Using Cognitive Radio for Interference-Resistant Industrial Wireless Sensor Networks: An Overview

Tapiwa M. Chiwewe, *Member, IEEE,* Colman F. Mbuya, Gerhard P. Hancke, *Senior Member, IEEE*

***Abstract*—Industrial wireless sensor networks have to contend with environments that are usually harsh and time varying. Industrial wireless technology, such as WirelessHART and ISA 100.11a, also operates in a frequency spectrum utilised by many other wireless technologies, and with wireless applications rapidly growing it is possible that multiple heterogeneous wireless systems would need to operate in overlapping spatiotemporal regions. Interference such as noise or other wireless devices affects connectivity and reduces communication link quality. This negatively affects reliability and latency, which are core requirements of industrial communication. Building wireless networks that are resistant to noise in industrial environments and can coexist with competing wireless devices in an increasingly crowded frequency spectrum is challenging. To meet these challenges, we need to consider the benefits that approaches finding success in other application areas can offer industrial communication. Cognitive radio methods offer a potential solution to improve resistance of industrial wireless sensor networks to interference. Integrating cognitive radio principles into the lower layers of industrial wireless sensor networks can enable devices to detect and avoid interference and potentially opens the possibility of utilising free radio spectrum for additional communication channels. This improves resistance to noise and increases redundancy in terms of channels per network node or adding additional nodes. In this paper, we summarise cognitive radio methods relevant to industrial applications, covering cognitive radio architecture, spectrum access and interference management, spectrum sensing, dynamic spectrum access, game theory and cognitive radio network security.**

***Index Terms*—Cognitive radio, industrial wireless sensor networks, Internet of Things, spectrum management, spectrum sensing.**

I. INTRODUCTION

WIRELESS technologies have been named as an appealing alternative for distributed control systems, automotive systems, industrial and factory automation, and other interconnected embedded systems [1], [2], [3]. They offer several advantages over traditional wired communication systems such as enhanced physical mobility, fewer infrastructure requirements, less risk of cable damage, reduced connector trouble and simplicity of upgrading [4], [5]. It has been established that industrial and factory environments pose significant challenges for wireless communications. Industrial applications set high requirements for reliability while these applications also operate in environments that are arguably more prone to interference [1], [6]. Coexistence is also an increasingly important aspect when implementing Industrial Wireless Sensor Networks (IWSNs). With industrial applications no longer confined to controlled factory environments and extending to applications such as building automation, smart grids and consumer utility use monitoring and control, these networks must be tolerant to coexisting with other industrial and consumer wireless systems. Any candidate radio system must maintain the required quality-of-service (QoS) in a coexisting environment and favourable transmission quality when functioning as a standalone system [7]. As the use of wireless networks continues to increase with growing consumer interests and with initiatives like the Internet-of-Things, radio spectrum is becoming a scarce commodity and practitioners will need to consider new approaches to coexistence and the utilisation of temporarily free bands.

The regulation of radio spectrum today is based on a fixed spectrum assignment policy, where government agencies regulate spectrum usage and assign portions of the spectrum over extended periods of time and large geographic areas to license holders or services such as mobile cellular communication or terrestrial television. Large portions of the allocated spectrum are utilised intermittently and spectrum use is congested at particular regions of the spectrum space, while a considerable part of it is left underutilised. Usage of assigned spectrum in time and space varies from 15% to 85% [8]. The inefficient use and scarcity of spectrum has demanded a new paradigm in wireless communication where the available wireless spectrum is exploited opportunistically. In such a paradigm, reliable communication is provided wherever and whenever needed, and radio spectrum is used more efficiently [9].

Cognitive Radio (CR) technology is a communication paradigm that has emerged in recent years that can mitigate interference and enhance reliability in a heavily congested wireless industrial network. A formal definition of a cognitive radio is: *"Cognitive radio: A radio or system that senses its operational electromagnetic environment and can*

Manuscript received April 26, 2013; revised February 03, 2014, September 30, 2014, March 09, 2015 and July 16, 2015; accepted September 20, 2015. This work was supported by the Centre for Telecommunications Engineering for the Information Society (CeTEIS), South Africa. Paper no. TII-13-0799.

T. M. Chiwewe is with the University of Pretoria, Pretoria 0001, South Africa, and also with the Council for Scientific and Industrial Research (CSIR), Pretoria 0001, South Africa (e-mail: tapiwa.chiwewe@ieee.org).

C. F. Mbuya is with the University of Pretoria, Pretoria 001, South Africa, and also with MWR InfoSecurity, Johannesburg 2000, South Africa (e-mail: colman.mbuya@mwrinfosecurity.com).

G. P. Hancke is with the University of Pretoria, Pretoria 0001, South Africa, and also with the City University of Hong Kong, Kowloon, Hong Kong (e-mail: ghancke@ieee.org).

TABLE I
WIRELESS INDUSTRIAL STANDARDS

	IWLAN	ZigBee	WirelessHART	ISA 100.11a	WISA
Bandwidth	22 MHz	2 MHz	2 MHz	2 MHz	1 MHz
Channels, Selection	14, static	16, static	15, dynamic	15, dynamic	77, dynamic
Data Rate	11-54 Mbps	250 kbps	250 kbps	250 kbps	1 Mbps
Frequency Band(s)	2.4 GHz, 5 GHz	2.4 GHz	2.4 GHz	2.4 GHz	2.4 GHz
MAC Layer	IEEE 802.11	IEEE 802.15.4	Proprietary	Proprietary	Proprietary
Radio	IEEE 802.11b/g/a	IEEE 802.15.4	IEEE 802.15.4	IEEE 802.15.4	IEEE 802.15.1
Topology	Star	Star, Full-Mesh	Full-Mesh	Star, Star-Mesh, Full Mesh	Cellular, Star

dynamically and autonomously adjust its radio operating parameters to modify system operation, such as maximize throughput, mitigate interference, facilitate interoperability, access secondary markets." [10]. Long established methods of sharing spectrum assume that network nodes collaborate categorically in an unchanging environment [11]. In Cognitive Radio Networks (CRNs) though, interactions with other users and the dynamic environment must be taken into account to adapt the operational configuration.

CRs are not limited to a set of channels as in frequency-agile approaches, but are more general and can operate in different frequency bands. Through an intelligent decision making process that considers sensed spectrum variations and actions chosen by other users in the network, the tight requirements for reliable and real-time communication in industrial networks can be met. This will help to avoid a loss of time and money or physical damage. There are several existing approaches to avoid interference in these networks, some already heading in a CR direction when sensing congestion and switching to alternative channels. CR still offers the opportunity not only to ensure media access in heavily congested areas but also to extend the lower layers of existing IWSN protocol stacks to find additional bandwidth for additional channels or high-bandwidth communication.

In this paper, we initiate a discussion of benefits and challenges of using CR in industrial environments, focusing on different interference sources, coexistence and existing multi-access techniques. Next, an overview of spectrum sensing techniques is given. This is followed by a presentation on dynamic spectrum management and a discussion on the use of game theory to share spectrum. Finally, we cover security issues in CRNs as an aspect that directly affects the reliability of IWSNs.

II. WIRELESS INDUSTRIAL NETWORKS

A. Interference in Wireless Industrial Networks

Industrial environments often have higher QoS requirements than typically found in homes and offices. More communication devices are involved and their number is more variable. It is necessary to meet specific safety and security requirements, and performance must be deterministic with certain degradation. Coupled with the harsh environment, this means that the spectrum resources vary over time and space. This situation may be exacerbated by device mobility and traffic fluctuations.

Multipath fading, radio interference and noise are the root causes of problems affecting the reliability of data and effective operating range in wireless communication systems. The interference affects the successful delivery of packets and the controller will have to operate with an incoherent view of a physical process [12]. Interference due to multipath fading occurs when several versions of a transmitted signal get to a receiver due to reflections off obstacles like factory floors and walls. This causes a phase variance between different copies of the signal, resulting in destructive interference and ultimately reduced signal strength, lower network throughput and reduced communication range.

When different radio signals exist in the same place, at the same time, and in a common frequency range, then Radio Frequency Interference (RFI) occurs. This is particularly a problem when using devices that operate in the Industrial, Scientific and Medical (ISM) and Unlicensed National Information Infrastructure (U-NII) bands, which are both unlicensed and used for different networks including Wireless Personal Area Networks (WPANs) and Wireless Local Area Networks (WLANs). This can be exacerbated by poor frequency planning and an overly crowded frequency spectrum. WirelessHART, ISA 100.11a, WISA (Wireless Interface for Sensors and Actuators), ZigBee, Wi-Fi and Bluetooth devices operate in the 2.4 GHz ISM band, as do other devices such as welding equipment, radio frequency lighting, microwave ovens and cordless phones. Industrial WLAN (IWLAN) expands the function of IEEE 802.11 based consumer Wi-Fi to achieve performance improvements such as greater reliability, enhanced roaming, longer communication range and deterministic operation. Table I gives a comparison of different industrial wireless platforms that need to coexist [13], [14] and [15].

While one cause of RFI is co-channel interference (CCI) where two or more radio transmitters use the same frequency, another cause is electromagnetic radiation from other unforeseen sources. Whatever the cause, the operation of sensitive communication equipment is disturbed [16].

Interference signals can be classified as broadband or narrowband. Narrowband interference is predominantly caused by intentional transmissions, whereas broadband interference is usually from incidental radio frequency emitters [17]. Broadband sources have a relatively flat power spectral density across a wide range of frequencies whereas narrowband signals are modelled as a continuous wave at a specific frequency. Broadband interference can come from arc/vapor lamps, computers, electrostatic discharge, electric switch contacts, ignition systems, inverters, motors, pulse generators, thermostats and voltage regulators. Narrowband interference can be caused by cellular telephones, electronic ballasts, local oscillators, microwave and ultrasonic equipment, pager transmitters, power-line hum, and radio and television transmitters [18], and so on etc. Fig. 1 shows different interference sources found in industrial environments.

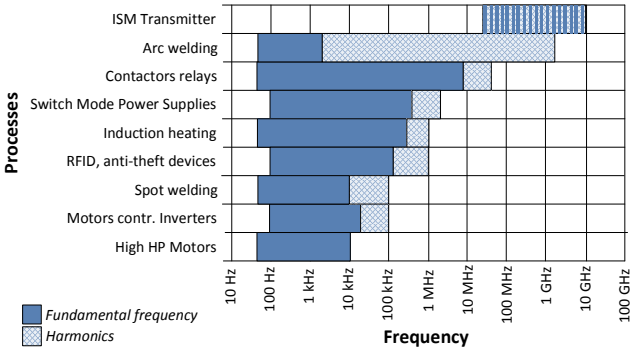

Fig. 1. Frequency of different processes and devices in industry [19].

B. Interference Management using Traditional Techniques

Most traditional schemes to manage interference make use of multiple access techniques classified as deterministic or random. Multiple access techniques isolate stacks of radio resources allocated to multiple users within radio range of each other such that each user communicates using an exclusive set of radio resources at any time. Other interference management techniques include spread spectrum, diversity, power control and MIMO.

1) Deterministic Assignment Multiple Access

Deterministic multiple access schemes are contention-free and seek to avoid collisions by allotting radio resources which include code, channel and time slot to several radios from a central entity [20]. It is possible to use contention free schemes in time, frequency, code and space division multiple access networks.

- In *Time Division Multiple Access* (TDMA), access to a frequency band is scheduled in time. When the time comes for a user to send or receive data, all other users are kept inactive during the allotted timeslot. In TDMA it is necessary for all nodes to be synchronised to avoid interference [21].
- Another multiple-access scheme for wireless systems is *Frequency Division Multiple Access* (FDMA). In this technique, a frequency band is split into several channels and each channel is allocated to a single user. Any communication signals sent or received by the user do not cause interference to other users' transmissions. Orthogonal Frequency-Division Multiple Access (OFDMA) is a multi-user adaptation of the widely used Orthogonal Frequency-Division Multiplexing (OFDM) digital modulation scheme. OFDMA achieves multiple access by dynamically assigning a subset of subcarriers to single users.
- A more advanced digital technique is *Code Division Multiple Access* (CDMA). This is a common part of third and fourth generation wireless communication systems. CDMA enables several users to be multiplexed over a common physical channel through using a unique coding scheme where each transmitter is assigned a code and spread-spectrum technology [22], [23].
- *Spatial Division Multiple Access* (SDMA) makes use of information gathered in the spatial dimension and the temporal dimension to attain meaningful advancement transmitting wireless information. Significant increases in capacity, coverage and quality of wireless systems is attainable through spatially selective transmission and reception of RF energy. Spatial multiplexing and diversity is achieved by using technologies such as antenna arrays and multi-dimensional non-linear signal processing.

2) Random Multiple Access

In contention-based random channel access schemes, nodes contest one another to send data using the shared wireless channel. If no collision arises a sent packet is then received successfully. A collision occurs when several nodes send data at the same time such that the signal-to-interference-plus-noise ratio (SINR) at the receiver is below the SINR floor necessary to decode the sent packet without error. In the event of a collision, it is possible for a node to try to resend the packet. The particular method chosen to retransmit the packet is decided by the protocol in use. Some popular contention-based channel access schemes follow below [24].

- ALOHA: In this scheme, nodes transmit packets immediately when they have some to send. In the event of a collision, the packet is retransmitted later. ALOHA functions by dividing time into slots, and packets are sent aligned to the time slots.
- Carrier Sense Multiple Access (CSMA): This is a probabilistic channel access scheme where a node senses the state of the channel prior to attempting transmission. The node initiates a transmission attempt if the channel is idle. Should a collision occur, the node waits for a packet transmission interval before transmitting the packet again. Two enhanced variations of CSMA are CSMA with collision detection (CSMA/CD) and CSMA with collision avoidance (CSMA/CA). CSMA/CD is not workable in wireless networks. In CSMA/CA, should the channel be sensed as busy before transmission, transmission is delayed for a random amount of time to decrease the probability of collisions.

3) Spread Spectrum Techniques

Two used spread spectrum techniques are *Direct Sequence Spread Spectrum* (DSSS) and *Frequency Hopping Spread Spectrum* (FHSS). DSSS can address a crowded spectrum but is far from sufficient [25]. Should the power of the interfering signal fall within the jamming margin then DSSS can remove interference completely. FHSS gives reduced likelihoods of colliding with other transmissions. DSSS is preferred for low to medium narrowband interference whereas FHSS is preferred for heavy interference environments and applications with elevated bandwidth requirements involving a great deal of data. Similar to spread spectrum, *Ultra Wide Band* (UWB) communications transmit in a way as not to interfere with using traditional narrowband and carrier waves in the same frequency band.

4) Diversity Schemes, Power Control and MIMO

Besides the techniques covered above, different diversity schemes such as path diversity, channel diversity, temporal diversity, and transmit power control (TPC) may also manage interference and consequently improve link quality and reliability. Likewise, multiple-input multiple-output (MIMO), where multiple antennas are used at the transmitter and receiver, may be adopted. For multi-user MIMO, SDMA techniques can be employed.

5) Multiple Access Techniques in Wireless Industrial Platforms

The multiple access techniques of typical wireless industrial platforms are constructed by combining the previously discussed techniques.

- WISA utilises TDMA and Frequency Division Duplex (FDD), where the uplink channel used is different to the downlink channel. The TDMA scheme is managed by the base station of each cell. Additionally a frequency hopping scheme is used to further assist in avoiding interference.
- WirelessHART uses a TDMA scheme with timeslots of 10 ms. A time slot can be allocated to an individual device or multiple devices where a CSMA/CA mechanism is used. Frequency hopping is also applied and the channel to be used is indicated by a network manager which also allocates time slots to devices.
- ISA 100.11a also uses a TDMA scheme where timeslots are configured according to a slotted channel-hopping pattern or a slow channel-hopping pattern. The network manager manages the TDMA scheme.
- ZigBee has two communication modes namely beaconed and non-beaconed mode. In beaconed mode, a superframe slotted structure comprising two parts is used. The first part of the frame is for general use where CSMA/CA is used for access. The second part of the frame comprises slots dedicated to specific nodes in the network. In non-beaconed mode, an unslotted CSMA/CA based multiple access scheme is used.

III. COGNITIVE RADIO

In section II.A different sources of interference in wireless industrial networks were identified. As was highlighted, many industrial wireless platforms such as IWLAN, WirelessHART, ISA 100.11a and WISA operate in the unlicensed ISM bands. Using unlicensed bands however, results in challenges such as mutual interference between dissimilar coexisting radio systems and spectrum scarcity. This interference can cause the SINR at receivers to fall below the required threshold to communicate successfully. Traditional interference mitigation schemes highlighted in section II.B do not address these challenges of mutual interference and spectrum scarcity.

One solution is to use licensed spectrum regulated by bodies such as the Federal Communications Commission (FCC), which is a long and costly process. Another option is to use the unlicensed 5 GHz band, which has the advantage of being less crowded, though it is susceptible to the same problems as the 2.4 GHz band [1].

Using CRs is another solution that does not suffer from the shortcomings of the ones above. CRs have features such as spectrum sensing and reconfigurability that can adequately solve the challenges identified. The coexistence of co-located dissimilar wireless networks that must provide QoS guarantees can benefit from using CRs.

A. Cognitive Radio Fundamentals

CRs are borne out of a software radio, which is a transceiver whose communication functions are realised as programs running on a suitable processor. It comprises all the layers of a communication system, from the physical layer to the application layer [26]. A software-defined radio (SDR) is a practical implementation of a software radio in which received signals are sampled after a suitable band selection filter instead of directly sampling antenna output. If in addition, a SDR can sense its environment, track changes, and react upon its findings, then it is referred to as a CR. CRNs can provide high bandwidth wireless communication to users through dynamic spectrum access (DSA) techniques and heterogeneous architectures.

In CR terminology, *primary users* (PUs), also known as *incumbent users,* are licensed users with legacy rights or higher priority to utilise a particular part of the spectrum. *Secondary users* (SUs), also referred to as *cognitive users*, are unlicensed users with a lower priority, and exploit the spectrum opportunistically such that PUs do not suffer harmful interference from them. SUs as a result must possess CR capacity, such as dynamic spectrum access techniques, that will allow them to function in the most favourable channel. Only users with a tangible legal or regulatory right to spectrum are considered PUs. In unlicensed bands, e.g. in ISM frequency bands where most of the industrial wireless network technology operates, there are no PUs. Despite the perceived importance of some applications, SUs compete equally for the same resource.

A CRN can be multiband, multichannel, multiservice and multi-standard [26]. CR shall give SUs the ability to (1) detect licensed PUs and evaluate which parts of the wireless spectrum are available for use (spectrum sensing), (2) select the best available spectrum channel (spectrum decision), (3) coordinate access to this channel with other SUs (spectrum sharing) and (4) vacate the channel when a licensed user is detected (spectrum mobility) [27]. The dynamic spectrum access operation where CRs use temporarily unused spectrum, also known as white space or a spectrum hole, is illustrated in Fig. 2.

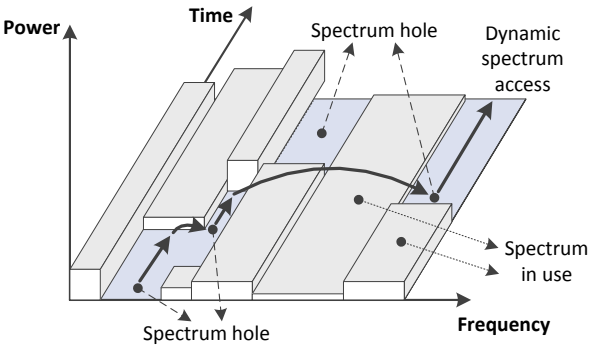

Fig. 2. Spectrum hole concept [27].

The two main characteristics of a CR are its *cognitive capability* and *reconfigurability* [28].

- **Cognitive capability**: This enables the platform to determine the current occupancy of the spectrum. Information on spectrum utilisation should be available on an ongoing basis and updated on the platforms spectrum allocation module in order for the transmission parameters to be set. Spectrum sensing approaches can be of two types, wideband and narrowband. The accuracy of spectrum access decisions when using wideband sensing is negatively affected by delays in getting spectrum utilisation information. Narrowband sensing, however, investigates a small portion of the spectrum and as a result, spectrum access

opportunities can be missed. Nonetheless, the fast response time of narrowband sensing can more accurately track the dynamic nature of spectrum utilisation.

- **Reconfigurability**: This enables the configuration of the transceiver's operating parameters to be changed in real time without modifying the hardware components that affect the radio transmission. Configured transceiver parameters include the operating frequency, modulation type, error control scheme and transmission power. Using MIMO antennas can produce significant increases in spectral efficiently and gives rise to a cognitive MIMO radio that offers the ultimate in flexibility with four degrees of freedom: carrier frequency, channel bandwidth, transmit power and multiplexing gain [9] .

To provide the above capabilities a new structure for the radio frequency (RF) transceiver is required. The most important parts are shown in Fig. 3. These include the baseband processing unit and the radio front end, that in the beginning were proposed for SDRs [8]. The RF front-end amplifies, mixes, and performs analog-to-digital (A/D) conversion on the received signal, while the baseband processing unit modulates and demodulates the signal. To accommodate the dynamic RF environment, a control bus can be used to re-configure each constituent part. A unique feature of the CR transceiver is that it has a wideband RF front-end that can sense over a wide range of frequencies simultaneously [29]. The RF hardware should be adjusted to operate anywhere in a large spectrum range and this is leveraged by hardware technologies which include an adaptive filter, a power amplifier and a wideband antenna.

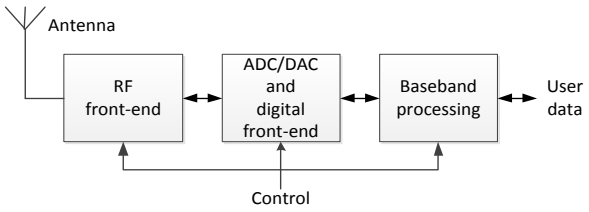

Fig. 3. Cognitive radio transceiver architecture [8].

There are several advantages of using CR solutions. CRs can prolong the useful service life of communication systems by allowing the possibility to change radio configurations on CR equipment that has already been placed into service. CR applications that have already been invested in can be ported to new SDR platforms that are more capable. It becomes easier to keep up with the rapid evolution of communications standards [30] as base stations and other radios can have their software upgraded.

Some challenges exist, however, concerning the CR transceiver. Receiving transmissions from several radios that operate using different bandwidths, at different power levels and in different locations means that the CR transceiver needs to sense weak signals in a large dynamic range, which is a major design problem [8].

B. Interference Management and QoS

In CRNs, interference can be avoided by taking advantage of the secondary system, being a new system, deployed within a service area of a *legacy* primary system, which can interpret signals sent in the primary system [31]. SUs are continuously exposed to signals from the PUs and techniques to avoid this interference should be employed. SUs can sense the channel just prior to transmission and periodically during transmission to maintain awareness of spectrum opportunities. It is possible for a channel that has been identified by a SU as available to suddenly become occupied by a PU during transmission, giving rise to harmful collisions and interruptions. Predictive modelling can avoid such scenarios [32]. Through careful design of CRNs, significant gains in terms of interference are attainable [33].

Each industrial application has its own set of QoS requirements. Safety data has high fail-safety and reliability demands, while closed-loop controls and machine control have high response-time demands. Data transmitted for visualisation and recording purposes requires a high data rate. Wireless networks are failure-prone but the reliability of IWSNs can be improved by using CRNs and taking advantage of their ability to provide efficient mechanisms for failure prevention and recovery and providing dependable communication and uniform QoS in varying circumstances. A study into dynamic spectrum sharing in the TV band demonstrated a system with low noise, high receiving sensitivity and anti-interference competence [34].

CRs have been used in Television White Spaces (TVWS) to solve the problem of interference between Portable Cognitive Emergency Wireless Networks (PCENs) [35]. IEEE 802.22, a Wireless Regional Area Network (WRAN) based on CR, has been analysed to determine its Transmission Control Protocol (TCP) performance, and cross-layer solutions were suggested to boost its throughput [36]. A new metric called Quality of Coexistence (QoC) [37] was proposed to characterise how well SU networks and mixed PU and SU networks coexist. Interference in multi-hop CRNs can also be controlled using routing solutions [38] and topology control [39]. A cross layer CRN framework was proposed for smart grids that mitigates the adverse effect of noisy and congested spectrum bands [40]. In [41] a practical model for cumulative interference in CRNs is developed and then used to develop a power control scheme for low interference and good secondary network QoS. Throughput aware routing has been used to address the QoS requirements in CRNs [42]. Queuing theory can analyse the impact of PUs maximum tolerable delay on SUs performance [43]. An area that has yet to be explored is that of developing a low-power industrial sensor node in the CR paradigm together with the controlling mechanisms for channel hand-off to contend with RF interference in a dynamic wireless channel [4].

C. Benefits and Limitations of Cognitive Radio Approaches in Industrial Wireless Sensor Networks

Current IWSNs typically operate within the congested unlicensed ISM frequency bands. CR can allow these networks the flexibility to operate in licensed bands as SUs. For critical communication, some co-operation with PUs will be required to ensure availability of spectrum over extended periods. This co-operation entails negotiation, spectrum management and enforcement, and is best guaranteed with standardisation, which is a core requirement of IWSNs [14].

Current CR standardisation efforts are focused on

exploiting TVWSs [44]. This is in response to new regulations by regulators worldwide that allow the use of unused TV bands in the Ultra High Frequency (UHF) and Very High Frequency (VHF) bands. These activities cover the IEEE 802.22 WRAN, the IEEE 802.11 WLAN, and the IEEE 802.15 WPAN. IEEE 802.22 [45] is a CR standard for WRANs and is arguably not yet suitable for small IWSNs, such as building automation, although applications covering large geographic areas such as those involving Smart Utility Networks (SUNs) and infrastructure monitoring could be catered for by this standard. Standardisation efforts more attractive to industrial users are IEEE 802.11af [44] and IEEE 802.15.4m [46]. IEEE 802.11af can be of benefit to industry if, for instance, IWLAN is adapted to support this standard then one attractive aspect is that technical amendments to the standard allow legacy IEEE 802.11 devices to operate legally in TVWS. IEEE 802.15.4m seeks to enable IEEE 802.15.4 wireless networks to take advantage of TVWS spectrum and this can be of great advantage to industrial standards such as WirelessHART and ISA 100.11a. Once these standardisation activities are complete, it will be possible to estimate the implementation cost and complexity, and subsequently commercial devices will become available. Ettus Research and National Instruments already offer Universal Software Radio Peripheral (USRP^{TM}) platforms that can be used for research, experimentation and prototyping of CRs.

Given ongoing regulatory and standardisation efforts to cater for legal licensed band operation of CRs, their more immediate impact might be to allow more efficient operation of IWSN in congested unlicensed space. With the increased use of consumer wireless devices and the boundaries between consumer and industrial wireless networks becoming blurred, improved coexistence is required. This can be seen, for instance, when operating building automation networks in residential buildings or for the monitoring of critical infrastructure in cities. CR technology is designed for a competitive environment, and is therefore well suited to provide coexistence and resistance to different RFI. Inherently, networks using CR technology are resistant to interference resulting in fewer communication errors. There is a lower channel access delay and a decreased number of retransmissions leading to less jitter and lower latency. There is no need to manually configure channel access for the network, as through self-organisation, network nodes decide what channels to use as their environment changes.

The exact requirements for industrial wireless communication vary across applications and from one engineer's opinion to another. These properties of CR appear to match up well with the basic IWSN requirements: redundancy, tolerance to interference [4], [5], [25], [13] timely transmission, reduced latency, reduced retransmissions, lower frame loss [5], [25], [13], and increased robustness in communication links due to changing environment, network topology or node location [4], [5], [25], [13].

CRs have higher complexity compared to traditional wireless systems and benefits of adopting them must be weighed against economic and technical consequences. IWSNs are often comprised of resource-constrained devices [4], [5]. Reduced computational resources limit the choices of CR features that can be implemented, for example, wideband spectrum sensing may not be well suited to resource-limited devices. This does not mean that CRs are unfeasible for IWSNs as the remaining options can still work well. For example, narrowband sensing with cooperation among nodes can be used instead of wideband sensing. Another alternative is to have an infrastructure-based network with a node hierarchy where devices with more resources at their disposal perform tasks which are more computationally intensive or that require special hardware capabilities. The results are then shared with less powerful devices in the network that can then, for example, change their operational characteristics such as PHY parameters based on this. One area of interest is whether devices could do spectrum sensing and channel selection in a timely manner so as to not introduce significant time delays when setting up new channels, which would negatively affect real-time communication.

CRNs are not at a stage where they offer a complete alternative to existing industrial wireless networking technology. Aspects of CR technology could be integrated into the lower layers of existing industrial wireless protocol stacks to provide improved resistance to interference, increase the number of channels, or to set up ad-hoc high-bandwidth channels, which provide for non-traditional industrial uses such as multimedia applications which may involve video monitoring or transmitting visual data for cyber-physical systems [13]. Simple cognitive aspects, such as dynamic channel selection, carrier sensing and multiple access are already used by existing industrial protocols, so looking at the more advanced concepts in this area is the logical next step to improve these network stacks.

Advanced CR features allow for real-time adaptation of resource utilisation where the characteristics, needs and demands of different applications are automatically taken into consideration. This can include traffic patterns and bandwidth requirements. Unlike traditional wireless networks, such continuous adaptive behaviour is an advancement that can cater for a dynamic environment and circumstances. A CR can, for example, exploit the cyclic nature of most real-time traffic in industrial networks to create adaptive MAC scheduling schemes that enhance the efficiency of spectrum occupation and network throughput.

IV. Spectrum Sensing

CR introduces opportunistic use of spectrum white spaces not utilised by licensed users [47]. To do this, the ability of CRs to sense, measure, learn and have an awareness of channel features, spectrum availability, signal power, the working environment, user applications and their requirements, existing nodes and networks, local policies and other regulations on their operation, is used [48]. In CRNs, SUs need a cognitive capability such as reliable spectrum sensing to evaluate if a channel is in use by an incumbent user and change their radio parameters so as to utilise an unused region of the spectrum. Spectrum sensing is therefore a critical component for establishing a CRN. Detection reliability can be improved by employing Cooperative Spectrum Sensing (CSS). The various aspects of spectrum sensing are shown in Fig. 4 [48].

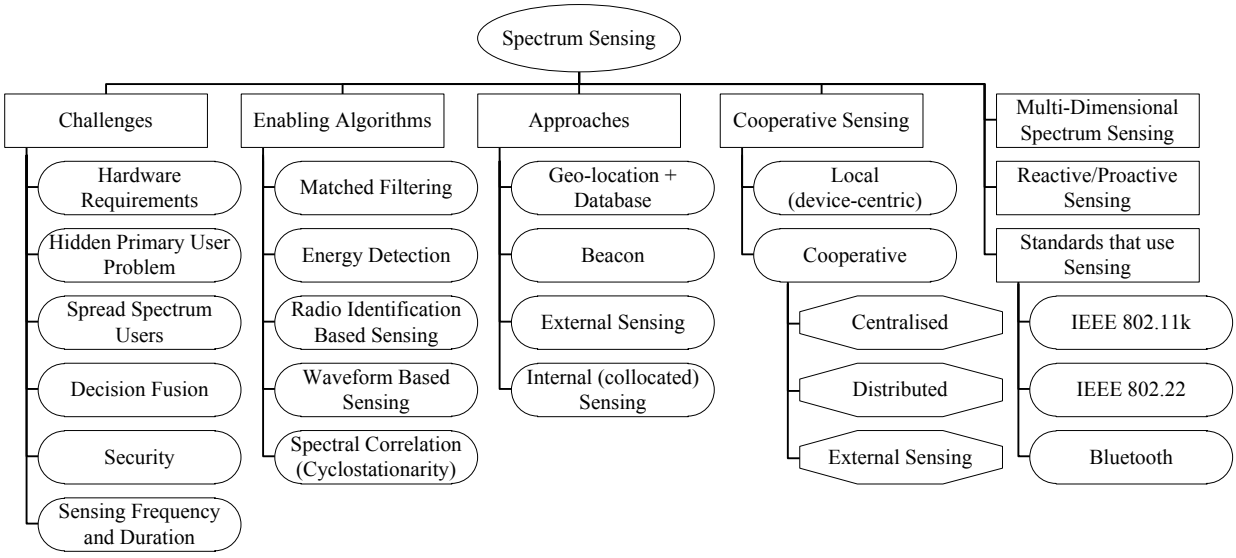

Fig. 4. Different aspects of spectrum sensing for cognitive radio [48].

A. Multiple Hyperspace Dimensions

The definition of a spectrum opportunity determines how spectrum space is measured and exploited. The conventional spectrum opportunity definition is "*a band of frequencies that are not being used by the primary user of that band at a particular time in a particular geographic area*" [49] and only the three dimensions of frequency, time and space are exploited. Traditional sensing methods consider these three dimensions but other dimensions can be considered to discover spectrum opportunities. It is possible to tackle the coexistence problem using the concept of multidimensional electromagnetic (EM) space utilisation where the dimensions of frequency, time, space, code, power and polarisation can distinguish different wireless signals [7]. Cognitive radio uses these dimensions as shown in Table II.

TABLE II
MAIN DIMENSIONS OF HYPERSPACE [7] AS USED BY COGNITIVE RADIO

Dimension	Opportunity
Frequency	Make use of frequency multiplexing.
Time	Make use of time multiplexing.
Space	Location dependent communication or exploiting spatial transmission features through techniques such directional antennas.

Transmissions that use spread spectrum, frequency or time hopping codes are unfamiliar to traditional spectrum sensing algorithms and pose a major problem for spectrum sensing. The dimensions introduced produce a radio space that can be defined as "*a theoretical hyperspace occupied by radio signals, which has dimensions of location, angle of arrival, frequency, time, and possibly others*" [50]. This hyperspace may be referred to as electrospace, radio spectrum space, transmission hyperspace or merely as spectrum space, and it can illustrate how the radio environment can be shared among multiple (licensed and/or unlicensed) systems.

B. Spectrum Sensing for Cognitive Radio

1) Energy Detection

Energy detection is a semi-blind spectrum sensing method that estimates the energy of a received PU signal and compares it to a threshold value to decide on the presence of a PU. The optimal threshold value depends on the estimated noise power. Also known as radiometry, it has low implementation and computational cost and does not require a priori information of the PU signal, unlike other detection methods. Its main drawback is its reliance on accurate noise estimation, which is typically very difficult to achieve, especially in environments with low signal-to-noise ratio (SNR) [51], [52]. It is also very difficult to detect PUs that use spread spectrum signals using energy detection [53].

2) Feature Based Detection

Feature based detectors exploit known properties of a PU signal for detection. The exact implementation of a feature based detector depends on the property of the PU signal being exploited. In systems where the PU signal contains a periodicity, usually because of signal modulation, detection can be performed using the cyclic auto-correlation function [54], [55]. This is due to the redundancy in signal periodicies resulting in modulated signals being cyclostationary with autocorrelation. Known as cyclostationary based detection, this form of spectrum sensing usually only requires knowledge of one or two periodic features in the PU signal to achieve good detection results [56]. It also has the added advantage of being able to distinguish PUs from each other, the background noise and other transmissions [57].

PU signal features can also be exploited to identify the communication technology employed by PUs in radio identification based sensing. Detectors extract signal features such as channel bandwidth and cycle frequencies, and use machine learning techniques to classify the technology being used [53], [58], [59].

3) Coherent Detection

Coherent detection is used when PUs transmit signals with patterns known to the detector. These patterns are usually used by the PU for channel estimation and frequency synchronisation. Examples of such patterns include pilot signals, preambles, midambles and spread sequences. Detection could be performed by correlating the PU signal received with a known copy of the signal [51], [60]. The result of the correlation is then compared with a threshold value to determine the presence or absence of a PU. This form of detection, known as waveform or correlation-based detection is more reliable and has a shorter convergence time compared to energy detectors.

Alternatively, a matched filter could also be used for detection of PUs when the known patterns are transmitted. Matched filter detectors reach a probability of misdetection very quickly but at the cost of large implementation complexity and power consumption [61], [62]. Another drawback of matched filter detectors is that they require almost perfect knowledge of the characteristics of the PU signal to demodulate the received signals.

4) Other Sensing Methods

Multitaper spectrum estimation, random Hough transform and wavelet transform estimation [48] are other methods for sensing spectrum. Multitaper spectrum estimation has been demonstrated to approximate a maximum likelihood Power Spectral Density (PSD) estimator and is nearly optimal for wideband signals in a proposed algorithm [9]. The algorithm is computationally intensive but is less complex than the maximum likelihood estimator. The random Hough transform has been used to detect radar pulses in IEEE 802.11 communication system channels [63]. It is possible to use it to discover any signal that has a periodic pattern. Wavelets have been used to detect a wideband signal's PSD edges [64] found at the boundaries between occupied and empty bands. After finding the edges, the power within each frequency band is estimated. It is then possible to make a binary classification of the frequency spectrum bands as empty or occupied. Multi-resolution spectrum sensing can be accomplished while leaving the sensing circuitry unaltered through altering the carrier frequency and pulse width of the wavelet basis functions [65].

C. Sensing Methods Feasibility in Industrial Environments

The performance of an energy detector mostly depends on the accuracy of noise power estimation. It has been shown that a deviation of 1 dB in the estimation of noise variance, results in energy detection performing worse off than other feature based detection methods. The varying nature of background noise due to factors such as temperature fluctuations [66] in an industrial environment make it difficult to implement an accurate energy detector. The inability of energy detectors to detect spread spectrum signals means they would be unsuitable for industrial applications that use DSSS and FHSS [53].

Feature based detectors are more robust to changing background noise while also providing higher detection accuracy than energy detectors. Waveform based detectors have better convergence time than energy detectors at low SNR making them a suitable candidate for industrial applications [51]. Waveform based detectors require PUs to transmit known pilot symbols or patterns [48] that may not be possible in some industrial applications. Cyclostationary based detectors are more complicated and have a higher observation time than waveform based detectors.

Matched filter detectors are the optimal detectors if perfect knowledge of the PU signal is available. The high cost in terms of implementation complexity and energy make this method unsuitable for most industrial applications [48].

With industrial applications that use spread spectrum techniques, spectrum sensing becomes difficult using the methods discussed. Some suggest that this problem could be mitigated if the detectors [48] know information about the hopping patterns and signal synchronisation. This problem can also be avoided if new spectrum sensing methods that exploit spectral opportunities in the code dimension are developed. The different spectrum sensing algorithms are compared in Fig. 5 according to complexity and accuracy.

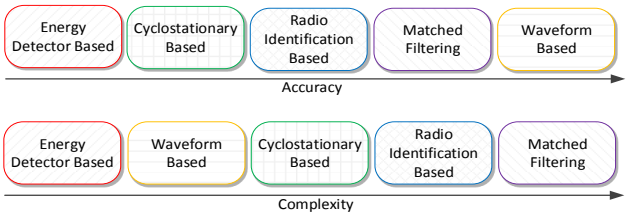

Fig. 5. Main sensing methods ranked according to their sensing accuracy and complexity [48].

V. Dynamic Spectrum Management

Fluctuations in the spectrum available and the various requirements for QoS of different applications impose challenges in wireless networks that can be addressed by dynamic spectrum management with CRs [8]. In spectrum management, the best available spectrum band to meet a user's communication requirements is selected while not creating undue interference to other users.

Dynamic spectrum management stands in contrast to conventional coexistence management, which seeks to achieve coexistence through careful network planning, restrictions on the use of radio systems, and network organization by a human expert or a specialized tool. Procedures, guidelines and standards have been drafted for coexistence management such as is in the VDI/VDE 2185 guideline part 2 and the technical specification IEC/TS 62657-2. Such coexistence management can be complex and costly but it has shown that coexistence in wireless automation systems is possible given the small data payloads and typical communication intervals. Dynamic spectrum management is self-organising and can achieve automated coexistence management so as to maintain a high level of reliability of each process and high global system availability.

A. Spectrum Decision

Deciding on the best spectrum band among the available bands under the QoS requirements of the applications is referred to as spectrum decision [8], [67]. In the first step of spectrum decision, statistical PU information and local readings from CRs are used to characterise each band (spectrum characterisation). The next step of spectrum decision is to select the most suitable spectrum band, based on the earlier characterisation (spectrum selection). Finally, there may be a need for a SU to reconfigure the communication protocol, hardware and the RF front-end under the QoS requirements and the prevailing radio environment. This is the reconfiguration step.

Some challenges in spectrum decision include supporting spectrum decision over heterogeneous spectrum bands, using a cooperative framework with reconfiguration, and designing adaptive spectrum decision models that consider application needs and spectrum capacity [8].

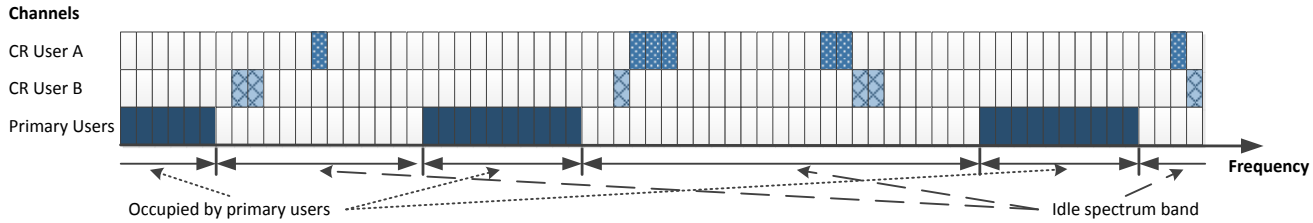

Fig. 6. Channel structure of the multi-spectrum decision [8].

1) Spectrum Characterisation

The available spectrum holes show different time varying characteristics. They should be characterised in a way that considers temporal variations in the radio environment and factors such as signal bandwidth and frequency. Parameters that represent a particular spectrum band therefore must be defined as follows [27]:

- *Interference temperature:* The allowable power of a SU can be determined using the interference level at the receiver of a PU. This is then used to estimate the capacity of the channel.
- *Path loss:* This is tightly coupled to the frequency and range as path loss increases with operating frequency, culminating in a loss in transmission range. Increasing transmission power can compensate for the loss in range but other users may experience an increase in interference.
- *Wireless link errors:* The error rate of the channel changes according to the choice of modulation scheme and the in-band interference level.
- *Link layer delay:* Each spectrum band will require a different link layer protocol to address the differences in wireless link error, interference and path loss. The result of this will be different link layer delays.

A metric that captures the statistical characteristics of licensed networks to depict the inherent fluctuations of secondary networks has been proposed. This metric is called the *primary user activity* [8]. Given that there is uncertainty on the availability of a spectrum band for the entire duration of a SU's communication, approximation of the PU activity is essential in spectrum decision.

2) Spectrum Selection

Once the available spectrum bands are characterised, the most suitable band must be chosen. This choice is made using a spectrum selection rule based on QoS requirements, data rate, spectrum characteristics, delay bound, transmission mode and the acceptable error rate. SUs cannot gain exclusive access to a reliable wireless channel for extended periods because of the operation of primary networks. In addition, CRs may not identify any individual spectrum band that meets user requirements. As a result, CRs can use transmissions using multi-radio in which each transceiver is tuned to different bands of non-continuous spectrum for various users and transmit data concurrently as shown in Fig. 6.

Spectrum selection is influenced by the underlying CRN topology [67]. In centralised, infrastructure based CRNs with a point-to-multipoint topology the spectrum selection is normally performed at the base station (BS) or access point (AP). In distributed multi-hop CRNs, spectrum selection can be done locally in a non-cooperative fashion that does not involve the exchange of information, or cooperatively where SUs exchange information, thus allowing the global channel state to be discovered quickly and accurately, albeit with greater communication overhead. Multiple hops and variable spectrum opportunities make up the communication session and hence there is a close link between the rule to select spectrum and routing protocols in distributed CRNs and hence a dynamic decision framework is needed that can accommodate the changing channel conditions and user requirements for QoS.

3) Reconfiguration

Aside from the selection of routes and spectrum bands, another part of spectrum decision is reconfiguration in CRNs. Protocols for separate layers of the protocol stack need to accommodate the channel parameters of the spectrum in use. An example of this is in ad-hoc CRNs where, as a result of multi-hop communication, the spectrum decision function must look at the end-to-end route [27]. The available spectrum bands will differ from hop to hop resulting in spectrum dependent connectivity, which makes it difficult to calculate the optimal pairing of spectrum bands and routing path to use. Selection of spectrum bands and the routing path must therefore be done simultaneously.

The proper communication modules need to be selected once the spectrum has been decided, and this includes the physical layer technology. Adaptive protocols have been developed that can ascertain the best combination of modulation, coding scheme and the transmission power for a new spectrum band by taking into account changes in signal attenuation [68].

B. Spectrum Sharing

The wireless channel is a shared medium, and as a result it is necessary to coordinate the transmission attempts between different SUs. In order for this to work effectively, several MAC protocol functions should be included in spectrum sharing. The coexistence of SUs and licensed PUs in CRNs and the large extent of spectrum opportunities introduce some spectrum sharing challenges in CR networks. Theoretically, the amount of RF spectrum available covers the entire RF range (3 kHz to 300 GHz) although in practice it is more limited than this due to propagation concerns and other technical constraints including hardware limitations that make some portions more preferable. Sharing spectrum with licensed users is known as *vertical spectrum sharing* and this produces licensed band operation of the CRN. Sharing spectrum with unlicensed radio systems is known as *horizontal spectrum sharing* and gives rise to unlicensed band operation of the CRN. An example of a CRN network architecture is shown in Fig. 7.

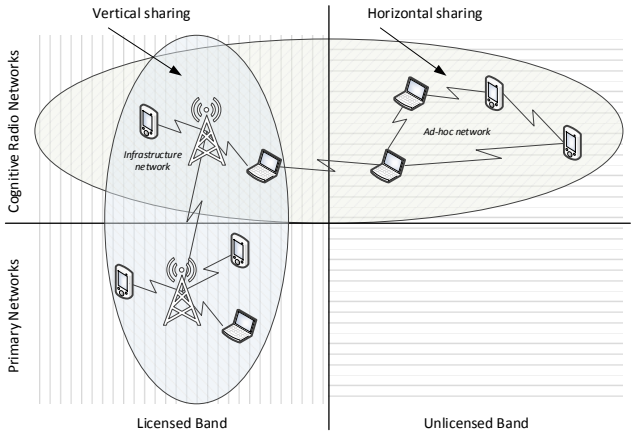

Fig. 7. Example CRN architecture [27].

1) Classification of Approaches

Four attributes can classify approaches for solving spectrum sharing challenges, namely the *architecture, spectrum allocation behaviour, spectrum access technique* and *scope*. The architecture can be *centralised*, where there is control by a central entity, or *distributed*, where individual nodes carry out local policies collaboratively to share spectrum. In terms of allocation behaviour, this can be *cooperative* or *non-cooperative*. Cooperative spectrum sharing exploits the interference measurements of all nodes in such a way that the effect of transmission by one node on other nodes is taken into consideration [69]. In non-cooperative sharing, solutions are determined using local information considering a single node only. Cooperative approaches perform better than non-cooperative ones, and provide a closer approximation of the global optimum.

The access technology used in spectrum sharing can be overlay spectrum sharing or underlay spectrum sharing [70]. In underlay spectrum sharing, techniques that spread the transmitted signal over a large band of spectrum are used, so that PUs regard transmissions by CR nodes as noise and simultaneous uncoordinated spectrum usage is achieved. These techniques include OFDM, UWB, and spread spectrum. Transmission power can be strictly limited in underlay sharing to reduce potential interference. In overlay sharing there is opportunistic access to spectrum white spaces while avoiding harmful interference to other radios using the same spectrum, whether or not the frequency is assigned to licensed users. This approach requires new protocols and algorithms. Dynamic Frequency Selection (DFS) is a simple example of overlay sharing. In terms of scope, spectrum sharing techniques can be inside a CR network (intra-network spectrum sharing) or between multiple coexisting CR networks (inter-network spectrum sharing) as shown in Fig. 8.

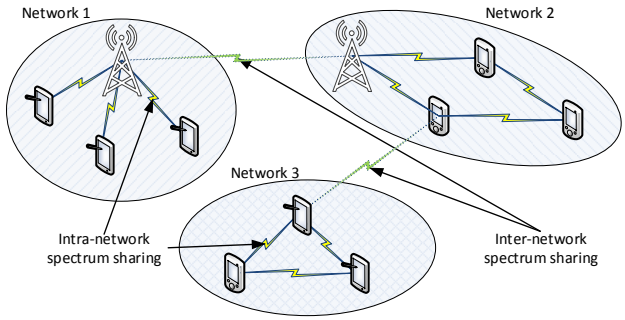

Fig. 8. Inter-network and intra-network spectrum sharing in CRNs [8].

2) Resource Allocation

Resource allocation in spectrum sharing can be based on *power control* where SUs adjust their transmission power to attain resource equity and meet QoS requirements, or *channel allocation* where SUs select the proper channels to use. Traditional approaches to spectrum sharing are based on fully cooperative, static, centralised models not applicable to dynamic environments where SUs must adjust their operating parameters based on interaction with the environment and other users [11].

Spectrum sharing using power control in a multi-user CR environment involving competition and cooperation is a multi-user communication theoretic problem. A full appreciation of multi-user communication theory has yet to be established, though there are two diverse disciplines of information theory and game theory that can help solve this challenging problem. Iterative water filling is one particular information theory based technique that can be used for power control [9].

Graph theory has been investigated for solving the channel allocation problem, where the problem is reduced to a variant of the graph colouring problem, however the global optimisation problem has been shown to be NP-hard and is typically not practical. Some heuristic based approaches have been suggested that produce good solutions [55], [71], [72]. Game theory, local bargaining and rule based techniques can also be used for channel allocation.

From the above it can be seen that game theory can be used for both power control and channel allocation. In addition, it can provide an efficient distributed scheme for sharing spectrum that describes the conflict and cooperation among SUs. It allows interactions between SUs to be modelled and formulated, and as a result enables each SU to reasonably determine its best course of action [27], [73]. Better flexibility of radio resource usage can be achieved to improve system performance while complexity and signalling overhead is reduced. Game theory is therefore well suited for spectrum sharing and is described in more detail in section VI.

C. Spectrum Mobility

Spectrum mobility occurs when a SU needs to change its operating spectrum bands. This is largely due to PU activity on spectrum that the CR would have previously selected as the best available spectrum. Adaptive protocols that adhere to channel conditions at the operating frequency are required for different layers of the network stack. These protocols must be resilient to spectrum hand off and the delays that come with it. Spectrum mobility management in CRNs ensures seamless and speedy changeover resulting in minimal performance loss when performing spectrum hand off. Protocols for mobility management need details on the time taken for spectrum hand off which can be obtained from a sensing algorithm. On obtaining this information, ongoing communications can proceed with minimal loss in performance.

VI. GAME THEORY FOR SPECTRUM SHARING

Game theory is a mathematical tool that analyses strategic interactions among multiple decision makers [11]. Using a game theoretic model to study CRNs has several advantages, the first of which is that it enables the actions and behaviour of network users to be analysed using an established structure. Secondly, game theory provides measures to determine the most favourable solution to the problem of spectrum sharing. Game theory offers well defined equilibrium criteria and can be used under diverse game conditions to measure the optimality of a game. This is useful as spectrum sharing is a challenging multiple objective optimisation problem. Thirdly, distributed methods to share spectrum dynamically using local information alone can be developed using non-cooperative game theory.

Four categories can classify game theoretic spectrum sharing schemes namely (1) non-cooperative games and Nash equilibrium, (2) economic games, auction games and mechanism design, (3) cooperative games and (4) stochastic games.

A strategic form game theory model has three main components:

- a finite set of players, denoted by N;
- a set of actions, denoted by A_i for each player i; and
- a payoff/utility function, denoted by $u_i: A \rightarrow \mathbb{R}$ which measures the outcome of player i determined by the actions of all players, $A = \times_{i \in N} A_i$.

A. Non cooperative Games and Nash Equilibrium

Non-cooperative games are those in which interactive players make decisions independently. When each player plays its best strategy, while considering the actions of other players, the equilibrium attained is known as Nash Equilibrium (NE). NE does not provide details on how to arrive at the equilibrium but gives information on the eventual equilibrium outcome. The equilibrium exists but is not always unique and has to be determined for each case. When SUs do not have global knowledge, they can begin from a position of their discretion and use a rule based update strategy giving a prediction that converges to the equilibrium. A shortcoming of NE is that in adversarial games involving selfish players, it is prone to over competition.

It is possible for a game to have multiple equilibrium points, in which case it is desirable to evaluate the performance of each and find the optimal one if it exists. However, defining optimality in such scenarios involving multi-objective optimisation is not simple. A popular way to do so is to use Pareto optimality, a payoff profile where no one strategy can improve a player's performance without degrading that of another.

In [74] a non-cooperative spectrum access game is considered where SUs access several spectrum holes in licensed bands simultaneously. The existence of a Nash equilibrium is demonstrated and settings for equilibrium spectrum access are derived. A comprehensive analysis of the competitive spectrum access game under different system settings is presented and it is shown that an increase in the number of SUs increases the price of anarchy (PoA). The PoA also increases as the number of wireless channels increase.

B. Economic Games, Auction Games and Mechanism Design

How people interact with one another in markets can be dealt with by applying game theory to economics. Useful theoretical results and games of interest are produced covering auction theory and micro-economics. There are several reasons why economic games can be applied in CRNs. First, economic models are suitable in scenarios in which PUs can sell rights to unutilised spectrum in the secondary spectrum market. The exchange can be carried out through pricing, auctions, or similar means. Second, economic games are not confined to scenarios with explicit buyers and sellers, but can extend to include spectrum sharing situations that do not involve secondary spectrum markets. Third, it is important to appreciate CRNs from an economic point of view and formulate efficient processes to control the spectrum market, as their success will greatly depend on the combination of policy, markets and technology.

1) Oligopolistic competition

In a completely competitive market, the point where the demand and supply curves meet is the market equilibrium. At the opposite extreme is a monopoly, where one firm controls the market of one product. An oligopoly is a more complicated market that lies in between a monopoly and full competition, where due to large obstacles to participate in economics there are few firms. Due to the few firms, each can affect the price and subsequently other firms; such as influence their price selection strategy and the amount of goods to supply to the market. This relationship can be modelled through several game theory constructs such as the *Cournot game,* the *Bertrand game,* the *Stackelberg game* and the *Cartel maintenance game*. These methods can be used in different spectrum markets.

2) Auction games

Auction theory is an applied form of game theory that investigates attributes and relationships in auction markets. An **auctioneer** conducts an auction by sourcing **bids** from prospective purchasers, and the result of the auction is determined by the rules of the auction. Four simple ways to classify an auction are:

- **English (open ascending price) auction**: an auction where participants openly bid against each other with each subsequent bid being larger than the other until an individual bidder remains that wins the product.
- **Dutch (open descending price) auction**: an auction where the auctioneer begins with a high asking price, which is lowered until a bidder accepts.
- **Second price (sealed bid) auction**: in this auction all bidders submit sealed bids at once and the highest bidder wins the product at the price of the second highest bid.
- **First price (sealed bid) auction**: in this auction all bidders submit sealed bids and the product goes to the highest bidder at a payment equal to their own bid price.

In [75] an auction based mechanism between primary and SUs is proposed for spectrum leasing. The scheme is

cooperative and numerical results show that the primary network could achieve a higher throughput with cooperation as opposed to when there is no cooperation among users. SUs are shown to increase their quality of service and PUs enjoy other benefits such as increased link reliability.

3) Mechanism design

Mechanism design seeks to answer the question of which is the most favourable product assignment. A "**principal**" designs the game structure and chooses a mechanism serving their interest. Players known as "**agents**" have privileged information known to themselves as in auction games. The principal asks the agents for some "**messages**" to elicit their private information for the game. Incentives in the form of monetary gains known as "**transfers**" are given to players, as they are not necessarily honest. In mechanism design, incentives and resource constraints are equally taken into account when allocating spectrum with privileged information.

C. Cooperative Games

Cooperative games arise when there is a common understanding among network users on the way to share available spectrum opportunities fairly. Cooperative games can be put in two main categories, namely bargaining games and coalition games.

1) Bargaining games

In bargaining games, individuals negotiate an agreement that benefits all parties. Decisions cannot be imposed on any player without their consent, as players have conflicting interests. In a bargaining game with two players $\mathrm{N} = \{1,2\}$ (extendable to accommodate additional players) for an agreement, player 1 has utility u_1 and player 2 utility u_2. In the instance they do not agree, then they have utilities u_1^0 and u_2^0 respectively. All potential utility pairs are in the set U.

Several bargaining games have been proposed in literature. In [76] a two-tier spectrum access market is proposed. In the first tier, PUs trade spectrum to a set of SUs for a long period using a Nash bargain game model. The SUs then use the second tier to redistribute the spectrum amongst each other in a smaller time scale using a strategic bargain game. A new Nash bargaining game is proposed for OFDMA CRs in [77]. On average, the proposed game is shown to achieve close to optimal capacity.

2) Coalition games

Coalition games describe how a group of players can collaborate through cooperative associations that will advance their payoff in a game. In [78] a partitioned coalition game is proposed that encompasses spectrum sharing and spectrum sensing. The game allows for SUs to freely switch between coalitions depending on the time spent in spectrum sensing and spectrum access. A hedonic coalition game is proposed in [79] for both spectrum sensing and sharing where a coalition represents SUs who sense and use a specific channel. Results show SUs achieve better utility with iteration and converge to a partition stable both individually and in terms of Nash-stability.

D. Stochastic Games

A stochastic game involves a dynamic environment with constant game state transitions based on actions by the players. CRNs are dynamic with a time varying radio environment, influenced by player actions like occupying a spectrum segment, and as a result changing spectrum opportunities. As stochastic games are designed for dynamic environments, this approach is potentially more suited to CRNs when compared to the other games. Stochastic games can be used for *spectrum auction, transmission control* or *anti-jamming defence* in CRNs [11].

VII. SECURITY

To deploy industrial CRNs successfully, it is necessary to develop and put in place security procedures that will guarantee the resilience of the network and individual CR nodes against security attacks. Many industrial applications may be mission critical and may have certification or standardisation requirements that make security crucial. The peculiarities of industrial networks restrict the use of classical approaches to security [80]. The cognition and re-configurability of CRs central to their functioning introduce a new class of security concerns distinct to those evident in conventional wireless networks [81]. Vulnerabilities present in this new CR technology can be exploited by antagonists to compromise the integrity of a CR network and induce severe performance degradation. Security threats associated with cognitive ability include licensed user emulation, transmission of false spectrum sensing observations and selfish misbehaviours. Reconfiguration related threats include the download of malicious software and configuration files. Besides these threats, CRs are prone to all the long established threats found in traditional wireless networks.

CRNs must support several security objectives just like all other wireless technologies [82]. The objectives above help to leverage Information Assurance (IA), defined by the National Security Agency [83] as "measures intended to protect and defend information and information systems by ensuring their availability, integrity, authentication confidentiality and non-repudiation". Examples of general network security threats, services and mechanisms in the CR context are shown in Table III.

A. Attacks against Cognitive Radio Networks and Detection Techniques

1) Primary user emulation attacks

An underlying feature of a CR is its capability to perform spectrum sensing, since it accesses spectrum opportunistically. In opportunistic spectrum access, the CR must leave a licensed region of spectrum if a PU transmission exists. This requires the CRs to perform spectrum hand-off as part of spectrum mobility when seeking different spectrum white spaces for transmissions. Spectrum hand-off has the undesirable effect of degrading the CRs performance as more time for spectrum sensing is needed, which reduces the time that can be used for spectrum access. Adversaries can exploit this integral CR procedure through the mimicking of incumbent signals. There are two categories of nodes that launch Primary User Emulation Attacks (PUEAs) [81]:

- **Greedy** nodes: These nodes seek to gain sole access to a particular spectrum band by transmitting fake incumbent signals, forcing other nodes to leave the band.

TABLE III
OTHER COGNITIVE RADIO THREATS AND PROTECTION TECHNIQUES [84]

Threat Description	Security Service Required	Affected Functionality	Protection Mechanism
Eavesdropping of cognitive control messages	• Confidentiality	• Spectrum sensing • Spectrum sharing	• Encryption • Frequency hopping
Jamming cognitive control messages	• Integrity	• Spectrum sensing • Spectrum sharing	• Frequency hopping
Compromise of a cognitive radio node	• Integrity • Trusted hardware	• Spectrum sharing • Spectrum mobility	• Identification of modified actions through signal analysis or reputation systems • Remote attestation
Malicious alteration of cognitive messages	• Integrity • Non-repudiation	• Spectrum sensing • Spectrum sharing	• Data origin authentication with MAC • Non-repudiation with digital signatures
Fake cognitive radio node	• Authentication • Source authentication of messages • Access control	• Spectrum sensing • Spectrum sharing	• Identification of masquerading threats through signal analysis • Authentication of CR Nodes

- **Malicious** nodes: These are adversarial nodes intending to cause Denial of Service (DoS) attacks to SUs by mimicking incumbent signals or to PUs by causing harmful interference. These nodes can form coalitions to cause extensive DoS attacks across several bands causing major disruptions in service.

Both attacks disrupt operation of the CRN and cause unfairness among network nodes. A PUEA can disrupt the operation of all stages of the cognitive cycle in a CRN; initially the radio-frequency environment is polluted by fake PU signals. This causes a cascading phenomenon that affects spectrum sensing, analysis and decision. Energy detection is the most widely used spectrum sensing technique due to its simplicity and low computational overhead [52], [85]. Energy detection is most susceptible to PUEAs due to its poor performance in environments with low SNR. In addition, since creating signals using carrier frequencies of PUs is simple, non-sophisticated adversaries can initiate PUEAs targeted at SUs that use energy detection. Learning CRs are more susceptible to PUEAs since they construct a manner of acting over an extended period founded on measurements recorded from the environment [86].

The FCC has expressed that "*no modification to the incumbent signal should be required to accommodate opportunistic use of the spectrum by SUs*". As a result, most detection techniques that have been proposed to protect against PUEAs involve no altering of the PU signal. In addition, some approaches presume that information is available on the position of incumbent user's transmitters. Considering this, different contributions to detecting PUEAs can be characterised as follows [81]:

- Whether or not incumbent signal is modified,
- cooperation or non-cooperation based,
- advantages and disadvantages from use,
- location-based or non-location-based, and
- tested using simulations or real implementations.

2) Spectrum sensing data falsification attacks

It is possible that some of the SUs will send false observations intentionally or inadvertently, resulting in hampering collaborative spectrum sensing in a Spectrum Sensing Data Falsification (SSDF) attack. In much the same way as with PUEAs, misbehaving nodes carrying out SSDF attacks can be classified as:

- **Malicious** nodes: These nodes send false observations to mislead the fusion center or other nodes into incorrectly asserting that an ongoing PU transmission is in progress or that there are no licensed user transmissions when that is not the case.
- **Greedy** nodes: These nodes constantly report that a particular band of licensed spectrum is occupied by PUs so that all other SUs evacuate it and the greedy nodes can then monopolise use of the band.
- **Unintentionally** misbehaving nodes: These nodes that have parts of their software malfunctioning leading them to report faulty observations on available spectrum.

The majority of approaches to detecting SSDF attacks presume a scenario in which cognitive users send their observations to a Fusion Center (FC) but the SUs are not trusted beforehand. These approaches propose methods to calculate reputation metrics with the aim to detect and isolate users that pose a security threat. The FC combines the reports generated by trusted nodes and does not include reports from identified attackers. These reports can be (i) continuous (such as the energy detector's power estimation) or (ii) binary (such as whether or not a primary transmission is present). If a node misbehaves but later acts appropriately then some approaches allow for restoring the reputation metric.

Different contributions [87], [88], [89] to SSDF detection can be characterised according to:

- Fusion rules in use,
- the type of reporting,
- advantages and disadvantages of use, and
- whether or not the reputation metric is restored.

3) MAC Layer Threats

It is of great importance to avoid interference to PUs in CRNs and to achieve this the MAC layer must interact closely with the lower layers. This cross layer operation does not follow the strict boundaries between layers of the waterfall like concept found in the OSI communications model. There are two categories of CR MAC protocols, (i) standardised such as the IEEE 802.22 protocol and (ii) application or scenario specific protocols. CR MAC protocols can also be categorised as being Direct Access Based (DAB) which do not permit global optimisation due to sender-receiver pairs maximising their individual optimisation goals, or Dynamic Spectrum Access (DSA) which use complicated optimisation techniques to attain a global goal adaptively [90]. These are shown in Fig. 9. Using a Common Control Channel (CCC) is a main characteristic of CR MAC protocols. The CCC is central to the operation of a CRN and can become the target of DoS attacks from adversaries.

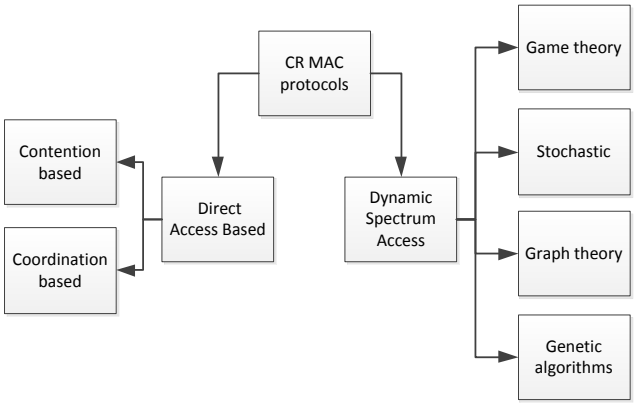

Fig. 9. Categories of cognitive radio MAC protocols [90].

VIII. CONCLUSION

In this paper, we discuss the potential benefits and current limitations of using cognitive radio techniques in industrial wireless sensor networks. Cognitive radio approaches can be added to the lower layers of existing industrial network stacks to improve resistance to interference, simplify coexistence with other industrial and consumer networks, and offer additional communication spectrum to allow wideband communication or additional narrow-band channels. Cognitive radio is a developing area and there are still some areas that need to be addressed. These include standardisation, latency and efficiency of spectrum sensing on restricted sensor nodes, the speed of channel selection and dynamic reconfiguration once a channel encounters interference, and compliance with timeliness constraints in industrial applications. The paper also provide an overview of different techniques for spectrum sensing and spectrum management in cognitive radio networks. We explore the application of game theory for spectrum sharing, and discuss selected security aspects of cognitive radio implementation.

REFERENCES

[1] A. Willig, "Recent and emerging topics in wireless industrial communications: A selection," *IEEE Trans. Ind. Informat.,* vol. 4, no. 2, pp. 102-122, 2008.

[2] J. Chen, X. Cao, P. Cheng, Y. Xiao and Y. Sun, "Distributed collaborative control for industrial automation with wireless sensor and actuator networks," *IEEE Trans. Ind. Electron.,* vol. 57, no. 12, pp. 4219-4230, 2010.

[3] J. Silvestre-Blanes, L. Almeida, R. Marau and P. Pedreiras, "Online QoS management for multimedia real-time transmission in industrial networks," *IEEE Trans. Ind. Electron.,* vol. 58, no. 3, pp. 1061-1071, 2011.

[4] V. C. Gungor and G. P. Hancke, "Industrial wireless sensor networks: Challenges, design principles, and technical approaches," *IEEE Trans. Ind. Electron.,* vol. 56, no. 10, pp. 4258-4265, 2009.

[5] G. Cena, L. Seno, A. Valenzano and C. Zunino, "On the performance of IEEE 802.11e wireless infrastructures for soft-real-time industrial applications," *IEEE Trans. Ind. Informat.,* vol. 6, no. 3, pp. 425-437, 2010.

[6] F. P. Rezha and S. Y. Shin, "Performance analysis of ISA 100.11a under interference from an IEEE 802.11b wireless network," *IEEE Trans. Ind. Informat.,* vol. 10, no. 2, pp. 919-927, 2014.

[7] K. Ahmad, P. -. Ostfeld, U. Meier and H. Kwaśnicka, "Exploitation of multiple hyperspace dimensions to realize coexistence optimized wireless automation systems," *IEEE Trans. Ind. Informat.,* vol. 6, no. 4, pp. 758-766, 2010.

[8] I. F. Akyildiz, W. -. Lee, M. C. Vuran and S. Mohanty, "A survey on spectrum management in cognitive radio networks," *IEEE Commun. Mag.,* vol. 46, no. 4, pp. 40-48, 2008.

[9] S. Haykin, "Cognitive radio: Brain-empowered wireless communications," *IEEE J. Select. Areas Commun.,* vol. 23, no. 2, pp. 201-220, 2005.

[10] Federal Communications Commission, "Notice of proposed rulemaking and order: Facilitating opportunities for flexible, efficient, and reliable spectrum use employing cognitive radio technologies," vol. ET Docket No. 03-108, Feb 2005.

[11] B. Wang, Y. Wu and K. J. R. Liu, "Game theory for cognitive radio networks: An overview," *Computer Networks,* vol. 54, no. 14, pp. 2537-2561, 2010.

[12] G. Gamba, F. Tramarin and A. Willig, "Retransmission strategies for cyclic polling over wireless channels in the presence of interference," *IEEE Trans. Ind. Informat.,* vol. 6, no. 3, pp. 405-415, 2010.

[13] P. Gaj, J. Jasperneite and M. Felser, "Computer Communication Within Industrial Distributed Environment—a Survey," *IEEE Trans. Ind. Informat.,* vol. 9, no. 1, pp. 182-189, 2013.

[14] S. Petersen and S. Carlsen, "WirelessHART versus ISA100.11a: The format war hits the factory floor," *IEEE Ind. Electron. Mag.,* vol. 5, no. 4, pp. 23-34, 2011.

[15] T. Kaiser, M. D. Pérez-Guirao and A. Wilzeck, "Cognitive radio & networks in the perspective of industrial wireless communications," in *2009 2nd International Workshop on Cognitive Radio and Advanced Spectrum Management, CogART 2009,* 2009, pp. 24-29.

[16] R. L. Kirlin, C. Lascu and A. M. Trzynadlowski, "Shaping the noise spectrum in power electronic converters," *IEEE Trans. Ind. Electron.,* vol. 58, no. 7, pp. 2780-2788, 2011.

[17] O. Staub, J. Zurcher, P. Morel and A. Croisier, "Indoor propagation and electromagnetic pollution in an industrial plant," in *IECON Proceedings (Industrial Electronics Conference),* 1997, pp. 1198-1203.

[18] K. S. Low, W. N. N. Win and M. J. Er, "Wireless sensor networks for industrial environments," in *Proceedings - International Conference on Computational Intelligence for Modelling, Control and Automation, CIMCA 2005 and International Conference on Intelligent Agents, Web Technologies and Internet,* 2005, pp. 271-276.

[19] R. Steigmann and J. Endresen, "Introduction to WISA: WISA–Wireless Interface for Sensors and Actuators," *White Paper, ABB,* 2006.

[20] R. Jurdak, C. V. Lopes and P. Baldi, "A survey, classification and comparative analysis of medium access control protocols for ad hoc networks," *IEEE Commun. Surveys & Tutorials,* vol. 6, no. 1, pp. 2-16, 2004.

[21] S. Stanczak, M. Wiczanowski and H. Boche, *Fundamentals of Resource Allocation in Wireless Networks: Theory and Algorithms.* Springer, 2009.

[22] G. M. Dousoky, M. Shoyama and T. Ninomiya, "FPGA-Based spread-spectrum schemes for conducted-noise mitigation in DCDC power converters: Design, implementation, and experimental investigation," *IEEE Trans. Ind. Electron.,* vol. 58, no. 2, pp. 429-435, 2011.

[23] J. Wang, Q. Gao, Y. Yu, H. Wang and M. Jin, "Toward robust indoor localization based on Bayesian filter using chirp-spread-spectrum ranging," *IEEE Trans. Ind. Electron.,* vol. 59, no. 3, pp. 1622-1629, 2012.

[24] A. Bachir, M. Dohler, T. Watteyne and K. K. Leung, "MAC essentials for wireless sensor networks," *IEEE Commun. Surveys & Tutorials,* vol. 12, no. 2, pp. 222-248, 2010.

[25] V. C. Gungor, B. Lu and G. P. Hancke, "Opportunities and challenges of wireless sensor networks in smart grid," *IEEE Trans. Ind. Electron.,* vol. 57, no. 10, pp. 3557-3564, 2010.

[26] F. K. Jondral, "Software-defined radio - Basics and evolution to cognitive radio," *Eurasip Journal on Wireless Communications and Networking,* vol. 2005, no. 3, pp. 275-283, 2005.

[27] I. F. Akyildiz, W. -. Lee and K. R. Chowdhury, "CRAHNs: Cognitive radio ad hoc networks," *Ad Hoc Networks,* vol. 7, no. 5, pp. 810-836, 2009.

[28] A. Khattab, D. Perkins and M. A. Bayoumi, "Opportunistic spectrum access: From theory to practice," *IEEE Veh. Technol. Mag.,* vol. 7, no. 2, pp. 62-68, 2012.

[29] Hyung-Jung Kim, Jin-Up Kim, Jae-Hyung Kim, Hongmei Wang and In-Sung Lee, "The Design Method and Performance Analysis of RF Subsampling Frontend for SDR/CR Receivers," *IEEE Trans. Ind. Electron.,* vol. 57, no. 5, pp. 1518-1525, 2010.

[30] T. Ulversoy, "Software defined radio: Challenges and opportunities," *IEEE Commun. Surveys & Tutorials,* vol. 12, no. 4, pp. 531-550, 2010.

[31] K. Nishimori, H. Yomo and P. Popovski, "Distributed Interference Cancellation for Cognitive Radios Using Periodic Signals of the Primary System," *IEEE Trans. Wireless Commun.,* vol. 10, no. 9, pp. 2971-2981, 2011.

[32] G. M. Shrestha, K. Ahmad and U. Meier, "Statistical analysis and predictive modeling of industrial wireless coexisting environments,"

in *IEEE International Workshop on Factory Communication Systems - Proceedings, WFCS,* 2012, pp. 125-134.

[33] N. Devroye, M. Vu and V. Tarokh, "Cognitive radio networks: Highlights of information theoretic limits, models, and design," *IEEE Signal Process. Mag.,* vol. 25, no. 6, pp. 12-23, 2008.

[34] Chang-Jiang You, Xiao-Wei Zhu, Xiao-Dong Zhang, Jing Liu, Zhi-Gang Cao, Jia Chen, Luong Ngoc Quyen and Wei-Yu Zong, "Study of RF Subsystem Used in Dynamic Spectrum Sharing System at TV Band," *IEEE Trans. Ind. Electron.,* vol. 60, no. 6, pp. 2346-2357, 2013.

[35] G. P. Villardi, G. Thadeu Freitas De Abreu and H. Harada, "TV white space technology: Interference in portable cognitive emergency network," *IEEE Veh. Technol. Mag.,* vol. 7, no. 2, pp. 47-53, 2012.

[36] Muhammad Faisal Amjad, B. Aslam and C. C. Zou, "Transparent cross-layer solutions for throughput boost in cognitive radio networks," in *Consumer Communications and Networking Conference (CCNC), 2013 IEEE,* 2013, pp. 580-586.

[37] Chen Sun, G. P. Villardi, Zhou Lan, Y. D. Alemseged, H. -. Tran and H. Harada, "Optimizing the Coexistence Performance of Secondary-User Networks Under Primary-User Constraints for Dynamic Spectrum Access," *IEEE Trans. Veh. Technol.,* vol. 61, no. 8, pp. 3665-3676, 2012.

[38] M. Cesana, F. Cuomo and E. Ekici, "Routing in cognitive radio networks: Challenges and solutions," *Ad Hoc Networks,* vol. 9, no. 3, pp. 228-248, 5, 2011.

[39] T. M. Chiwewe and G. P. Hancke, "A Distributed Topology Control Technique for Low Interference and Energy Efficiency in Wireless Sensor Networks," *IEEE Trans. Ind. Informat.,* vol. 8, no. 1, pp. 11-19, 2011.

[40] G. A. Shah, V. C. Gungor and O. B. Akan, "A Cross-Layer QoS-Aware Communication Framework in Cognitive Radio Sensor Networks for Smart Grid Applications," *IEEE Trans. Ind. Informat.,* vol. 9, no. 3, pp. 1477-1485, 2013.

[41] T. Zheng, Y. Qin, H. Zhang and S. -. Kuo, "A self-configurable power control algorithm for cognitive radio-based industrial wireless sensor networks with interference constraints," in *IEEE International Conference on Communications,* 2012, pp. 98-103.

[42] P. T. A. Quang and D. -. Kim, "Throughput-aware routing for industrial sensor networks: Application to ISA100.11a," *IEEE Trans. Ind. Informat.,* vol. 10, no. 1, pp. 351-363, 2014.

[43] J. Hu, L. -. Yang and L. Hanzo, "Maximum average service rate and optimal queue scheduling of delay-constrained hybrid cognitive radio in nakagami fading channels," *IEEE Trans. Veh. Technol.,* vol. 62, no. 5, pp. 2220-2229, 2013.

[44] C. -. Sum, G. Villardi, M. A. Rahman, T. Baykas, H. Tran, Z. Lan, C. Sun, Y. Alemseged, J. Wang, C. Song, C. -. Pyo, S. Filin and H. Harada, "Cognitive communication in TV white spaces: An overview of regulations, standards, and technology," *IEEE Commun. Mag.,* vol. 51, no. 7, pp. 138-145, 2013.

[45] C. R. Stevenson, G. Chouinard, Z. Lei, W. Hu, S. J. Shellhammer and W. Caldwell, "IEEE 802.22: The first cognitive radio wireless regional area network standard," *IEEE Commun. Mag.,* vol. 47, no. 1, pp. 130-138, 2009.

[46] C. -. Sum, M. -. Zhou, L. Lu, R. Funada, F. Kojima and H. Harada, "IEEE 802.15.4m: The first low rate wireless personal area networks operating in TV white space," in *IEEE International Conference on Networks, ICON,* 2012, pp. 326-332.

[47] J. Mitola III and G. Q. Maguire Jr., "Cognitive radio: making software radios more personal," *IEEE Pers. Commun.,* vol. 6, no. 4, pp. 13-18, 1999.

[48] T. Yücek and H. Arslan, "A survey of spectrum sensing algorithms for cognitive radio applications," *IEEE Commun. Surveys & Tutorials,* vol. 11, no. 1, pp. 116-130, 2009.

[49] P. Kolodzy, "Next generation communications: Kickoff meeting," in *Proc. DARPA,* 2001, .

[50] L. Drozd, "Computational electromagnetics applied to analyzing the efficient utilization of the RF transmission hyperspace," in *Proc. IEEE/ACES Int. Conf.* 2005, pp. 1077-1085.

[51] H. Tang, "Some physical layer issues of wide-band cognitive radio systems," in *2005 1st IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, DySPAN 2005,* 2005, pp. 151-159.

[52] F. F. Digham, M. -. Alouini and M. K. Simon, "On the energy detection of unknown signals over fading channels," *IEEE Trans. Commun.,* vol. 55, no. 1, pp. 21-24, 2007.

[53] T. Yucek and H. Arslan, "Spectrum characterization for opportunistic cognitive radio systems," in *Military Communications Conference,* 2006, pp. 1-6.

[54] S. Shankar, C. Cordeiro and K. Challapali, "Spectrum agile radios: Utilization and sensing architectures," in *Proc. IEEE DySPAN,* 2005, pp. 160-169.

[55] Q. Peng, K. Zeng, J. Wang and S. Li, "A distributed spectrum sensing scheme based on credibility and evidence theory in cognitive radio context," in *IEEE 17th International Symposium on Personal, Indoor and Mobile Radio Communications,* 2006, pp. 1-5.

[56] E. Axell, G. Leus, E. G. Larsson and H. V. Poor, "Spectrum sensing for cognitive radio : State-of-the-art and recent advances," *IEEE Signal Process. Mag.,* vol. 29, no. 3, pp. 101-116, 2012.

[57] A. Fehske, J. Gaeddert and J. H. Reed, "A new approach to signal classification using spectral correlation and neural networks," in *2005 1st IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, DySPAN 2005,* 2005, pp. 144-150.

[58] T. Farnham, G. Clemo, R. Haines, E. Seidel, A. Benamar, S. Billington, N. Greco, N. Drew, Truong Hong Le, B. Arram and P. Mangold, "IST-TRUST: A perspective on the reconfiguration of future mobile terminals using software download," in *IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, PIMRC,* 2000, pp. 1054-1059.

[59] J. Palicot and C. Roland, "A new concept for wireless reconfigurable receivers," *IEEE Commun. Mag.,* vol. 41, no. 7, pp. 124-132, 2003.

[60] A. Sahai, R. Tandra, S. M. Mishra and N. Hoven, "Fundamental design tradeoffs in cognitive radio systems," in *Proc. of Int. Workshop on Technology and Policy for Accessing Spectrum,* 2006, .

[61] R. Tandra and A. Sahai, "Fundamental limits on detection in low SNR under noise uncertainty," in *2005 International Conference on Wireless Networks, Communications and Mobile Computing,* 2005, pp. 464-469.

[62] D. Cabric, S. M. Mishra and R. W. Brodersen, "Implementation issues in spectrum sensing for cognitive radios," in *Conference Record - Asilomar Conference on Signals, Systems and Computers,* 2004, pp. 772-776.

[63] K. Challapali, S. Mangold and Z. Zhong, "Spectrum agile radio: Detecting spectrum opportunities," in *Proc. Int. Symp. Advanced Radio Technologies,* 2004, pp. 61-65.

[64] Z. Tian and G. B. Giannakis, "A wavelet approach to wideband spectrum sensing for cognitive radios," in *Proc. IEEE Int. Conf. Cognitive Radio Oriented Wireless Networks and Commun. (Crowncom),* 2006, pp. 1054-1059.

[65] Y. Hur, J. Park, W. Woo, K. Lim, C. -. Lee, H. S. Kim and J. Laskar, "A wideband analog multi-resolution spectrum sensing (MRSS) technique for cognitive radio (CR) systems," in *Proceedings - IEEE International Symposium on Circuits and Systems,* 2006, pp. 4090-4093.

[66] R. Umar and A. U. H. Sheikh, "A comparative study of spectrum awareness techniques for cognitive radio oriented wireless networks," *Phys. Commun.,* vol. 9, pp. 148-170, 2013.

[67] M. T. Masonta, M. Mzyece and N. Ntlatlapa, "Spectrum decision in cognitive radio networks: A survey," *IEEE Commun. Surveys & Tutorials,* vol. 15, no. 3, pp. 1088-1107, 2013.

[68] M. B. Pursley and T. C. Royster IV, "Low-complexity adaptive transmission for cognitive radios in dynamic spectrum access networks," *IEEE J. Select. Areas Commun.,* vol. 26, no. 1, pp. 83-94, 2008.

[69] C. Peng, H. Zheng and B. Y. Zhao, "Utilization and fairness in spectrum assignment for opportunistic spectrum access," *Mobile Networks and Applications,* vol. 11, no. 4, pp. 555-576, 2006.

[70] R. Menon, R. M. Buehrer and J. H. Reed, "Outage probability based comparison of underlay and overlay spectrum sharing techniques," in *2005 1st IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, DySPAN 2005,* 2005, pp. 101-109.

[71] F. Khozeimeh and S. Haykin, "Self-organizing dynamic spectrum management for cognitive radio networks," in *CNSR 2010 - Proceedings of the 8th Annual Conference on Communication Networks and Services Research,* 2010, pp. 1-7.

[72] H. Zheng and C. Peng, "Collaboration and fairness in opportunistic spectrum access," in *IEEE International Conference on Communications,* 2005, pp. 3132-3136.

[73] Q. Yu, "A Survey of Cooperative Games for Cognitive Radio Networks," *Wireless Personal Communications,* pp. 1-18, 2013.

[74] J. Elias, F. Martignon, A. Capone and E. Altman, "Non-cooperative spectrum access in cognitive radio networks: A game theoretical model," *Computer Networks,* vol. 55, no. 17, pp. 3832-3846, 12/1, 2011.

[75] S. M. M. Toroujeni, S. M. -. Sadough and S. A. Ghorashi, "An auction-based approach for spectrum leasing in cognitive radio networks," in *2011 Wireless Advanced, WiAd 2011,* 2011, pp. 106-109.

[76] D. Xu, X. Liu and Z. Han, "Decentralized bargain: A two-tier market for efficient and flexible dynamic spectrum access," *IEEE Trans. Mobile Comput.,* vol. 12, no. 9, pp. 1697-1711, 2013.
[77] Q. Ni and C. C. Zarakovitis, "Nash bargaining game theoretic scheduling for joint channel and power allocation in cognitive radio systems," *IEEE J. Select. Areas Commun.,* vol. 30, no. 1, pp. 70-81, 2012.
[78] W. Saad, Z. Han, R. Zheng, A. Hjørungnes, T. Basar and H. V. Poor, "Coalitional games in partition form for joint spectrum sensing and access in cognitive radio networks," *IEEE J. Sel. Topics Signal Process.,* vol. 6, no. 2, pp. 195-209, 2012.
[79] X. Hao, M. H. Cheung, V. W. S. Wong and V. C. M. Leung, "Hedonic coalition formation game for cooperative spectrum sensing and channel access in cognitive radio networks," *IEEE Trans. Wireless Commun.,* vol. 11, no. 11, pp. 3968-3979, 2012.
[80] M. Cheminod, L. Durante and A. Valenzano, "Review of Security Issues in Industrial Networks," *IEEE Trans. Ind. Informat.,* vol. 9, no. 1, pp. 277-293, 2013.
[81] A. G. Fragkiadakis, E. Z. Tragos and I. G. Askoxylakis, "A Survey on Security Threats and Detection Techniques in Cognitive Radio Networks," *IEEE Commun. Surveys & Tutorials,* vol. 15, no. 1, pp. 428-445, 2013.
[82] S. E. Frankel, B. Eydt, L. Owens and K. A. Scarfone, "SP 800-97. establishing wireless robust security networks: A guide to IEEE 802.11i," National Institute of Standards & Technology, Tech. Rep. 2206307, 2007.
[83] National Security Agency. (2015, Feb). *NSA's Information Assurance Definition*. Available: http://www.nsa.gov/ia/.
[84] G. Baldini, T. Sturman, A. R. Biswas, R. Leschhorn, G. Gódor and M. Street, "Security aspects in software defined radio and cognitive radio networks: A survey and a way ahead," *IEEE Commun. Surveys & Tutorials,* vol. 14, no. 2, pp. 355-379, 2012.
[85] S. P. Herath, N. Rajatheva and C. Tellambura, "Energy detection of unknown signals in fading and diversity reception," *IEEE Trans. Commun.,* vol. 59, no. 9, pp. 2443-2453, 2011.
[86] C. Clancy, J. Hecker, E. Stuntebeck and T. O'Shea, "Applications of machine learning to cognitive radio networks," *IEEE Wireless Communications,* vol. 14, no. 4, pp. 47-52, 2007.
[87] W. Wang, H. Li, Y. Sun and Z. Han, "Attack-proof collaborative spectrum sensing in cognitive radio networks," in *Proceedings - 43rd Annual Conference on Information Sciences and Systems, CISS 2009,* 2009, pp. 130-134.
[88] A. W. Min, K. G. Shin and X. Hu, "Attack-tolerant distributed sensing for dynamic spectrum access networks," in *Proceedings - International Conference on Network Protocols, ICNP,* 2009, pp. 294-303.
[89] N. Nguyen-Thanh and I. Koo, "An enhanced cooperative spectrum sensing scheme based on evidence theory and reliability source evaluation in cognitive radio context," *IEEE Commun. Lett.,* vol. 13, no. 7, pp. 492-494, 2009.
[90] A. De Domenico, E. Calvanese Strinati and M. -. Di Benedetto, "A survey on MAC strategies for cognitive radio networks," *IEEE Commun. Surveys & Tutorials,* vol. 14, no. 1, pp. 21-44, 2012.

Tapiwa M. Chiwewe (S'09-M'13) received the B.Eng. and M.Eng. degrees in computer engineering from the University of Pretoria, Pretoria, South Africa, in 2006 and 2010, respectively. He is currently pursuing the Ph.D. degree in computer engineering from the Advanced Sensor Network Group, University of Pretoria.

He is a Senior Research Engineer with the Council for Scientific and Industrial Research, Pretoria. His research interests include wireless sensor networks and cognitive radio networks.

Colman F. Mbuya received the B.Eng. degree in computer engineering from the University of Pretoria, Pretoria, South Africa, in 2013 where he is currently pursuing the M.Eng. degree in computer engineering.

He is working as an Information Security Consultant with MWR InfoSecurity, Johannesburg, South Africa. His research interests include spectrum allocation and data security for wireless sensor networks, as well as mobile and web application security.

Gerhard. P. Hancke (S'99–M'07–SM'11) received the B.Eng. and M.Eng. degrees in computer engineering from the University of Pretoria, Pretoria, South Africa, in 2002 and 2003, and the Ph.D. degree in computer science from the Security Group, Computer Laboratory, University of Cambridge, Cambridge, U.K., in 2008.

He is an Assistant Professor with the City University of Hong Kong, Kowloon, Hong Kong. His research interests include system security, embedded platforms, and distributed sensing applications.