in reaching a steady state, as the entire adaptation process must repeated each time the game is played. An alternative is Bayesian game theory which introduces a degree of randomness to account for imperfect information, and allows for learning as each player updates the probability distributions it uses to describe the characteristics of other players.

II-3.2.3 Practical considerations

The cooperative and non-cooperative spectrum access strategies discussed above rely on simultaneous observations and decisions. In practice, it is likely that pairs of nodes wish to set up links at different times, and nodes may join or leave the network due to changing requirements and mobility. It seems likely that an opportunistic approach to establishing links would often be more effective in terms of delay as well as in reduced overhead for information sharing.

An additional complication in the application of dynamic spectrum techniques will be other cognitive radios. Their behaviour is, by definition, unpredictable to other users as they 'jump' into and out of spectral bands, and vary their spectral occupancy, waveform characteristics and power.

The development of spectral sensing techniques to-date has emphasised the non-interference with primary users. In a world with cognitive radios, it may be difficult to distinguish between authorised users of the spectrum and opportunistic users. Certainly this distinction is important: while a CR should give way to a primary user, it need not to a secondary one.

The very existence of cognitive radios, even at a low cognition level (see Table 2), will necessitate the advancement of cognitive technologies to deal with their own kind.

II-3.3 Over/underlay techniques

The ideal operation for a cognitive radio is to identify spectrum holes, Fig. 7(a), and 'jump' to those frequency bands to transmit with the appropriate bandwidth, as illustrated in Fig. 7(b). This is called **overlay** operation. Note that the frequency bands selected for a specific link may be non-contiguous.

As noted above, in practice, the distinction between white and gray space may not be clear. Therefore, it is essential that the cognitive radio is capable of using signalling techniques that do not degrade the performance of other undetected users. One approach to this is to **underlay** the signal, by spreading the signal energy over a wide bandwidth at very low power spectral density, Fig. 7(c). Ultra-wideband (UWB) methods provide a possible solution, but care must be taken not to raise the interference floor unacceptably, especially when many UWB signals are transmitted simultaneously in overlapping bands.

II-4 RADIO PARAMETER SELECTION

While dynamic spectrum access is the key component in achieving greater use of the available frequency bands, another important aspect is the selection of radio parameters to make effective use of the identified bands. This process has been referred to as 'reading the radio's meters' and 'turning the radio's knobs' [1, Ch. 7].

At each individual radio, 'meters' might include:

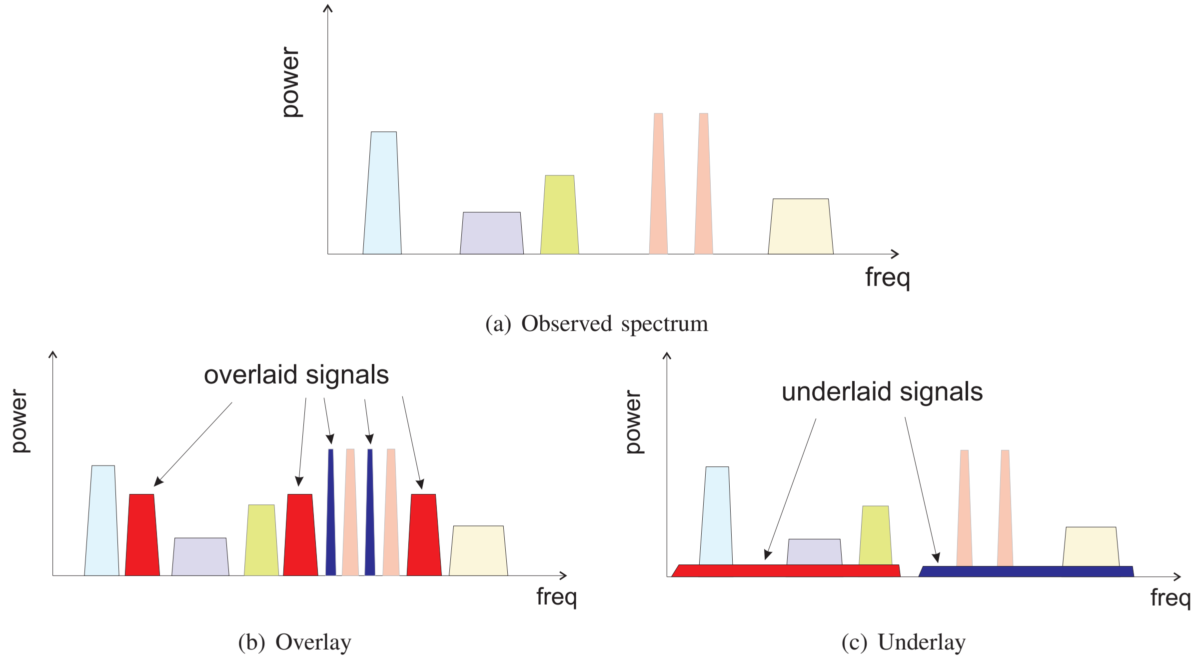


Figure 7: **Overlay and underlay techniques.**

- physical conditions, such as location and speed;
- radio parameters, such as SNR and SIR;
- radio capabilities, such as power level; and
- performance parameters such as BER, FER and packet delay.

The radio may be pre-programmed to 'know' the nature of the relationship among parameters, for example, BER is affected by speed through the effects of Doppler spread. Programmed expressions relating bit error probability for different modulations enable the radio to calculate the power required, for example, to achieve the desired QoS.

A more sophisticated approach to the problem of determining the optimal radio parameters when there are multiple objectives, such as QoS, power consumption, complexity, was proposed by researchers at Virginia Tech's Centre for Wireless Technology. In that system, the radio structure incorporates a 'cognitive engine' that observes the performance of each layer of the OSI stack and uses biologically-inspired methods to determine optimal operating parameters. They proposed using a genetic algorithm to address the multi-objective problem, taking account of BER, power and spectral efficiency while attempting to minimise spectrum occupancy, maximise data rate and avoid interference [20].

From a practical standpoint, the true relationships among observations ('meters') and associated optimal actions ('knobs') are likely to be highly complex: propagation characteristics do not match theoretical models, radio systems may be nonlinear, noise is non-Gaussian, etc. Furthermore, the optimality of the solution will be affected by the quality of the observation information obtained. It is possible that a simplified model would be more stable, or less sensitive to inaccurate information, leading to more robust behaviour. The trade-off is that the action may not have the full desired effect, and the OODA loop may require more cycles to reach a satisfactory result, wasting battery power, increasing delay and decreasing overall spectral efficiency.

II-5 COOPERATIVE COMMUNICATIONS STRATEGIES

The cognitive capability of the CRs enables them to behave cooperatively and to exploit their spatial separation as a source of diversity, even when they have only a single antenna. This can be exploited through the use of "virtual MIMO", in which relaying nodes act cooperatively to transmit the same information to a destination node. These concepts can be applied in multi-hop networks, wherein nodes receive the information in one time-slot, and retransmit it, using either an amplify-and-forward or a decode-and-forward strategy, in the next time-slot [21]. The destination then receives multiple versions of the message, and exploits the spatial and temporal diversity to improve the accuracy of detection (Fig. 8).

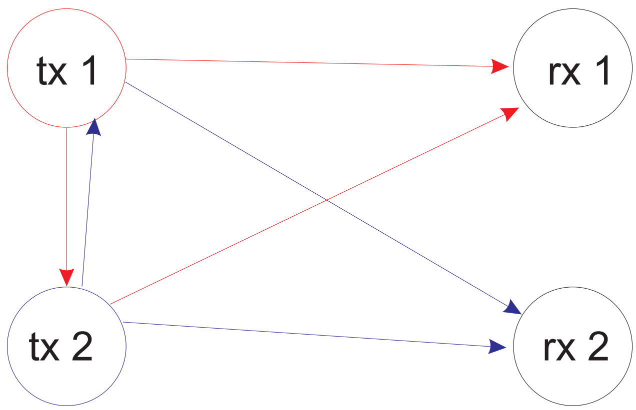


Figure 8: **Simple cooperative communications scenario**

This model can be extended to cooperative coding, in which two or more nodes transmit not only their information, but the information of their partner(s). A typical scenario [22] is that node 1 encodes its data into a codeword of length $K = K_1 + K_2$ bits, and transmits the punctured codeword in a frame of length K_1. Node 2 encodes its own data similarly, also transmitting K_1 bits. Node 1 attempts to decode node 2's data based on the punctured codeword, and, if successful, regenerates and transmits the corresponding length-K_2 codeword in the second frame. If node 1 cannot decode the first K_1 codeword from node 2, it transmits its own K_2-bit codeword in the second frame instead. Node 2 operates in a similar way. In this way, the two nodes are able to behave cooperatively, achieving a performance gain due to the added diversity, with no side information passed between them.

CRs capable of cooperative communications should be capable of assessing the benefit, in both a selfish and an altruistic sense, and the cost, in terms of required resources (power, time, spectrum, computation, etc.). For example, a node that hears a transmission intended for a destination far away may offer little diversity gain if it retransmits the message, and therefore would choose not to waste its battery power and block that frequency for any other local users. The intermediate node may also decide not to transmit if it knows there are a sufficient number of other nodes relaying the information to achieve a suitable diversity gain.

II-6 CONCLUSIONS

Software defined radios provide an unprecedented level of flexibility and adaptability for military radios. The technology is maturing as programs such as JTRS require their use for all platforms. At the same time, the potential for fully upgradeable and interoperable waveforms has not been reached, and further platform development and standardisation is required to make waveforms readily and rapidly portable from one radio to another.

The introduction of cognitive concepts into radios is intended to provide a degree of autonomy to the device, particularly with respect to frequency selection. Many investigations have demonstrated that, even though the spectrum below 3 GHz is fully assigned, it is largely unused. The development of technologies that support the dynamic use of this un- or under-used spectrum is important for military communications, in particular to support the high throughput demands of net-enabled communications.

Cognitive radios are conceived to be aware, adaptive and intelligent, identifying suitable frequency bands for operation and having the agility to jump quickly to those bands, while monitoring for the appearance of the authorised user. This adaptability requires the reasoning capability to select suitable radio parameters, including power, bandwidth, modulation and coding.

For networked operations, the challenges of dynamic frequency access include sharing the necessary information and making the appropriate decisions without overloading the system with overhead messages.

The original vision of a cognitive radio was a 'personal assistant device' which would be capable, for example, of determining which network to join based on the device's perception of the operator's requirements, of learning the operator's behavioural patterns and demands, and of gathering information expected to be of use to the operator. These CRs would autonomously share information and negotiate with other devices to provide seamless connectivity everywhere.

This vision is not consistent with military applications of cognitive radio technology. The required radio behaviour is different, *a priori* knowledge of other systems and the capability to share knowledge among primary and secondary users may be non-existent, and co-operative strategies are threatened by malicious users. The development of policies for connectivity and networking must include consideration of the vulnerabilities of these devices, for example to mitigate spoofing and enforce a trust mechanism.

The current state-of-the-art of cognitive radio technology for military applications is associated with the DARPA XG program. To date, there has been a proof-of-concept demonstration on a small scale. The operation of cognitive radios in a world of authorised, or primary, users is gaining acceptance, although there are still regulatory hurdles to overcome. Some significant civilian programs underway include:

- IEEE 802.22 WRAN system, making use of unused TV channels;
- IEEE 802.11h which supports dynamic frequency selections to enable WLANs to share spectrum;
- IEEE 802.15.3a which incorporates spectrum 'sculpting' using OFDM over wide bandwidths;
- IEEE Project 1900, developing standards supporting new technologies and spectrum management techniques.

Future challenges include the development of suitable policy-based approaches to reasoning, in particular to dynamic spectrum access. Different policies would likely apply in different operational scenarios and for different primary users, e.g., opportunistic devices may yield to public emergency services but not to civilian commercial systems. When competition for spectrum comes from other opportunistic devices, it may not be desirable to yield to their attempts to access the spectrum. In fact, it may be preferable under some conditions to continue to occupy the spectrum to maintain access to the frequency band.

As the number of adaptive and cognitive radios in use increases, the need for higher levels of cognition increases as the devices now have to address the unpredictable dynamic behaviour of other systems.

Abbreviations and acronyms

CR	cognitive radio
CORVUS	COgnitive Radio for Virtual Unlicensed Spectrum
DARPA	US DoD Defense Advanced Research Projects Agency
DoD	US Department of Defense
FCC	US Federal Communications Commission
ITU	International Telecommunications Union
JTRS	US DoD joint tactical radio system
MIMO	multiple-input, multiple-output
NCW	net-centric warfare
NEOps	net-enabled operations
OODA	Observe, Orient, Decide, Act
PU	primary user
QoS	quality of service
SCA	software communications architecture
SDR	software-defined radio
SDRF	SDR Forum
SIR	signal-to-interference ratio
SNR	signal-to-noise ratio
SU	secondary user
WLAN	wireless local area network
WRAN	wireless regional area network
XG	DARPA's neXt Generation program

References

[1] B. A. Fette, ed., *Cognitive Radio Technology*. Oxford, UK: Elsevier, 2006.

[2] Software Defined Radio Forum. Available at: `http://www.sdrforum.org`.

[3] Communications Research Centre Canada, "SCARI-OPEN: open source reference implementation of SCA." Available at: `http://www.crc.ca/en/html/crc/home/research/satcom/rars/sdr/sdr`.

[4] L. Pucker, "Maximizing waveform portability in a radio architecture through a common hardware abstraction layer model," *IEEE Commun. Mag.*, pp. 28–29, Mar. 2006.

[5] R. J. Lackey and D. W. Upmal, "Speakeasy: The military software radio," *IEEE Commun. Mag.*, pp. 56–61, May 1995.

[6] P. G. Cook and W. Bonser, "Architectural overview of the SPEAKeasy system," *IEEE J. Select. Areas Commun.*, vol. 17, pp. 650–661, Apr. 1999.

[7] Joint Tactical radio System. Available at: `http://enterprise.spawar.navy.mil/body.cfm?type=c&category=27&subcat=60`.

[8] J. Mitola, *Cognitive Radio: An Integrated Agent Architecture for Software Defined Radio*. PhD thesis, Royal Institute of Technology (KTH), Sweden, 2000.

[9] "Notes on John Boyd's military strategy." Available at: "`http://www.d-n-i.net/second_level/boyd_military.htm`".

[10] M. McHenry, E. Livsics, T. Nguyen, and N. Majumdar, "XG dynamic spectrum access field test results," *IEEE Commun. Mag.*, vol. 45, no. 6, pp. 51–57, 2007.

[11] P. Marshall and T. Martin, "XG Communications Program – overview." Available at `http://www.darpa.mil/sto/solicitations/WAND/pdf/XG_overview_for_WAND.pdf`.

[12] A. Sahai, N. Hoven, and R. Tandra, "Some fundamental limits on cognitive radio," in *Proc. Allerton Conference on Communication, Control, and Computing*, Oct. 2004.

[13] D. Cabric, S. M. Mishra, D. Willkomm, R. W. Broderson, and A. Wolisz, "A cognitive radio approach for usage of virtual unlicensed spectrum," in *Proc. 14th IST Mobile Wireless Communications Summit*, (Germany), June 2005.

[14] J. Tsitsiklis and M. Athans, "On the complexity of decentralized decision making and detection problems," *IEEE Trans. Automat. Contr.*, vol. 30, pp. 440–446, May 1985.

[15] S. M. Mishra, A. Sahai, and R. W. Brodersen, "Cooperative sensing among cognitive radios," in *Proc. ICC '06, Int. Conf. Commun.*, vol. 4, pp. 1658–1663, June 2006.

[16] J. Neel, J. Reed, and R. Gilles, "Game models for cognitive radio algorithm analysis," in *SDR Forum Tech. Conf.*, Nov. 2004.

[17] S. Haykin, "Cognitive radio: Brain-empowered wireless communications," *IEEE J. Select. Areas Commun.*, vol. 23, pp. 201–220, Feb. 2005.

[18] N. Nie and C. Comaniciu, "Adaptive channel allocation spectrum etiquette for cognitive radio networks," in *DySPAN 2005*, pp. 269–278, Nov. 2005.

[19] Z. Li and K. J. R. Liu, "Dynamic spectrum sharing: A game theoretical overiview," *IEEE Commun. Mag.*, vol. 45, pp. 88–94, May 2007.

[20] T. W. Rondeau, C. Rieser, B. Le, and C. W. Bostian, "Cognitive radios with genetic algorithms: Intelligent control of software defined radios," in *SDR Forum Technical Conference*, (Phoenix, AZ), pp. C–3 – C–8, 2004.

[21] J. N. Laneman, D. N. C. Tse, and G. W. Wornell, "Cooperative diversity in wireless networks: Efficient protocols and outage behavior," *IEEE Trans. Inform. Theory*, vol. 50, pp. 3062–3080, Dec. 2004.

[22] A. Nosratinia, T. E. Hunter, and A. Hedayat, "Cooperative communication in wireless networks," *IEEE Commun. Mag.*, vol. 42, pp. 74–80, Oct. 2004.