Journal of Network and Computer Applications 97 (2017) 140–156

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

journal homepage: www.elsevier.com/locate/jnca

A survey of cognitive radio handoff schemes, challenges and issues for industrial wireless sensor networks (CR-IWSN)

Stephen S. Oyewobi[a,*], Gerhard P. Hancke[a,b]

[a] Department of Electrical, Electronic and Computer Engineering, University of Pretoria, South Africa
[b] Department of Computer Science, City University of Hong Kong, Kowloon, Hong Kong

ARTICLE INFO

Keywords:
Cognitive radio
Industrial wireless sensor network
Opportunistic use
Spectrum handoff
Quality of service

ABSTRACT

Industrial wireless sensor network (IWSN) applications are mostly time-bound, mission-critical and highly delay sensitive applications therefore IWSN defines strict, stringent and unique QoS requirements such as timeliness, reliability and availability. In IWSN, unlike other sensor networks, late arrival of packets or delay or disruption to an on-going communication are considered as critical failure. Also, because IWSN is deployed in the overcrowded industrial, scientific, and medical (ISM) band it is difficult to meet this unique QoS requirements due to stiff competition for bandwidth from other technologies operating in ISM band resulting in scarcity of spectrum for reliable communication and/or disruption of ongoing communication. However, cognitive radio (CR) provides more spectral opportunities through opportunistic-use of unused licensed spectrum while ensuring minimal interference to licensed users. Similarly, spectrum handoff, which is a new type of handoff in cognitive radio, has the potential to offer increase bandwidth, reliable, smooth and interference-free communication for IWSNs through opportunistic-use of spectrum, minimal switching-delays, and efficient target channel selection strategies as well as effective link recovery maintenance. As a result, a new paradigm known as cognitive radio industrial wireless sensor network (CR-IWSN) has become the interest of recent research efforts. In this paper, we highlight and discuss important QoS requirements of IWSN as well as efforts of existing IWSN standards to address the challenges. We discuss the potential and how cognitive radio and spectrum handoff can be useful in the attempt to provide real-time reliable and smooth communication for IWSNs.

1. Introduction

Advancements in wireless technologies have created a proliferation of high-end wireless devices and generated huge competition for RF spectrum (Trigui et al., 2013; Yang et al., 2015a). According to FCC regulations, only a licensed user has exclusive right to utilize the licensed band of the radio spectrum. This method of static spectrum access and underutilization of licensed radio spectrum by licensed user has created the perception of “Spectrum Scarcity”. However, spectrum scarcity is not as a results of the physical scarcity of usable radio spectrum but rather of inadequate spectrum management policies (Christian et al., 2012; Liu et al., 2008). FCC puts radio spectrum usage in the range of 15–85% and spectrum underutilization as large as 85% in space, time and location (Liu et al., 2008; Maheshwari and Singh, 2014; Wyglinski et al., 2008). Therefore, the challenge of spectrum scarcity requires a dynamic spectrum access (DSA) solution where available radio spectrum can be utilized opportunistically. Such candidate solution will ensure that spectrum is use more efficiently and reliable communication are provide ubiquitously (Chiwewe et al., 2015). To address this problem, a new paradigm is being proposed in literature and identified as cognitive radio. Cognitive radio (CR) is a radio that makes opportunistic-use of radio spectrum by dynamically adjusting its radio operating parameters and autonomously modifying system operation through sensing of its operational electromagnetic environment (Chiwewe et al., 2015). In CR terminology, the primary user (PU) is the licensed high priority user of the licensed radio spectrum with legacy right to the spectrum band. In contrast, the secondary user (SU) an unlicensed lower priority user, also known as cognitive radio user (CR user) is an opportunistic-user of the radio spectrum. SU utilizes the radio spectrum opportunistically by identifying unused spectrum space known as spectrum hole or white space (Chen and Hong, 2013). Reports from FCC and shared spectrum company indicates that white spaces exist in licensed spectrum band accordingly by FCC regulations unlicensed user can now use TV white spaces for their communication (Bhushan et al., 2015; Chen and Hong, 2013; Liu et al., 2008). In line with the vision of the FCC, the IEEE

---

* Corresponding author.
E-mail addresses: oyewobistephen@gmail.com (S.S. Oyewobi), ghancke@gmail.com (G.P. Hancke).

http://dx.doi.org/10.1016/j.jnca.2017.08.016
Received 25 April 2017; Received in revised form 18 July 2017; Accepted 25 August 2017

802.22 WRAN was developed as a license-exempt standard to use cognitive radio for wireless access to TV white space (TVWS) (Chen and Hong, 2013; Chiwewe et al., 2015). The industrial, scientific, and medical (ISM) unlicensed band where industrial wireless sensors network (IWSN) nodes are deployed together with Wi-Fi and Bluetooth devices has become overcrowded resulting in intense competition for available bandwidth in the ISM band. In addition, unlike traditional wireless sensor networks (WSNs) (Nellore and Hancke, 2016a, 2016b), IWSNs define stricter and stringent QoS requirements (Bara et al., 2015; Baviskar et al., 2015; Dobslaw et al., 2015; Kruger et al., 2015; Nagarajan and Dhanasekaran, 2015; Papadopoulos, 2015). To meet these goals, different working groups such as WINA, ISA, and the ZigBee working groups have developed various industrial standards including WIA-PA, ISA100.11a, WirelessHART, and ZigBee (Batista et al., 2012; Chung et al., 2015; Evans-Pughe, 2003; Miao et al., 2010; Tang et al., 2010; Yang and Dong-Seong, 2013) for specific industrial applications QoS requirements. Similarly, the potentials of cognitive radio to benefit IWSNs QoS requirements to alleviate interference caused by congestion experienced on the ISM band has also been recognized and a new paradigm known as cognitive radio industrial wireless sensor network (CR-IWSN) has become the interest of recent research efforts. To achieve this goal, however, requires integrating dynamic spectrum access (DSA) potentials advanced for cognitive radio into IWSN nodes. Cognitive radio and DSA makes every sensor in IWSN a cognitive sensor node and enables it to recognize unused channels in overcrowded band as well as to be able to make opportunistic use of the channel for communication. Conversely, the pre-emptive priority to the channel belongs to the PU (licensed user) who needs not inform the SU (CR user) before it reclaims the channel. Therefore for CR-IWSN optimal performance, SU subjugates licensed spectrum space with minimal interference to the licensed user and must vacate previously occupied channel at the arrival of a PU and concludes on-going communication at a target unoccupied channel (Chakraborty and Misra, 2015; Chen and Hong, 2013; Kaur et al., 2009). This process is known as spectrum handoff. Unlike consumer and simple sensing WSN (Opperman and Hancke, 2011; Potter et al., 2013), timeliness, precision, reliable and stable communication are unique QoS requirements of IWSN systems and applications because most IWSN applications are time-bound as well as mission-critical (Cheng et al., 2016; Silva et al., 2015; Silva and Hancke, 2016). Therefore, reliable and stable communication is of critical importance and top priority in IWSNs (Kumar et al., 2014; Phala et al., 2016). For instance, in industrial automation; precision and timeliness are important and in industrial monitoring; availability, reliability, delay-intolerance, and robustness of communication links are key (Abu-Mahfouz and Hancke, 2011; Silva and Hancke, 2016). Yet, these requirements can be relatively difficult to achieve when operating in the ISM band due to interference and overcrowding which result in continuous switching, high latency due to switching, reduced link capacity and disruption of on-going communications. However, spectrum handoff can offer increase bandwidth, reliable, smooth and interference-free communication for IWSNs through opportunistic-use of spectrum, minimal switching-delays, and efficient target channel selection strategies as well as effective link recovery maintenance. A well-planned and designed spectrum handoff technique will provide reliable communication by reducing number of spectrum handoffs and maintaining quality communication link for IWSN systems and applications. As important as this topic is, only few research efforts have focused on spectrum handoff for IWSN. Our objective in this paper is to draw attention and focus to this important topic. The rest of the paper is organized as follows; in Section 2 we introduce industrial systems and applications, then we discuss CR-IWSN in Section 3, thereafter, we discuss IWSN requirements in Section 4, industrial systems and a review of existing industrial standards are presented in Sections 5 and 6 respectively. In Section 7 we introduce cognitive radio and in Section 8 we explain how DSA can benefit IWSN, spectrum handoff strategies and metrics are discussed in Sections 9 and 10 respectively. In Section 11, we introduce some spectrum algorithms, Sections 12–14 discuss non-DSA related functionalities, related works and future directions respectively and we conclude in Section 15.

2. Industrial systems and applications

There are several attempts to classify industrial systems and applications by different working groups such as WINA, ISA, and the ZigBee working groups. Most classifications are based on functions perform by different industrial systems and applications e.g. industrial automation, industrial monitoring, safety, process control, automobile, aerospace, space mission, and manufacturing. ISA classification however, is based on criticality of data sensed, monitored, or transmitted by wireless sensor nodes and operational requirements of industrial systems and applications deployed to area of interest, as follows; safety systems, closed loop regulatory systems, closed loop supervisory systems, closed loop control systems, alerting system and information gathering systems, which we have discussed in Section 5. Nonetheless, sometimes actions of different classes of systems described are interweaved, for instance, when sensor nodes are deployed in real-life IWSN environments they may perform more than one role e.g. alerting objective in a temperature monitoring system is un-critical primarily, but when the monitored temperature rise above a threshold level, the alerting system may be mandated to act as a safety system. For this reason, the previously mentioned classes of systems above can be categorize into three major industrial systems as follows; (1) safety systems, (2) control systems and (3) monitoring systems (Ban et al., 2016);

1. Safety systems

   Fire safety is one important domain where WSN have been deployed. WSN systems installed in this area bring important features such as real-time and close monitoring of fire fighters, including early responders like police, and paramedics during fire hazards. For industrial domain application, safety systems are deployed in potentially dangerous application such as nuclear plants, and furnace monitoring. For safety of the systems, applications and personnel in this category especially in the nuclear plants, prognostic monitoring/maintenance rather than diagnostic measures will prevent major problem and disaster due to ageing of components used in plants.
2. Control systems

   This category comprises of the closed loop and open loop systems mentioned above, the closed loop system can further be divided into; process control and factory automation. Process control systems usually have delay requirements of less than 100 ms and are mainly for monitoring and actuation. Factory automation on the other hand, has stricter delay requirements in the range of 2–25 ms e.g. in robotics for robot control. Open loop systems are identical to closed loop systems though it includes a human in the loop to activate the control actions.
3. Monitoring systems

   This category comprises of the last two classes mentioned in the general classification i.e. alerting and information gathering systems. WSN nodes deployed for these systems have minimum requirements and extensive field of operations. These include fields such as environmental monitoring e.g. forest fire detection, flood detection, pollution study, and healthcare monitoring e.g. for prognostics and remote-monitoring of patients and their vital data as well as for tracking of doctors in the hospital, and also for traffic monitoring e.g. movement tracking (Hu et al., 2008), including military applications e.g. battle damage assessment. These systems collect data over a long period in a given location and these data are studied to arrive at a conclusion.

Table 1
Summary of the different industrial systems and QoS requirements.

Industrial System	Categories	QoS requirements	Delay tolerance
Safety systems	Safety systems e.g. Alarm systems	Timeliness, and availability	$\leq 100\ ms$
Control systems	Closed loop and Open loop systems, process control and factory automation	Timeliness, reliability, availability, and energy efficiency	$\leq 25\ ms$
Monitoring systems	Alerting systems and information gathering systems	Reliability, availability, energy efficiency and load balancing	$\leq 100\ ms$

Table 1 shows delay sensitivity, reliability, availability and timeliness as QoS requirements of industrial systems, these are strict and stringent QoS requirement difficult to achieve when operating in environments such as industrial environments where noise, interference and overcrowding are relatively and significantly high, however, with a well-designed spectrum handoff scheme with minimum delay tolerance these QoS requirements can be achieved.

3. Cognitive radio industrial wireless sensor network

Conventional wireless technology has experienced tremendous growth and has gained massive deployment for small and home offices as well as enterprise offices. However, it has experienced limited application for industrial installations due to certain peculiarities of the industrial wireless sensor network domain like; (a) harsh environment, (b) interference and electromagnetic compatibility, (c) safety and security constraints and (d) battery autonomy (Zhuo et al., 2015a). Though, issues relating to IWSN applications such as process automation and manufacturing industries may not have been addressed by existing wireless technology due to their unique requirements. IWSN can benefit from the flexibilities that cognitive radio offers e.g. real-time surveillance applications like tracking that requires minimum communication delay can benefit from design of adaptive spectrum handoff scheme with minimum switching handoff latency. Similarly, to offer cognitive radio flexibilities for IWSN an area known as cognitive radio industrial wireless sensor network (CR-IWSN) has emerged, this paradigm started a few years ago and the major addition of CR-IWSN to IWSN is that each sensor in the IWSN is a CR sensor node (Zhuo et al., 2015b). Fig. 1 shows a typical CR-IWSN architecture. The reasons leading to the applications of CR to industrial wireless sensor network have been identified as follows:

1. The ISM band where the industrial wireless sensor technology like WIA-PA, ISA100.11a, WirelessHART, and ZigBee are deployed with other wireless technology such as IEEE 802.15.4 or Bluetooth, IEEE 802.11 WLANs has become overcrowded creating intense competition for available bandwidth in the ISM band (Zhuo et al., 2015a);
2. The potential of cognitive radio to provide more spectral space by opportunistic spectrum-use instead of spectrum leasing which involves complex negotiation and high cost, therefore contradictory to the low-cost QoS requirements of IWSNs (Dobslaw et al., 2015);
3. The potential of cognitive radio to achieve better spectral and energy efficiency as CR sensor nodes can exploit unused spectrum and periods of PUs and
4. CR can achieve better communication range because of CR sensor nodes capabilities to operate in lower frequency bands (Zhuo et al., 2015a)

Unlike traditional wireless sensor networks (WSNs), industrial wireless sensor network (IWSNs) are different in terms of their QoS requirements (Oualha et al., 2012). In Section 5, we discuss industrial networks applications and their requirements, which include reliability, availability, timeliness, and interference mitigation that needs to be met in industrial environments. Noise and interference impose a constraint on the performance of IWSN applications and makes it difficult to meet these requirements. Typical interference effects in IWSN environments include; data loss, transmission delay, false alarm, false command, jitters, and loss of synchronizations (Ban et al., 2016). Similarly, strong multi-path and fast channel variations characteristics of industrial environments leads to packet loss and high latency (Zheng et al., 2012). Therefore, without a reliable and efficient communication protocol, the performance of IWSNs are degraded resulting in shortened network lifetime, decreased propagation speed and increased packet loss rate (Yu et al., 2013).

4. IWSN requirements

Industrial wireless sensor network defines some requirements that industrial standards are expected to meet, we give a brief review of these requirements below:

1. Minimal cost and compactness

   For large-scale deployment of IWSNs, low-cost and compact sensor nodes are essential (Heng et al., 2010), cost in this case includes; implementation cost, replacement and logistics costs, training and servicing cost. Compactness aids in decreasing space for installation of large-scale network of nodes as well as saving cost (Oualha et al., 2012).
2. Self-configuration and self-organization

   Due to the large scale of network nodes in most IWSNs as well as failure/mobility and temporal power down of nodes in the network, topology is not always static. Mobile nodes as well as failed nodes makes the topology dynamic, however, by using self-configurable IWSNs, failed sensor nodes can be replaced by new sensors and existing nodes can be ejected without distorting the main objective of the application (Heng et al., 2010). Nodes are also required to operate (self-organize and self-configure) with minimum human intervention when deployed in crucial locations that may not be easily approachable e.g. WSN node installed in severe conditions such as dangerously cold weather or near massive machines operating at extreme temperature including nuclear plants and mines for monitoring (Oualha et al., 2012). Cognitive radio functionality of reconfiguration can be of benefit to IWSN in this regard.
3. Efficient protocols and scalable architectures

   Heterogeneous industrial applications usually deployed within the same infrastructure have different QoS requirements, therefore, IWSNs architecture should be scalable and robust enough to support applications with different requirements without degradation in QoS (Oo et al., 2013). Systems flexibility, robustness and reliability can improve when systems are designed in module and layers. Similarly, scalability can be enhanced when new industrial systems are interoperable with existing legacy solutions like fieldbus and Ethernet-based systems (Heng et al., 2010).
4. Resistance to noise and co-existence

   Industrial environments are usually noisy and contain heterogeneous networks deployed side by side with machineries and communications systems. This create interference to IWSN signal since it operates on low-power signal and are very sensitive to noise increasing path loss. IWSN standards should efficiently withstand and work properly in the presence of interference (Oualha et al., 2012). IWSN nodes with cognitive capabilities should be able to manage challenges relating to co-existence in the ISM band, which are caused by interference.
5. Low-delay

   Industrial wireless systems especially closed loop regulatory systems are highly sensitive to delay. IWSN communication are

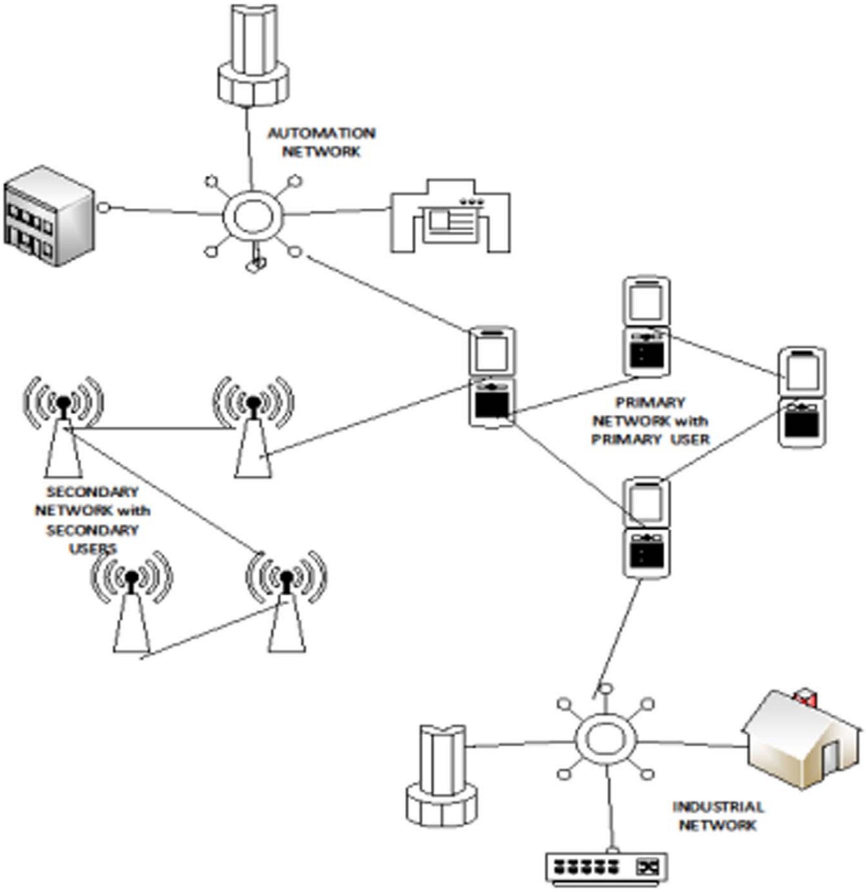


Fig. 1. CR-IWSN architecture (Zhuo et al., 2015b).

required to have real-time guarantees and predictable behaviour. Interference-mitigating or interference-controlled cognitive behaviour or adaptive protocols with cross-layer solutions can reduce communication latency for IWSNs. We have only discussed IWSN requirements that can benefit from cognitive radio capabilities and solutions. Kumar and Hancke (2014), Kumar et al. (2014) should be seen for IWSN requirements, protocols and challenges for details.

5. Industrial systems and requirements

We begin by looking at classification of industrial systems based on the ISA classification. ISA classifies industrial systems based on criticality of data and operational requirements as follows (Ban et al., 2016):

1. Safety systems

   These include e.g. fire alarm systems where nodes are usually stationary and are installed in a uniform pattern around the area of interest to traverse the entire area. In this case, action is triggered by events and is usually immediate- in the order of milliseconds or seconds -. QoS requirements for safety systems includes time bounded delivery, reliability, and availability. Event-based protocol should be developed for transport and routing functions to meet these QoS (Oualha et al., 2012). A QoS-based multipath routing protocol like MMSPEED and well-designed handoff schemes are good solution. Also safety systems can benefit from MAC solution like ER-MAC, which is a custom built MAC for emergency response (Oualha et al., 2012).
2. Closed loop regulatory systems

   These are systems where periodic measurements are taken based on occurrence of an events and these measurements are sent to a controller intermittently, then based on this, a controller formulate a decision and sends it to an actuator which acts according to the decision. In other words, closed loop regulatory systems are systems where feedbacks are used to regulate operations of the system. Periodic measurements and strict timing are critical to the smooth operations of these systems than the safety systems. For these systems, timely delivery, availability, reliability, and energy efficiency are important QoS requirements. A stable and energy-aware spectrum handoff scheme, which has reliable and timely switching with minimum failure probability, is important here. For the transport layer functions, a real-time protocol would be appropriate; an example is RT2 a real-time protocol developed for WSAN (Oualha et al., 2012).
3. Closed loop supervisory systems

   Unlike close loop regulatory systems, here, feedbacks/measurements are non-critical and non-periodic but are based on events. An example of this category are systems that gather statistical data and reacts base on observation of an established tendency, which relates to an event. QoS requirements are similar to closed regulatory systems requirements, however, comparatively less critical. Therefore, handoff schemes and MAC solutions that are time-bounded efficient and energy-efficiency aware like QoS-MAC and PEDAMACS are potential or candidate solutions (Oualha et al., 2012).
4. Open loop control systems

   These categories of systems are similar to the closed loop systems, but in this case, wireless sensor nodes are only duty-bound to assemble and transfer data to a central database. A human operator is responsible for analyzing the data, and based on this, undertakes required measures if any measures are required. Data communicated by nodes in the open loop system are not time-bound or time-critical data due to the human control in the loop. e.g. the security application of WSN for detection and classification of threat in a geographical location and transmission of the information about the threat, to a distant observer (a human) for investigation through internet (Oloyede and Hancke, 2016; Dobslaw et al., 2015). Protocols and schemes for handoff and routing that are event-based, energy-efficient and decentralized would be appropriate as candidate schemes for these categories based on the QoS defined by these systems (Ban et al., 2016) TEEN/APTEEN are suitable routing and MAC solutions that have been developed for similar scenarios (Oualha et al., 2012).

5. Alerting systems

   These include e.g. systems with regular or event-triggered alerting systems like WSN for prolonged observation of temperature in a furnace where alarms or beeps are triggered at different stages of the work to indicate completion of that part of the work. Requirements here are similar to safety systems requirements although no emergency actions are involved, and it includes; reliability, availability, and energy efficiency (Oualha et al., 2012).

6. Information gathering systems

   These include e.g. in industrial perspective, WSN nodes installed in an area of interest to gather information such as temperature and moisture for a definitive duration of time. In battlefield, WSN application for battlefield supervision to observe activities of rival forces on dangerous terrain, approach route and path. After a long period of time this information can then be analyze to arrive at a long term plans for controlling these parameters in the case of industry or arriving at decision like intelligent targeting via intelligent ammunition equipped with WSNs in battlefields. QoS requirements for this category of systems include energy efficiency and load balancing since this system are installed to collect data on deployed area for long period. Efficient energy clustering and routing schemes (Ban et al.), as well as energy-aware handoff and MAC protocols should be developed for this category of WSN systems (Oualha et al., 2012).

6. Review of some IWSN standards

IWSN is expected to meet some basic requirements such as high reliability, low latency, low power, easy deployments and maintenance, and self-healing. To address these challenges of the IWSN some working groups such as the wireless industrial networking alliance (WINA), ZigBee Alliance, HART communication foundation (HCF), Chinese industrial wireless alliance and ISA 100 have attempted to define and establish industrial wireless technology standards such as ZigBee, WirelessHART, WIA-PA, and ISA100.11a. All these standards are based on IEEE 802.15.4 standard and design for different application domains (Al Agha et al., 2009; Kumar S et al., 2014). In this section, we attempt a brief review of the existing industrial wireless technologies.

6.1. WIA-PA

WIA-PA (Wireless Network for Industrial Automation- Process Automation) is an industrial standard proposed in 2007 by the Chinese industrial alliance aimed at designing a real-time, highly reliable, energy efficient, anti-interference, and intelligent multi-hop WSN and harsh industrial environments solution (Du and Liu, 2010; Heng et al., 2010; Hua et al., 2009; Kumar et al., 2014; Miao et al., 2010; Tang et al., 2010; Xin et al., 2011). It is based on the ISO/OSI network model, however, only the physical layer, data link layer network layer, and application layer are defined in the WIA-PA protocol stack (Du and Liu, 2010; Xin et al., 2011). WIA-PA is fully compatible with the IEEE802.15.4 standard for process measurement, monitoring, and control of wireless networks and it is reactive to dynamic changes in network conditions through self-organizing and self-healing mesh network design (Kumar Kumar S et al., 2014 et al., 2014). It supports spread spectrum, narrowband and multi-channel communications. At the MAC layer, it uses the following technologies for medium access including CSMA, TDMA, and FDMA (Du and Liu, 2010; Kumar et al., 2014). WIA-PA supports two network topology structures; a hierarchical network topology, which combines a star and mesh, or star network topology (Du and Liu, 2010; Heng et al., 2010; Xin et al., 2011). It supports and employs three types of frequency hopping i.e. adaptive frequency switch, adaptive frequency hopping and timeslot hopping and has 16 communication channels in 2.4 GHz frequency band. It offers support and is inter-operable with WirelessHART and also supports inter-operability with other application standards like Probus, and Modbus (Kumar et al., 2014). Security is handle at both the data link and application layers in WIA-PA, however, security features are optional (Liang et al., 2011). WIA-PA depends on the security manager to supervise the management of security keys, authenticate gateway and handle field devices. Security services on the terminals/nodes are handle on a point-to-point framework on the data link and end-to-end at the application layer.

6.2. WirelessHART

WirelessHART was ratified by the HCF in September 2007 as the first open communication standard designed especially for process measurement as well as control applications as specified in the HART protocol specification revision 7.0 (Al Agha et al., 2009; Chen et al., 2014; Chung et al., 2015; Nobre et al., 2014; Soto et al., 2014; Petersen and Carlsen, 2011; Zhu et al., 2009; Song et al., 2008). WirelessHART is compatible with the IEEE802.15.4-2006 physical layer and operate at the 2.4 GHz frequency band with 15 channels (Kumar et al., 2014). Prior to the release of WirelessHART, other standards relating to office and manufacturing automation such as ZigBee and Bluetooth were operational, but these standards could not match the strict and tight QoS requirements as well as higher security concerns of industrial applications (Song et al., 2008). For instance, ZigBee and Bluetooth are not designed to provide guaranteed end-to-end wireless communication delay and therefore could not be deployed for monitoring applications that are required to forward updates from sensors every one second. In addition, industrial environments are prone to more interferences and obstacles due to the harsh environment compared with office environments. ZigBee does not have a built-in channel hopping technique and therefore will fail in harsh industrial environments (Song et al., 2008). WirelessHART adopts some unique features, which includes a Time Synchronized Mesh Protocol (TSMP) for medium access control and network layer (Chen et al., 2014; Kumar et al., 2014). TSMP uses TDMA technology to provide a collision free and deterministic communication, therefore, provides reliability of 99.9%, which makes it robust in noisy and harsh environments as well as for critical applications (Chen et al., 2014; Kumar et al., 2014; Song et al., 2008). Notably among WirelessHART MAC layer features is channel hopping, a network wide time synchronization, channel blacklisting, a strict $10\ ms$ time slot, and industry standard AES-128 cipher and keys (Song et al., 2008). Though, WirelessHART does not have any energy-aware ad-hoc routing strategy in its network layer (Al Agha et al., 2009) however, its network layer does have a self-organizing and self-healing mesh networking technique (Song et al., 2008) which allows it to reroute messages around interference and obstacles. Another distinguishable feature of WirelessHART is that it maintains a central network manager, duty-bound to keeping up-to-date routes and communication registry for the network and therefore guarantees network performance. Unlike ZigBee that uses only a star topology (Jindal and Verma, 2015), WirelessHART topology adopts a cluster, a mesh or a star topology, and therefore can be used for large and scalable industrial control systems. WirelessHART does support legacy systems that operate on wired HART framework (Kumar et al., 2014; Song et al., 2008) and unlike WIA-PA, in WirelessHART features relating to security are compulsory, it is the duty of the security manager to generate and store all keys by the security services. Security is handle at the MAC as well as the network layers; on the MAC layer on one hand, data integrity is provided on a hop-by-hop basis using encryption mechanism, on the network layer on the other hand, it is provided on an end-to-end basis. The security manager handles all security services and it is enforced within the gateway device or the network manager as it usually referred to by vendors (Kumar et al., 2014; Petersen and Carlsen, 2011).

6.3. ISA100.11a

The international society of automation (ISA) initiated a task on an alliance of standards to define wireless systems for industrial automation and control applications, and the first standard to be developed by ISA was ISA100,11a and it got ratified as ISA standards in September 2009 (Petersen and Carlsen, 2011). ISA100.11a is a protocol designed for secure and reliable wireless communication for alerting, monitoring, and supervisory control, as well as open loop and close loop control applications in process and industrial automation (Akhlaghpasand and Shah-Mansouri, 2015; Kumar et al., 2014; Yang and Dong-Seong, 2013). The PHY layer of ISA100.11a is based on IEEE802.15.4 and it adopts direct-sequence spectrum spreading (DSSS), and offset-quadrature phase shift keying (O-QPSK) modulation, as well as channel hopping and channel black listing to reduces interference effects (Kumar et al., 2014; Yang and Dong-Seong, 2013). It operates on the 2.4 GHz band using IEEE802.15.4 channel 11–25, while channel 26 described as optional. Channels are spaced 5 MHz apart and have a bandwidth of 2 MHz, including a maximum date rate of 250 kbps and a maximum transmitted power of 10 mW (10 dBm) (Petersen and Carlsen, 2011; Yang and Dong-Seong, 2013). ISA100.11a combines TDMA and CSMA at the data link layer (DLL), therefore has advantages of both solutions (Kumar et al., 2014), its DLL is divided into MAC sublayer, a MAC extension and upper DLL (Petersen and Carlsen, 2011). The MAC sublayer is responsible for sending and receiving individual date frame and is a subset of IEEE802.15.4 MAC. The MAC extension supports features not included in the IEEE802.15.4 MAC by annexing more spatial, frequency and time diversity into the carrier sense multiple access with collision avoidance (CSMA-CA) mechanism (Al-Yami et al., 2013). The upper DL takes control of routing inside the DL subnet and is responsible for the link and mesh aspects above the MAC level (Petersen and Carlsen, 2011). The ISA100.11a network layer (NL) is based on the internet engineering task force (IETF) 6LoWPAN specification (Petersen and Carlsen, 2011) and is compatible with IPv6 (Kumar and Hancke, 2014) as well as offer users the opportunity to connect to the internet, and therefore offer diverse possibilities. ISA100.11 adopts mesh, star, and it can as well combine both topologies (Kumar et al., 2014; Yang and Dong-Seong, 2013) and it accommodates both the graph and source routing protocols for mesh routing (Petersen and Carlsen, 2011). The transport layer (TL) supports connectionless services through a User Datagram Protocol (UDP) over IPv6 with an option of IETF 6LoWPAN specification defined compression (Petersen and Carlsen, 2011). However, the TL does not support acknowledged transactions, but includes better data integrity checks and additional authentication as well as encryption mechanisms. Like the WirelessHART, ISA100.11a has a security manager which is inside the same physical device as the system manager and gateway, and it is duty-bound to generate, store, and distribute all requisite security keys as well as authentication. End-to-end security is handle at the transport layer and ISA100.11a supports legacy protocol like the wired HART as well as provides interface for and facilitates co-existence with WirelessHART (Kumar et al., 2014; Ray et al., 2013).

6.4. ZigBee

ZigBee is based on IEEE802.15.4-2003 dual-PHY (868 MHz/ 915 MHz and 2.4 GHz) radio technology and adopts CSMA-CA MAC layer of IEEE802.15.4 on which it defines its network layer including its application layer (Al Agha et al., 2009; Biddut et al., 2015; Jindal and Verma, 2015; Sarijari et al., 2014; Wagner and Barton, 2012). It stipulates a network layer- for multi-hop mesh-networking (Wagner and Barton, 2012) which responsibilities includes mechanism to join and leave the network, to discover and maintain routes between devices as well as to apply requisite security to frames and to route frames to their required destinations (Al Agha et al., 2009). ZigBee is designed for low-cost building and home automation, industrial control and monitoring, including energy automation and embedded sensing (Biddut et al., 2015; Gungor and Hancke, 2009; Sarijari et al., 2014; Wagner and Barton, 2012; Yan et al., 2015). Some unique characteristics of ZigBee includes definition of a lightweight protocol stack for applications which requires low latency, low cost, high security, green power, low power consumption and low data rates (up to 250 kb@ 2.4 GHz, 40kbps@915 MHz, and 20kbps@868 MHz) as well as a distance range of 10 m −70 m (Biddut et al., 2015; Firdaus and Sahroni, 2014; Guo et al., 2014; Jindal and Verma, 2015; Nomura and Sato, 2014; Rezaeirad et al., 2014). However, authors in Gungor and Hancke (2009) observed that ZigBee cannot meet some industrial QoS requirements e.g. it does not have the capacity to serve a large number of nodes within a definite cycle time. ZigBee supports a star, mesh and tree topology. IEEE802.15.4 describes two medium access techniques; the coordinated and uncoordinated modes, however, ZigBee adopts the uncoordinated mode, which requires it to listen permanently to the communication channel. Therefore, the coordinator power is usually depleted in the process; however, energy is conserved in ZigBee by enabling low-power end devices to operate in the “doze” mode (lower than 10A) and switching them to normal operating modes in less than 300 s. Another disadvantage of the ZigBee is that support for device and sink mobility is implemented by proxies (Al Agha et al., 2009). Accordingly, some solutions that have been implemented includes an extension called low-power active router protocol for incorporation into ZigBee Pro 2009 by Crossbow and Telecom Italia, other improvement includes listening periodically to reduce wake-up period and radio duty cycle (Al Agha et al., 2009). ZigBee provides and supports three types of security modes and various level of security configuration based on the needs of the application like; residential, standard and high security modes as well as methods to establish and transport keys, to protect frames, and to manage devices respectively (Rezaeirad et al., 2014). Some challenges with the security features of the ZigBee is that its key management is centralized making it vulnerable when the trust center is compromised, and also ZigBee does not guarantee tight security when the sensor network is large. Authors in Rezaeirad et al. (2014) investigate the feasibility of LEAP+ in ZigBee to address these challenges by suggesting a replacement of ZigBee management key with an alternative scheme that is symmetric, decentralized, and scalable. Their experimental results confirm that a distributed key management system such as LEAP+ offers enhancement for security and provides improved scalability. Table 2 summarizes the important features of the four IWSN standards discussed above.

7. Cognitive radio

7.1. Network architecture

Cognitive radio network architecture has been grouped into two groups based on the components in the networks as; (a) primary network and (b) secondary network (Dobslaw et al., 2015) and based on the functions by the components in the network as; (a) infrastructure-based and (b) non-infrastructure-based CR networks (Oualha

Table 2
Summary of the different industrial systems and QoS requirements.

Protocol layers	WIA-PA	Wireless HART	ISA100.11a	ZigBee
PHY layer	2.4 GHz based on IEEE802.15.4–2006	2.4 GHz radio based on IEEE802.15.4–2006	2.4 GHz radio based on IEEE802.15.4–2006	Dual PHY (868 MHz/915 MHz and 2.4 GHz) radio technology based on IEEE802.15.4–2003
MAC layer	CSMA, TDMA, and FDMA based on IEEE802.15.4–2006	TDMA MAC based on IEEE802.15.4–2006	CSMA-CA MAC based on IEEE802.15.4–2006	CSMA-CA MAC based on IEEE802.15.4–2003
Network topology	Star, Mesh	Star, Mesh	Star, Mesh	Star
Network routing technique	Static redundant routing	Graph, source, hybrid and super-frame routing	Graph routing, source, hybrid	Tree routing
Network scalability		16-bit network address, 16-bit nickname and 64-bit address	64-bit network address and 64-bit device address	16-bit node address and 16-bit group address or 64-bit extended network address
Security Features	Available on (DLL and application layer) but optional	Available on (DLL and transport layer) and Mandatory	Available on (DLL and network layer) but optional	Available

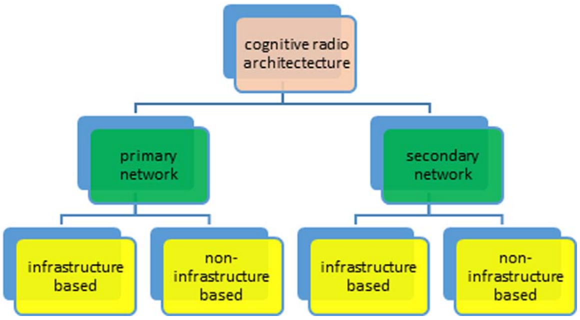


Fig. 2. Structure of cognitive radio architecture.

et al., 2012). Figs. 2 and 3 show the structure of the cognitive radio architecture and a cognitive radio network architecture respectively.

7.2. Infrastructure-based and Non-infrastructure-based Networks

Similar to cellular networks, in infrastructure-based CR network, as a standard CR nodes are responsible for spectrum sensing while the base station handles separate responsibilities including; spectrum decision, spectrum mobility and spectrum sharing (Christian et al., 2012). In non-infrastructure-based CR network, sometimes called cognitive radio ad-hoc networks (CRAHNs), CR nodes perform distributed non-centralized communication in a multi-hop pattern, therefore, CR nodes do not have a centralized entity and so, all spectrum-related functions are performed co-operatively by all nodes in the network (Christian et al., 2012). Consequently, huge traffic is generated in CRAHNs as nodes sends data through intermediate nodes and try to send information at the same time. Therefore, traffic management techniques need to be developed to meet the QoS requirements. Intelligent time-division multiple access (TDMA) scheduling can be adopted to manage heterogeneous nodes by allotting different or priority time slots to priority nodes e.g. priority can be giving to industrial wireless sensor network (IWSN) nodes in heterogeneous networks. Also, for CRAHNs to perform optimally, efficient decision-making cross-layer routing protocols needs to be developed for CRAHNs.

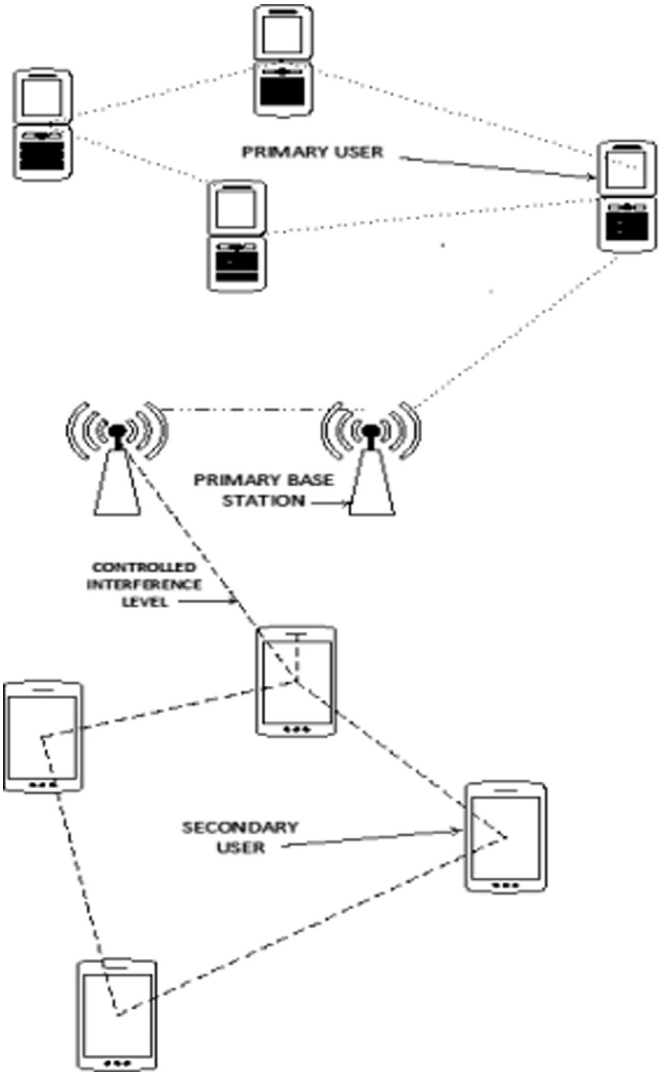


Fig. 3. Cognitive radio network architecture.

7.3. Primary network

The primary network, or existing, or licensed network is where the PU have license to use allocated spectrum band. In infrastructure-based licensed network, the PU is controlled by a primary base station, and due to its high priority in accessing spectrum, activities of the PU are not to have any interferences from the secondary user. However, due to spectrum heterogeneity of CRNs, CR users have capabilities to access the licensed spectrum held by primary users as well as the unlicensed portion of the spectrum through re-configuration of their RF front-end and wide access technology (Mukherjee and Nath, 2015). As depicted in Fig. 4. cognitive radio (CR) can make opportunistic use of spectrum through sensing of its operational electromagnetic environment and it is able to dynamically and autonomously adjust its radio operating parameters to modify system operation. Upon subjugating the licensed band, CR user other main activity is detection of the primary user. Therefore, effective and accurate spectrum sensing mechanisms should be developed that will enable CR user to able to detect signature of signal from a licensed user. CR users should release

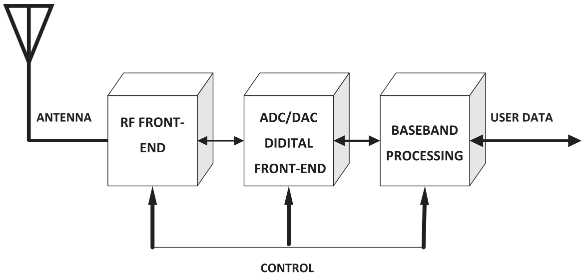


Fig. 4. CR transceiver architecture (Chiwewe et al., 2015).

a spectrum band at the time instant the activity of a PU is detected in the spectrum band previously occupied by CR users to continue communication in a new target channel. To evaluate the performance of spectrum sensing in CRN; sensing range of SU, PU activity, and PU transmission range, as well as velocity of nodes are important factors that should be considered. Authors in Rawat et al. (2015) consider the impact of SU mobility including the activities of a PU on spectrum sensing performance and develop mathematical models for both probability of miss-detection and expected overlapping time duration in cognitive vehicular networks. In IWSNs scenario, all of these parameters can be determine before a spectrum handoff scheme is designed or obtained during the implementation of the protocol e.g. the velocity of nodes in industrial scenarios are not as fast as in vehicular network and these can be factored into the design.

7.4. Secondary network

The secondary network also known as the dynamic spectrum access or unlicensed network usually have CR base station that connects CR users through single-hop connection for their communication. However, to operate in the licensed spectrum band with PU, CR user requires cognitive functionality since it does not have license and same priority as the PU to operate in a licensed band. Conversely, in the unlicensed band operation, a CR user has the same priority to access the unlicensed spectrum band as other CR users. Therefore, because numerous CR users may attempt to access the spectrum simultaneously, enhanced spectrum sharing techniques or schemes should be developed that would stimulate fair competition by CR users for unlicensed spectrum band to avert collision of CR users over corresponding portions of the spectrum. Another approach is to have spectrum brokers in the network that distributes spectrum resources between various CR networks. A fundamental concept in cognitive radio networks is network heterogeneity; CR users have prospect of accessing both CR and primary base stations. However, CR user interactions with the CR base station can be autonomous of the primary network as it occurs within the CR network through access on licensed spectrum as well as on unlicensed bands. Similarly, CR users can interact with other CR users by ad hoc connections through unlicensed band and the licensed bands. In contrast, however, CR users must access the primary network through the licensed band and requires an adaptive medium access protocol (MAC) to be implemented to enables it roam over networks with different access techniques (Dobslaw et al., 2015).

8. IWSN and dynamic spectrum access (DSA)

IWSNs usually comprise network of low power sensors installed in large numbers to monitor events that are application-dependent including time-bound and mission critical applications such as aerospace, automotive, and factory automation, or close-loop control where data delivery is strictly defined in time and reliability domains (Chiwewe and Hancke, 2016). In these applications, due to delay sensitivity of the applications, when a packet arrives late, the system treats it as a lost packet even though the packet actually arrived and an error is considered to have occurred (Rodriguez et al., 2015). Similarly, because of the low power attribute of the components nodes in IWSNs, and because they use the 2.4 GHz unlicensed ISM band also utilized by IEEE802.11b/g (WIFI) and Bluetooth devices interference among the devices in the ISM band occurs and limits IWSNs in particular (Hancke and Mbuya, 2014). For instance, Wi-Fi and Bluetooth can potentially interfere industrial network such as smart metering network and degrade performance. However, spectrum handoff can guarantee fast, reliable and real-time communication by ensuring minimum communication and switching latency (Hancke and Mbuya, 2014). For IWSNs to enjoy the benefits of spectrum handoff however, dynamic spectrum access (DSA) capabilities developed for cognitive radio have to be incorporated into IWSN nodes functionalities. Cognitive radio and DSA makes every sensor in IWSN a cognitive sensor node and gives it the ability to identify unused channels in congested band as well as to opportunistically utilize the channel for communication. The realization of DSA capabilities for IWSN requires implementing two important cognitive functionalities, which are spectrum sensing, and spectrum mobility (Ahmad et al., 2015).

8.1. Spectrum sensing

CR-based Networks impose unique challenges and diverse QoS requirements due to co-existence with PUs, and a CR user is designed to take advantage of variations in its surroundings therefore spectrum sensing becomes an important requirement for CR- based Networks (Mukherjee and Nath, 2015). Spectrum sensing is the technique that enables cognitive radio to exploit spectrum leftover opportunistically through awareness of the surroundings and cognition capabilities to adjust to their radio parameters accordingly (Zhang et al., 2016). In doing this, there are some policies, which the CR users have to respect. These are regulations concerning the amount of interference CR users can incur to the PU. One approach is the receiver centric-interference management and the other is transmitter-centric interference management (Zhang et al., 2016). However, the IEEE SCC41 cognitive radio network standard has suspended receiver centric approach because it requires knowledge -such as modulations, coding schemes and individual receivers location- of limits of interference at all receivers in the primary network. Spectrum sensing can be achieved at both the PHY layer and MAC layer respectively; at the PHY layer on one hand, sensing focuses on detecting the signal of the PU to identify habitation or release of the spectrum and some PHY layer sensing methods (Jiang et al., 2015) include energy detection, matched filter, feature detection and sequential spectrum sensing such shifted chi- square. MAC layer spectrum sensing on the other hand, determines the channel that CR users can sense and access. CR users should be capable of handling multiple technologies such as the ones operating at the ISM band including those that may appear across the spectrum. Moreover, CR users should be capable of sensing available spectrum as quickly as possible. Generally, there is a trade-off between sensing time (when using wideband spectrum sensing) and sensing accuracy (when using narrow band sensing). Cooperative sensing can be used to decrease sensing time and increase sensing accuracy. Similarly, spectrum sensing is sensitive to fading environment and shadowing; lots of work in literature have focused on non-cooperative sensing in fading environment. However, cooperative sensing has been proposed as the best way to solve fading and shadowing challenges, albeit, with other implications and challenges such as imperfect information exchange between CR users and additional communication and processing overhead. However, cooperative sensing provides high accuracy for spectrum sensing than non-cooperative sensing. Spectrum sensing is based on signal detection and can be model mathematically as a simple identification problem and formalised as an hypothesis test in Eq. (1) (Zhang et al., 2016):

$$y(k) = \left\{ \begin{array}{l} n(k)\text{: } H_0 \\ |s(k) + n(k)|\text{: } H_1 \end{array} \right\} \tag{1}$$

where $y(k)$ is the sample tested at time k, $n(k)$ is the noise at variance δ^2 which must not be white Gaussian noise, $s(k)$ is the signal to be detected by the network, H_0 is hypothesis with noise-only and H_1 is hypothesis with signal-plus-noise. H_0 represents sensed state for absence of signal and H_1 represents sensed state for presence of signal. Based on this hypothesis, four possible cases for detected signal can be deduced.

1. Showing hypothesis H_0 when H_0 is true $(H_0|H_0)$
2. Showing hypothesis H_1 when H_1 is true $(H_1|H_1)$
3. Showing hypothesis H_0 when H_1 is true $(H_0|H_1)$
4. Showing hypothesis H_1 when H_0 is true $(H_1|H_0)$

The result in 2 shows a scenario of the signal being detected correctly, while results in 3 and 4 are for scenario of signal being missed detected and for a case of false alarm respectively (Zhang et al., 2016). A mathematical model for probability of miss-detection was developed in Rawat et al. (2015) to evaluate the performance of a sensing algorithm. However, since September 10, 2010, focus has shifted from client sensing to database geo location using beacons; and when beacons are used advanced information such as channel quality can be obtained. The amount of spectrum space available for opportunistic-use depends on the definition of spectral opportunity used to measure and exploit spectrum space. Conventional definition of spectral opportunity and conventional sensing methods usually exploit three dimension of the spectrum space: frequency, time, and space (Mukherjee and Nath, 2015). However, other concept such as the multidimensional EM space utilization of; frequency, time, space, code, power, angle of arrivals (AoAs), and polarization can be used to differentiate wireless signals (Chiwewe et al., 2015; Mukherjee and Nath, 2015) and create additional spectrum prospects. Also, co-existence issues can be address using this concept since it defines how the radio environment can be shared among various (primary and/or secondary) systems. Spectrum detection methods that exploit this n-dimensions spectrum space for spectrum sensing, identify occupancy in all n-dimensions of spectrum space and find more spectrum space hole should be of interest for future research.

8.2. Spectrum mobility and spectrum handoff

Spectrum mobility management in cognitive radio networks (CRNs) considers fast and smooth switching for minimal spectrum handoff delay for low latency in communications. Important statistics that are related to the time duration of spectrum handoff can be obtained from sensing algorithm. When this is obtained, minimum performance-loss can occur to on-going communication (Chiwewe et al., 2015). New adaptive protocols for spectrum mobility managements need to be developed. In CRN, spectrum mobility is dependent on channel conditions or activity of the PUs on a licensed band. The habitation of PU on a licensed spectrum and channel conditions are both time varying and indeterminate. Therefore, availability of spectrum varies over time and space, consequently SU requires spectrum handoff to maintain reliable and robust communication. Unlike in traditional wireless network, spectrum mobility and spectrum handoff in CRNs are new issues and challenges in wireless resource management, which requires solution during implementation of dynamic spectrum access (DSA) (Christian et al., 2012; Liu et al., 2008; Riaz and Niazi, 2015). Spectrum mobility schemes which gives attention to variations of availability of spectrum in time and space as well as delay in switching when spanning spectrum distributed over a wideband of frequency needs to be developed for CRN. Due to its effectiveness in calculation and flexibility in modulation OFDM has been the preferred modulation for cognitive radio (Liu et al., 2008) Fig. 5 shows how DSA allows SU or CR users to utilize the white space of licensed users or PU's spectrum using cognitive radio technology. White space is defined by time, frequency and maximum power in a particular geographical location and can be used by the CR user as long as it does not interfere with the activities of the PU or licensed user (Yau et al., 2009).

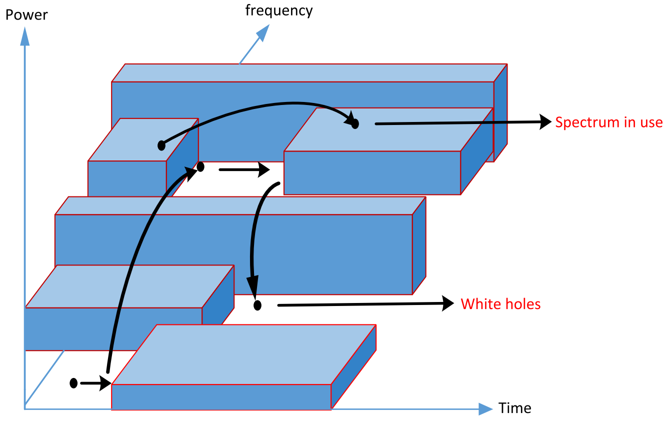


Fig. 5. An illustration of DSA (Chiwewe et al., 2015, Yau et al., 2009).

9. Spectrum handoff strategies

Spectrum handoff strategies can be implemented before an event that can trigger spectrum handoff happens or after the event has happened. In CRNs there are two events that can trigger spectrum handoff that can be related to PU activities; (a) PU activity/signal is detected on a licensed band previously occupied by a SU (b) SU mobility results in SU transmission coverage overlapping with PU current channel band (Christian et al., 2012). Based on the two events above spectrum handoff strategies can be categorized as; Non-handoff, reactive spectrum handoff, proactive spectrum handoff, and hybrid spectrum handoff. Similarly, spectrum handoff can be triggered by channel degradation (Christian et al., 2012). We attempt explanation of the spectrum handoff strategies in the preceding sessions.

9.1. Proactive spectrum handoff

Authors in Wang and Wang (2008) defined proactive spectrum handoff strategy based on target channel selection methods, in this case, secondary users ensure that target channels are available for spectrum handoff before it commence transmission. Broadly, in this approach, a CR user perform switching and reconfiguration of its RF front-end before a PU appears on the channel based on channel status prediction using previous channel usage statistics. Based on this information, CR users can predict when PU is likely to vacate or allocate a channel, and then condition and knowledge of the channels is periodically observed and continuously updated. In pro-active spectrum strategies accurate PU traffic modelling is a key factor, and performance of spectrum mobility scheme will be degraded when PU traffic model is predicted inaccurately (Christian et al., 2012).

9.2. Reactive spectrum handoff

Reactive spectrum handoff strategy is an on-demand or event-triggered approach where the CR users implement spectrum switching and reconfiguration of its RF front-end when a PU suddenly appears on a channel previously occupied by the SU (Song and Xie, 2010a). In this case, target channels from instantaneous outcomes of wideband sensing are selected for spectrum handoff Wang and Wang (2008). However, due to sensing and reconfiguration delay there is high latency in CR and PU transmissions, therefore, modification and adaptation of the different layers of the network stack is required (Chiwewe et al., 2015). Authors in Mukherjee and Nath (2015) suggests for instance, freezing of the TCP timer at the transport layer to prevent miss-interpretation of spectrum handoff delay as delay incurred from acknowledgement message at the transport layer. A cross-layer optimization framework for protocol adaption should be developed to address challenges of spectrum mobility and the delays that come with it. CR users should also be capable of wideband sensing in real-time to sense weak PU signal in a wide spectrum range (Chiwewe et al., 2015; Mukherjee and Nath, 2015).

9.3. *Hybrid handoff*

In Hybrid handoff strategy the strength of reactive and proactive strategies are combined by applying proactive spectrum sensing and implementing reactive handoff action (Christian et al., 2012). Most current efforts are concentrated on particular spectrum handoff strategy. Though, for each spectrum handoff strategy a different PU network is recommended, However, adaptive spectrum handoff algorithm with multiple spectrum strategies should be developed and spectrum leaving factors should be considered in the process design (Christian et al., 2012). In Southwell et al. (2012) authors propose a mobility game where players have mobility strategies that allow them gain points when they remain within their plan and pay a cost when they switch to other channels, a Nash equilibrium is established when changing spectrum handoff spectrum strategies does not benefit a player unilaterally. Some advantage of this strategy includes faster spectrum handoff time since the time used in implementing spectrum sensing is not included in the process of spectrum handoff. However, designated target channel at the time of spectrum sensing may have been re-occupied at the time of spectrum handoff leading to outdated target channel selection. In Table 3, we summarize the different spectrum strategies including their strength and weakness as well.

10. Spectrum handoff performance metric that will benefit IWSN

Spectrum handoff is a new type of handoff, and therefore the metrics on which its performance is measured are different from conventional handoff performance metrics due to several factors such as; type of network, elements involved in networks, and type of traffic the network supports. For performance metrics of conventional handoff scheme, decision schemes and handoff prioritization see Ahmed et al. (2014); Sgora and Vergados (2009). IWSNs have unique QoS requirements and handoff is a key element for maintaining continuous connection and achieving QoS defined by applications and systems. Therefore, in this section, we discuss handoff metrics that are relevant for IWSNs.

1. Delay

   This is the time between the instant a handoff request is initiated and the instant the handoff process is completed (Sgora and Vergados, 2009). For industrial systems and applications, minimal handoff delay/latency is required for spectrum handoff schemes due to delay sensitivity QoS requirements of industrial systems. High delay in spectrum handoff process will lead to high latency in communication, which is contradictory to the low latency requirements of industrial wireless systems.
2. Channel utilization efficiency

   This is the ratio of number of channels being served to the total number of channel in the system (Sgora and Vergados, 2009). Spectrum handoff schemes with smart and accurate target channel selection and low probability of misdetection will have high channel utilization efficiency. IWSNs define availability and reliability as QoS requirements for most of its systems and applications, therefore requires a spectrum handoff scheme with high channel utilization efficiency for optimal network and system performance.

Table 3
highlights and summaries of the pros and cons of the various spectrum handoff approaches described above.

Approach	Strategy	Strength	Weaknesses	latency	Recommended scenario	Applied for
Proactive spectrum handoff	Sensing and switching done before PU appears	Target channel selection availability, and fast switching response time	Needs accurate PU traffic model, continuous observation and update of channels and target channel becomes outdated	Very low latency when well-planned and designed	Well-modelled cognitive radio network	IWSN (Tran et al., 2015) CRN (Afsana et al., 2015; Lertsinsrubtavee et al., 2011; Zahed et al., 2012), CRAHNs (Song and Xie, 2010a, 2010b, 2012), CR-MANET (Nejatian et al., 2014)
Reactive spectrum handoff	Sensing and switching are done after PU appears	Accurate target selection	High sensing and reconfiguration delay resulting in slow response	Very high latency	General cognitive radio networks	Cognitive relay network (Wang et al., 2013), CRNs (Bhushan et al., 2015; Kaur et al., 2009; Potdar and Patil, 2013; Wang and Wang, 2012; Zhi-jin et al., 2015), Cognitive LTE network (Chen and Hong, 2013)
Hybrid spectrum handoff	Sensing done before PU appears and switching done after PU appears	Smart target channel selection and fast switching response time	Target channel selection may become outdated	Medium latency	Well-modelled cognitive radio networks	CRN (Li et al., 2013), Heterogeneous CRN (Qianbin et al., 2013),VoIP in CRN (Chakraborty and Misra, 2015), CR-IWSN (Son Duc et al., 2013)
Non handoff	Handoff is not performed	Smooth communication	Complex computation, botched/ disrupted communication, may cause interference to license user	Low to high latency	Well- modelled cognitive radio networks	Practically not achievable

3. Number of unnecessary handoff

   When a handoff process degrades the performance of a network instead of improving it. Then, the handoff is considered surplus and should be discouraged (Ahmed et al., 2014). This type of switching is considered as Ping-Pong Effect. IWSN applications and processes are time-bound and therefore requires minimal handoffs to maintain continuous communications. Spectrum handoff schemes should be developed for IWSN with minimal handoffs and low handoff latency.

4. Throughput

   This refers to the data rate achievable by the network during a communication inclusive of spectrum handoff periods. Spectrum handoff with higher throughputs are desirable and are important for IWSN systems and applications.

11. Spectrum handoff algorithms

With the unprecedented flexibilities that cognitive radio offers come the challenge of designing protocols and transmission schemes to fully exploit the CR capabilities. The potential of cognitive radio as a candidate for broadband provisioning for industrial wireless sensor network QoS requirements, and to improve radio communication efficiency of future wireless networks such as 5 G networks has been recognized. To design practical and effective protocols; different type of scenarios, assumptions and corresponding cognitive behaviours should be considered. This section discuss some spectrum handoff protocols based on the cognitive behaviour used in their design. Cognitive behaviour or how SU (CR user) use the licensed spectrum band can be grouped into three categories including interference-avoidance, interference-controlled and interference-mitigating cognitive behaviour. In Table 4, we present a summary of these cognitive behaviour in relation to spectrum handoff algorithms, and in Fig. 6, we give an illustration of typical spectrum handoff procedure. A major assumption for cognitive behaviour is that the primary network does not adapt to the SU (CR user or cognitive network) but the SU (CR user or cognitive network) to the primary (Wyglinski et al., 2008). The preceding sections are the different cognitive behaviour identified in literature.

11.1. Interference-avoidance cognitive behaviour

Under this cognitive behaviour, CR users allocate the licensed spectrum without interfering with PU activity, in other words, the tolerable interference at the PU receiver is set to zero. CR user achieve this by sensing the spatial, temporal, or spectralvoids and by adjusting their transmission, CR users can fill the sensed white spaces or spectral holes. While this assumptions are for theoretical purposes, attempts at developing practical methods of PU signal detections have also been of interest (Wyglinski et al., 2008). In addition to signal detection, cognitive radio user can implement MIMO when equipped with multiple antennas and transmits in the null space of the PU receive channel. The authors in Wang and Wang (2008) provided a pre-emptive resume priority M/G/1 queueing network model to analyze the condition in which a re-active or pro-active spectrum handoff should be implemented depending on sensing time. Clearly, their approach is interference-avoidance behaviour because their model is design to handle scenario where the secondary users need to change its operating channels when its transmission is interrupted. A technique to jointly optimize spectrum handoff scheduling and routing in multi-hop multi-radio cognitive networks is proposed in Feng et al. (2009) to maximize the throughput of a multi-hop cognitive radio network by implementing a cross-layer design approach. Their objectives are to minimize spectrum handoff latency for multiple links with network connectivity constraints and to rebuild routing path before performing spectrum handoff for affected flows. Their simulation results showed an improved network performance for their solution. Their work however, failed to show how their solution could be applied to real-life scenarios.

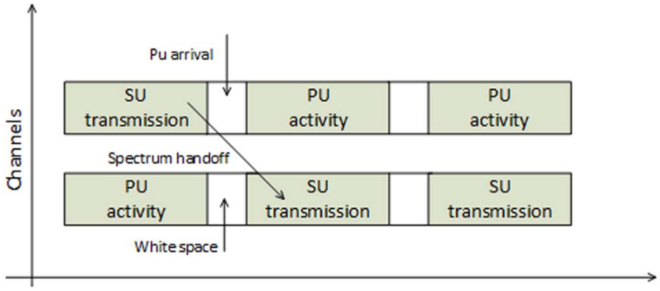


Fig. 6. An illustration of spectrum handoff procedure.

11.2. Interference controlled cognitive behaviour

In interference controlled behaviour, the interference caused by the SU (CR user or cognitive network) to the PU (primary network) is permitted or allowed when it is below a tolerable limit acceptable to the QoS constraints of the PU. When this is achieved, the SU can transmit over the same spectrum as the PU and this is termed underlay (Wyglinski et al., 2008). In wireless networks, spread-spectrum techniques are also used to achieve this objective to control interference. To obtain high SNR for enhanced data rate and throughput, high transmit power needs to be implemented, however, using high transmit power implies an increase in interference at the receiver of nodes in the network or at the PU receiver. Kaur et al. (2009) proposed a model with two fuzzy logic systems (FLS) to tackle the issue in a computational and hierarchical traceable fashion. Transmit power control was implemented in the first FLS while the decision to perform a spectrum handoff or not to another frequency was taken in the second FLS. The basis for their work was a trade-off for decision to control transmit power or switch to another frequency. However, their work did not consider other effects of modification to transmit power such as co-channel interference, and adjacent channel interference. Authors in Kaur et al. (2009) did not also consider the effect of a CR user changing its operating frequencies in the licensed bands to a lower or a higher frequency band than the previously occupied frequency which was the focus of the authors in Yang et al. (2015b). In their work Yang et al. (2015b) observed that when a CR user change its operating frequency from a high frequency to a low frequency during a spectrum handoff, its transmission range enlarges which increases the probability of interference to PUs. And also, the moment a CR user switches its operating

Table 4
Summary of spectrum algorithm based on cognitive behaviour.

Spectrum algorithm	Characteristics	Interference mechanism	Interference to PU activities	Potential interference mitigating strategy	Focus
interference-avoidance cognitive behaviour	tolerable interference is zero	prevention	not permitted	TDMA or FDMA	primary network
interference-controlled cognitive behaviour	tolerable interference is less than threshold	regulation	permitted	spread spectrum	primary network
interference-mitigating cognitive behaviour	tolerable interference is less than threshold	alleviation	permitted	ultra wide band	primary network, and secondary network

frequency from a low to a high frequency during a spectrum handoff its transmission coverage shrinks which leads to the possibility of connection failure between a transmitting pair. Therefore, Yang et al. (2015b) proposed a selection scheme to select optimal operating frequency in spectrum handoff for CRNs. Their work considers a trade-off between the probability of interference to licensed users and the probability of successful transmissions as well as end-to end throughput in both single hop and multiple hop scenarios.

11.3. Interference mitigating cognitive behaviour

In interference mitigating behaviour, in addition to information such as primary spectral gaps, interference temperature, information such as PU's code book that allows SU decode PU transmission and enables SU to transmit on the same channel as the PU are provided. This additional information, not only allows SU mitigates interference it incurs to the PU, but also that which it incurs from the PU (Wyglinski et al., 2008). This behaviour is termed overlay in literature. A spectrum handoff solution that takes into account the collision between SUs in a multi-SU spectrum handoff scenario in a CR-IWSN was introduced in Son Duc et al. (2013). In their approach, the sensor nodes are equipped with cognitive radios to perform spectrum handoff decisions if the PU signal is detected and to determine if the PU is a co- existence terminal or hidden terminal. If the PU is a coexistence terminal, then, SU transmission can continue uninterrupted, otherwise it switches to an unoccupied channel. Spectrum handoff strategies and cognitive behaviour schemes should consider minimum interference, spectral efficiency, reliable communication and low latency in their design, correspondingly, some performance metrics that have been used to determine the performance of spectrum handoff algorithm in literature include (Christian et al., 2012); number of handoff, link maintenance probability, handoff latency and effective data rate. (Christian et al., 2012) identify link maintenance and handoff latency as two important metrics for spectrum mobility and concludes that spectrum handoff techniques with probability of higher link maintenance and minimum handoff latency provides better spectrum agility to CRNs. Another issue in spectrum handoff that requires careful planning is routing recovery. One way of integrating routing recovery into spectrum schemes is by calculating new route and implementing spectrum handoff as soon as a new routing table is available. The other approach is to make two redundant channels available before commencing transmission to avoid routing calculation i.e. data channel and backup channel (Christian et al., 2012).

12. Non-DSA related cognitive functionality and challenges

For CRN systems operation four important functionalities are defined as follows; (a) Spectrum sensing involves sensing unused spectrum, (b) Spectrum decision and access is about deciding on the best channel, (c) Spectrum sharing relates to managing channel access between many users, and (d) Spectrum mobility is switching to target channel when a licensed user appears (Song and Xie, 2010a, 2010b; Wang and Wang, 2008). However, for the realization of dynamic spectrum access (DSA) for IWSNs only two of this functionalities are important i.e. spectrum sensing and spectrum mobility. In addition, compared with other cognitive radio functionalities, spectrum mobility has not been well researched in literature (Son Duc et al., 2013; Song and Xie, 2010b). Below we attempt a brief description of other cognitive functionalities and some challenges identified in literature as well as possible solutions. Fig. 7 shows the relationship between cognitive functionalities with dynamic spectrum access (DSA).

12.1. Spectrum decision and access

Based on the availability of spectrum, cognitive radio users decide on the spectrum band under the QoS requirements of applications that is best for each application. This allocation is driven by intrinsic and extrinsic policies, and involves the following steps (Chiwewe et al., 2015; Mukherjee and Nath, 2015). First step is spectrum characterization, in which case, statistical PU information such as knowledge of the activities of licensed users as well as essential readings like estimated interference level, length of availability of spectrum and probability that CR user will collide with licensed user as a result of sensing error from CR are employed for characterization of each band. The next step involved is spectrum selection, spectrum selection involves the process of choosing the best fitting spectrum band based on the characterization of spectrum done in the first step. In addition, spectrum choice is implemented according to a spectrum-selection rule using QoS requirements such as transmission mode, acceptable error rate, data rate spectrum characteristics, and delay bound (Chiwewe et al., 2015). A relationship linking the rules for spectrum-selection and routing protocols has been established especially in distributed or non-infrastructure based CRNs, therefore a dynamic framework needs to be developed to accommodate varying channel conditions and QoS requirements of users. The final step is reconfiguration, based on prevailing radio environment and QoS requirements of application, CR user may need to reconfigure its communication protocols, hardware and RF front-end. Implementing a co-operative framework with reconfiguration to support decision over heterogeneous spectrum bands remain an open issue, as well as adaptive models for spectrum decision that take into consideration application needs and spectrum scarcity (Chiwewe et al., 2015). Future research efforts should be focused in these directions.

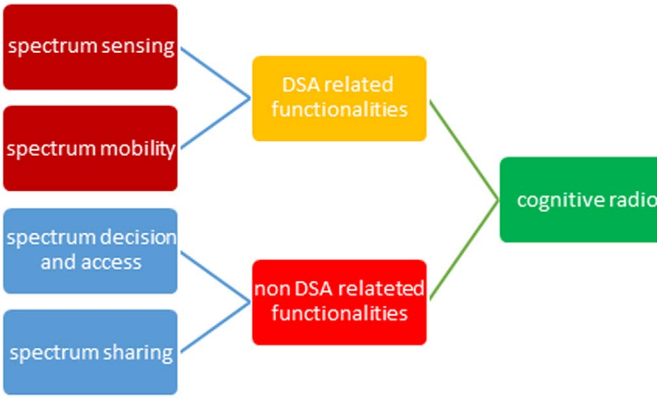


Fig. 7. Cognitive functionalities as it relates to DSA.

12.2. Spectrum sharing

The wireless channel remains a shared medium (Chiwewe et al., 2015) consequently numerous CR users may try to access the spectrum (Mukherjee and Nath, 2015) at the same time, it is therefore crucial to regulate the various transmission attempt among different SUs to avert multiple users collision in extended portions of the spectrum (Chiwewe et al., 2015; Mukherjee and Nath, 2015). To achieve this, a lot of MAC protocol functions should be incorporated in spectrum sharing (Chiwewe et al., 2015). Fixed-allocation MAC e.g. CDMA or FDMA or random access MAC e.g. ALOHA and CSMA-CA could be implemented for cognitive radio-based network e.g. CR-IWSNs depending on the needs of the application (Mukherjee and Nath, 2015). Spectrum sharing could be either vertical or horizontal spectrum sharing based on the components or network involved; when sharing is within the licensed band and is with licensed user it is known as vertical spectrum sharing, otherwise, when it is done outside the licensed band with unlicensed users it termed horizontal spectrum sharing. The co-existence of CR users and PUs in the CRNs and the immense spectral opportunities present spectrum sharing problems in CRNs, correspondingly four approaches have been introduced to address these spectrum sharing challenges (Chiwewe et al., 2015) including: architecture, spectrum allocation behaviour, spectrum access technique, and also scope. On architectural perspective, spectrum sharing can either be distributed, in which single nodes execute local policies in synergy with other nodes to share spectrum or centralized where control is centralized and a central entity take control based on a global optimization objective. Regarding spectrum allocation behaviour for spectrum sharing, it can be done in a co-operative way such that the transmission of all nodes is taken into consideration with respect to the interference measurements of all nodes in the network or in a non-cooperative manner where only a single node is taken into consideration when sharing is done (Chiwewe et al., 2015). In terms of access technique, CR user can employ an interference control approach (spectrum underlay) or implement an interference avoidance approach (spectrum overlay) of spectrum sharing (Mukherjee and Nath, 2015), in underlay approach, techniques such as OFDM, UWB and spread spectrum technique that allow CR user to transmit simultaneously with PU in an uncoordinated way are used. The technique allows transmitted signals to be spread over a large band of spectrum such that CR user' transmission is regarded as noise by PU, and to reduce interference to PU, transmission power of CR users is strictly regulated. As a result, efficient power control algorithm should be developed for secondary transmitters. In overlay, e.g. dynamic frequency selection (DFS), CR user take advantage of knowledge of availability of spectrum holes to transmit while ensuring that there is no interference incurred to the PU even if frequency is not assigned to the PU. Lastly, for scope, it can be intra-network spectrum sharing or within a CRN infrastructure or internetwork spectrum sharing i.e. among several co-existing CRNs. Game theory can be used to provide distributed and efficient spectrum sharing schemes that takes into consideration conflict and cooperation between SUs (Chiwewe et al., 2015).

13. Related work

One consideration for using CR technology once there is a link quality degradation is for SU to vacate the channel it is previously occupying through spectrum handoff, and resume communication immediately in available channel through proper target channel selection methods, which in some cases is incorporated into the spectrum handoff process or scheme. However, establishing a new channel is a non-trivial task and is subject to lots of factors including; channel availability during the period of spectrum handoff including common control channel (CCC) availability, channel capacity, and probability of future availability of channels (Christian et al., 2012). One way of addressing this problem is to employ cooperative sensing instead of local sensing (Son Duc et al., 2013) and to use backup channel list (BCL) (Christian et al., 2012). Another approach is to use channel availability prediction; accurate target channel can be predicted by SU based on historical spectrum statistics. e.g. if PU activity is based on human behaviour and if it can be statistically determined, then SU can estimate when the channel previously occupied by PU will be available and for how long it will be available by modelling the traffic of PU (Christian et al., 2012). Similarly, proper target channel/cell can be selected by stochastic connectivity estimation instead of received signal strength as was suggested in Won-Yeol and Akyildiz (2012). Still, poor target channel selection technique or method can lead to several spectrum handoffs which degrades overall network performance (Christian et al., 2012). However, these solutions might have been appropriate in CRNs not in IWSNs, for instance, probability that target channel will be available at the time of spectrum handoff in IWSN environments is very low due to variability of spectrum resource in IWSN aggravated by harsh environment as well as mobility of nodes and traffic fluctuation, therefore, solutions including channel availability prediction do not work in IWSNs. Likewise, due to interference and multi-path; signal strength, communication range, channel capacity, and network throughputs are greatly reduced in industrial environments, so, using cooperative sensing and BCL approaches do not work in IWSNs, Nevertheless, in an attempt to developed Standards with deterministic solutions to address some of these challenges, industrial-WLAN (IWLAN) which is an enhancement over IEEE 802.11-based consumer Wi-Fi was developed to provide deterministic operations in IWSNs, with additional reliability, improved roaming and longer communication range (Chiwewe et al., 2015). Similarly, with recent CR standardization efforts, standards including IEEE 802.15 WPAN, IEEE 802.11 WLAN, and IEEE 802.22 WRAN are capable of exploiting TVWSs permissible for CR technology, though, these standards are not yet suitable for IWSNs. Nonetheless, with some improvement such as IEEE 802.15.4 m which allows IEEE 802.15.4 wireless devices to opportunistically use TVWS spectrum, industrial standards including WirelessHART, ISA100.11a, WIA-PA, and ZigBee are able to take advantage of TVWSs to meet the QoS requirements of Chiwewe et al. (2015). Also, Impulse-radio ultra-wide band (IR-UWB) system was defined by the IEEE802.15.4a standard to mitigate the problem of degradation in time-critical IWSN (Jaber et al., 2016; Reinhold and Kays, 2013). Equally, another standard suitable for industrial environment is IEEE 802.11af, technical amendments in this standard allows legacy IEEE802.11 devices to legally operate in TVWS, though, IWSN systems and applications will fully benefit from this improvement, if for instance, IWLAN can be adapted to support this standard (Chiwewe et al., 2015). In addition, as an attempt to use cognitive solutions for IWSNs challenges authors in Chiwewe and Hancke (2016) presented cognitiva, a cognitive radio protocol designed for reliable multi-band operation in the license-free ISM band as well as TVWSs for industrial wireless network. In Muhammad Faisal et al. (2013) authors proposed a cross-layer solution to boost throughput in wireless regional area network (WRAN) based on cognitive radio network by reducing latency and increasing throughput through TCP performance enhancement. Simulation results of their mechanism showed that TCP performance was enhanced 20 times and bandwidth was conserved by reduction in retransmission overhead. To address the issue of co-existence, co-location and energy consumption in IWSNs, Zheng et al. (2012) developed a power control algorithm that self-configure for CR-IWSNs with interference constraints. Their approach gives consideration for energy-efficiency and optimization of system throughput for spectrum underlay. Results in their work showed an improvement in throughput and reduction in energy consumption with a guarantee that no interference is incurred to the users. Yau et al. (2009) suggest various cognitive solutions for IWSNs including cross-layer solutions e.g. by exploiting information from other layers more efficient decisions can be made by protocols, other solutions include context-aware and intelligent routing, topology management, and distribution of coordinators in large IWSNs as well as a cognitive radio-based reliability optimization for IWSNs. Juncheng and Weihua (2011) investigates what capacity can be achieve in a wireless network with a single-software defined radio (single-SDR) equipped transceiver for multi-hop network given any network flows. Result in their work presents and compares potential capacity for single SDR network with a multiple radio networks numerically and through simulation. Their work concludes that multiple radio network performs better than single-SDR network especially with moderate probability of channel availability, albeit extra cost of additional radios. It also provides direction for future network planning when applying SDR configuration. Reducing spectrum handoff effects by using parallel multiple transmission and mitigating channel contention between multiple SUs during spectrum handoff remain an open issue (Christian et al., 2012; Yunhuan et al., 2012).

14. Research challenges and future directions

In this section, we identified research challenges that are particular to both IWSNs and CR-WSNs and accordingly, we present a brief breakdown of the challenges, and also we give an insight into focuses that should define future research trend as it relates to CR-IWSNs including;

14.1. The non-Implementation of spectrum handoff due to resource allocation and co-existence issues in IWSNs

Spectrum handoff and Handoff issues in general, are reviewed in literature based on a general assumption that the values of network parameters and handoff decision parameters, such as bandwidth, symbol rate, wireless link error, holding time, target channel list, and handoff delay are always available or are known. Or at least, that these values can be obtained before handoff strategies are performed. However, this is not true in many real life scenarios, e.g. in IWSNs; because challenges in resource allocation and co-existence do exist, it is difficult to have the real value of these parameters. Therefore, estimated values, which are prone to error and makes it difficult to implement spectrum handoff policies and schemes, are used. Unless and until these issues i.e. resource allocation and co-existence are addressed with spectrum handoff in cognitive radio-based networks like CRSNs and CR-IWSNs in mind, implementation or physical realization of research efforts in spectrum handoff for IWSNs may have to wait, or at best remain as just research efforts in library shelves or published articles.

14.2. Radio resource allocation and power control in CR-IWSNs

In the nearest future due to the increasing demand and deployment of CR-IWSNs it is possible to have several CR-IWSNs designed for diverse applications to be installed in overlapping industrial locations by the same operator e.g. in an industrial monitoring scenario, related sensors might be deployed for nuclear plant monitoring and a cyber-physical sensing simultaneously. In such case, all the networks compete with each other for spectrum resources creating internetwork interference, similarly, sensor nodes in these networks would require various on-board computation for data processing and transmission resulting in battery power consumption and shortened network life-time. Therefore, efficient control power and radio resource allocation (power and spectrum allocation) schemes for CR-based networks for fair radio resource allocation and efficient power utilization are required and should be the interest of future research efforts. Authors in Ahmad et al. (2015) highlights inherent peculiarities of CR-IWSNs that might be of importance in the design of such protocols or schemes. For instance, it observed that unlike CRNs and similar to WSNs in CR-IWSNs, sensor nodes have no/low traffic in the absence of events and generate high and bursty traffic when an event is detected with increased probability of collision among multiple channel-competitive sensors. Therefore, spectrum allocation schemes for CR-IWSNs should take into account the bursty nature of the network traffic in CR-IWSN for increased communication reliability.

14.3. Co-existence

There are on-going efforts at designing low-power wireless network for IWSN to co-exist with other wireless standards. For instance, WirelessHART use channel blacklisting and combine frequency hopping with TDMA to improve co-existence, however, collision still happens resulting in degraded QoS of protocols and standards (J et al., 2011; Kumar and Hancke, 2014). Therefore, more effective and innovative techniques such as interference cancellation, effective radio resource management as well as more software defined radio solutions should be the interest of future research efforts. Similarly, to guarantee real-time services for IWSNs more research efforts needs to be geared towards developing real-time scheduling schemes and algorithms for IWSNs.

14.4. Cognitive M2M network

Machine-to-machine (M2M) communication is a new communication para-digm similar to internet of things (IoT). However, unlike IoT, which main distinguishing feature is information. e.g. the ‘connected things’ interconnections with each other and with humans (Maia et al., 2016), in M2M communication, the differentiating characteristic from other communication paradigms is its capability to completely eliminate human activities in the communication cycle, and the main focus in M2M communications, is connectivity (Ali et al., 2017, Sikorski et al., 2017; Verma et al., 2016; VrabiÄ et al., 2017). M2M interconnects intelligent machines in a digital network using diverse communication technologies to autonomously monitor and control machines without any human intervention (Bruns et al., 2015). However, full self-governing automation in M2M has given rise to several heterogeneous applications, having entirely dissimilar capabilities and functionalities to leverage on advantage of M2M. Consequently, number of devices taking part in M2M, is exponential, according to a report by Ericsson, this number will rise to 50 billion devices by 2020 (Maia et al., 2016). This geometric explosion necessitates huge improvement on existing access technique to maintain QoS requirements of different applications running on millions of machines. Some challenges created by M2M technology include congestion and overload in network, energy efficiency, heterogeneity, reliability, QoS, and ultra-scalable connectivity. To cater for millions of machines in M2M and to overcome challenges imposed by M2M, there is a need for more spectrum (Ali et al., 2017, Sikorski et al., 2017; Verma et al., 2016). Accordingly, authors in Verma et al. (2016) suggest incorporation of cognitive radio technology in M2M, they argue that due to limited licensed spectrum, a secondary spectrum is needed, to prevent M2M devices from consuming more energy and degrading network performance and efficiency. Developing techniques that would allow M2M to access and utilize primary spectrum as well as to opportunistically use the secondary spectrum remain an open issue in M2M. Nonetheless, when this is fully realised, M2M would find application in areas such as; smart metering, traffic monitoring, e-health care, and smart grid (Verma et al., 2016), cyber-physical production systems (CPPS) and industrial internet of things (IIoT) (VrabiÄ et al., 2017), as well as transportation (Maia et al., 2016).

14.5. Cognitive radio for 5 G networks

To fully realize the vision of 5 G wireless network as intended, present wireless-based networks would have to improve several capacities. Much of these new advancements should involve different ways of accessing the spectrum, and to a notably large extent, it should involve techniques of accessing higher frequency ranges using DSA technique developed for cognitive radio technology, other part of proposed improvements should include deployment of massive antenna configurations, similarly, direct device-to-device (D2D) communications, as well as ultra-dense deployments should be incorporated into proposed advancements (Gupta and Jha, 2015; Jaber et al., 2016). Nonetheless, innovations in mobile wireless communication has evolved from analogue voice calls to the present high quality mobile broadband services with end-user data rates of several hundreds of megabits per second. However, the envisioned future of mobile technology is a networked society with boundless and limitless data rates for access to infinite information and data sharing which is everywhere, every time for everyone and everything (Gupta and Jha, 2015; Jaber et al., 2016). In line with this, the vision of 5 G technology is to provide a network that supports (Gupta and Jha, 2015); 1000 times increased data volume per area, 10 times increased numbers of connected devices, 10–100 times increased typical user data rates, 10 times extended battery life for low power Massive Machine Communication (MMC) devices, 5 times reduced End-to End (E2E) latency. To achieve this goals, new technology components would have to be developed for the evolution of existing wireless based technologies into the intended future 5 G network (Gupta and Jha, 2015; Jaber et al., 2016; Sheng et al., 2015). Accordingly, future advancements and solutions to achieve the vision 5 G network should include (Ban et al., 2016; Jaber et al., 2016; Chen et al., 2016; Gupta and Jha, 2015; Rappaport et al., 2013; Sheng et al., 2015); incorporation of cognitive radio technology for 5 G network; - this includes extended spectrum band operations, as well as consideration of operation in new spectrum regimes to address issues and challenges such as heterogeneous network and co-existence as well as co-location of devices. Other needed improvements include the following, high speed packets access (HSPA), long time evolution (LTE), orthogonal frequency division multiple access (OFDMA) and scheduling, indoor/outdoor communications technologies e.g. millimeter wave and visible light communication utilizing high frequencies/large antenna arrays, mobile and static small cells and Wi-Fi overlay/offloads, as well as massive MIMO (Multiusers), and multi-hop/meshed networks.

14.6. Internet of things

Internet of Things (IoT) is a new paradigm introduced in the late 1990s and its objective is to connect sets of anyone, anything, any service, and any network anytime (Islam et al., 2015). The huge research interest generated by IoT in recent years is due to the values it promises to create (Perera et al., 2014). These value are aptly summarized in IoT vision, (Perera et al., 2014) which is; IoT promises to connect people and things anytime at anyplace with anything and anyone, if possible using any route or network and any platform to build a better world for human beings where things around us have the capabilities to distinguish between our likes, our wants, and our needs and act accordingly without explicitly being trained. When IoT is fully implemented, it has the capacity to provide solutions for a wide range of applications including (Islam et al., 2015; Perera et al., 2014; Pham et al., 2015; Sun et al., 2016; Wu et al., 2016; Xu et al., 2016; Zhu et al., 2015); smart and connected cities e.g. mobile crowd sensing and cyber physical sensing. Health care including; health services e.g. internet of m-health and wearable access, health applications including single-condition like glucose level sensing and clustered-condition such as medical management. Traffic congestion, security, emergency services, logistics and industrial control. However, some challenges of IoT that should be of interest to future research includes (Islam et al., 2015; Perera et al., 2014; Sun et al., 2016); challenges associated with resource limitations and energy management, cyber-security and privacy, security requirements (e.g. confidentiality, integrity, authentication, authorization, and fault tolerance), including security challenges (e.g. computational, energy, and memory limitations, with scalability), as well as interoperability issues and legacy devices.

15. Conclusion

In this paper, we have attempted to draw research focus and attention to the potentials and benefits of the very important topic of spectrum handoff and especially for its application for IWSNs - to address the challenges of timeliness, reliability and availability, which are unique QoS requirements for industrial systems and applications -. In addition, because spectrum handoff and cognitive radio, as solution for IWSNs challenges have not been given the much-needed attention in literature; We have highlighted and discussed the unique and stringent QoS requirements of IWSN that can benefit from spectrum handoff and cognitive radio. We also highlighted the potential of cognitive radio and spectrum handoff to provide more spectral hole, real-time, reliable and smooth communication for IWSN through opportunistic spectrum-usage, swift and seamless spectrum switching in the often competitive and overcrowded ISM band. We have also discussed efforts of existing IWSN standards to address the challenges presented by the uniqueness of IWSNs. While attempting to do this, we have presented cognitive radio architectures, functionalities and challenges and we have suggested possible solutions where necessary. We concluded by presenting research challenges and future direction for future research efforts.

Acknowledgement

We acknowledge the constructive feedbacks of anonymous reviewers which immensely improved this paper,and also Ayo Imoru, for his efforts in helping with editing and LATEX. Funding: This work was supported by the Council for Scientific and Industrial Research (CSIR), South Africa [ICT: Meraka].

References

Abu-Mahfouz, A.M., Hancke, G.P., 13–15 Sept. 2011 2011. ns-2 extension to simulate localization system in wireless sensor networks. In: AFRICON, 2011. pp. 1–7.

Afsana, F., Jahan, N., Sunny, F.A., Kaiser, M.S., Mamun, S.A., 21–23 May 2015 2015. Trust and energy aware cluster modeling and spectrum handoff for cognitive radio ad-hoc network. In: 2015 International Conference on Electrical Engineering and Information Communication Technology (ICEEICT). pp. 1–6.

Ahmad, A., Ahmad, S., Rehmani, M.H., Hassan, N.U., 2015. A survey on radio resource allocation in cognitive radio sensor networks. IEEE Commun. Surv. Tutor. 17 (2), 888–917.

Ahmed, A., Boulahia, L.M., Gaiti, D., 2014. Enabling vertical handover decisions in heterogeneous wireless networks: a state-of-the-art and a classification. IEEE Commun. Surv. Tutor. 16 (2), 776–811.

Akhlaghpasand, H., Shah-Mansouri, V., Aug. 30 2015-Sept. 2 2015 2015. Minimum delay scheduling for raw-data convergecast in wireless field networks. In: Proceedings of the 2015 IEEE Proceedings of the 26th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), pp. 1830–1834.

Al Agha, K., Bertin, M.H., Dang, T., Guitton, A., Minet, P., Val, T., Viollet, J.B., 2009. Which wireless technology for industrial wireless sensor networks? The development of ocari technology. IEEE Trans. Ind. Electron. 56 (10), 4266–4278.

Al-Yami, A.M., Harb, K., Abduljauwad, S., 26–28 Nov. 2013 2013. Industrial wireless sensor networks in the perspective of diversity and spectral efficiency. In: Proceedings of the 2013 IEEE Malaysia International Conference on Communications (MICC). pp. 390–395.

Ali, A., Shah, G.A., Farooq, M.O., Ghani, U., 2017. Technologies and challenges in developing machine-to-machine applications: a survey. J. Netw. Comput. Appl. 83, 124–139, 2017/04/01.

Ban, Y.L., Li, C., Sim, C.Y.D., Wu, G., Wong, K.L., 2016. 4g/5g multiple antennas for future multi-mode smartphone applications. IEEE Access 4, 2981–2988.

Bara, F.x, Gidlund, M., Zhang, T., 2015. Ubiquitous, yet deceptive: hardware-based channel metrics on interfered wsn links. IEEE Trans. Veh. Technol. 64 (5), 1766–1778.

Batista, N.C., Mel, R., x00Ed, cio, Matias, J.C.O., Catal, J.P.S., x00E, 25-28 March 2012 2012. Zigbee standard in the creation of wireless networks for advanced metering infrastructures. In: 2012 Proceedings of the 16th IEEE Mediterranean Electrotechnical Conference. pp. 220–223.

Baviskar, A., Baviskar, J., Wagh, S., Mulla, A., Dave, P., 4-6 April 2015 2015. Comparative study of communication technologies for power optimized automation systems: A review and implementation. In: Proceedings of the 2015 Proceedings of the Fifth International Conference on Communication Systems and Network Technologies (CSNT). pp. 375–380.

Bhushan, S., Bali, R.S., Kaur, A., 8-10 Oct. 2015 2015. Spectrum hand off in cognitive radio network using dynamic threshold. In: Proceedings of the 2015 International Conference on Green Computing and Internet of Things (ICGCIoT). pp. 1292–1297.

Biddut, J.H., Islam, N., Jany, M.H.R., Swapna, A.I., 10-12 Dec. 2015 2015. Performance analysis of large scale zigbee network design through geometric structure. In: 2015 Proceedings of the 2nd International Conference on Electrical Information and Communication Technology (EICT). pp. 263–268.

Bruns, R., Dunkel, J., Masbruch, H., Stipkovic, S., 2015. Intelligent m2m: complex event processing for machine-to-machine communication. Expert Syst. Appl. 42 (3), 1235–1246, 2015/02/15.

Chakraborty, T., Misra, I.S., 21-24 Sept. 2015 2015. Designing a real-time spectrum handoff algorithm for voip based cognitive radio networks. In: Radio and Antenna Days of the Indian Ocean (RADIO), 2015. pp. 1–2.

Chen, B., Zhu, C., Li, W., Wei, J., Leung, V.C.M., Yang, L.T., 2016. Original symbol phase rotated secure transmission against powerful massive mimo eavesdropper. IEEE Access 4, 3016–3025.

Chen, D., Nixon, M., Han, S., Mok, A.K., Zhu, X., Feb. 26 2014-March 1, 2014 2014. Wirelesshart and ieee 802.15.4e. In: Proceedings of the 2014 IEEE International Conference on Industrial Technology (ICIT). pp. 760–765.

Chen, Y.-S., Hong, J.-S., 2013. A relay-assisted protocol for spectrum mobility and handover in cognitive lte networks. IEEE Syst. J. 7 (1), 77–91.

Cheng, B., Cui, L., Jia, W., Zhao, W., Gerhard, P.H., 2016. Multiple region of interest coverage in camera sensor networks for tele-intensive care units. IEEE Trans. Ind. Inform. 12 (6), 2331–2341.

Chiwewe, T.M., Hancke, G.P., 14-17 March 2016 2016. Cognitiva; a cognitive industrial wireless network protocol: Protocol design and testbed implementation. In: Proceedings of the 2016 IEEE International Conference on Industrial Technology (ICIT). pp. 2042–2047.

Chiwewe, T.M., Mbuya, C.F., Hancke, G.P., 2015. Using cognitive radio for interference-resistant industrial wireless sensor networks: an overview. IEEE Trans. Ind. Inform. 11 (6), 1466–1481.

Christian, I., Moh, S., Chung, I., Lee, J., 2012. Spectrum mobility in cognitive radio networks. IEEE Commun. Mag. 50 (6), 114–121.

Chung, T.D., Asirvadam, V.S., Ibrahim, R.B., Saad, N.B., Hassan, S.M., 19-21 Oct. 2015 2015. Analyzing wirelesshart high-level data link control frame payload. In: 2015 IEEE International Conference on Signal and Image Processing Applications (ICSIPA). pp. 27–31.

Dobslaw, F., Gidlund, M., Zhang, T., 24-28 Aug. 2015 2015. Challenges for the use of data aggregation in industrial wireless sensor networks. In: 2015 IEEE International Conference on Automation Science and Engineering (CASE). pp. 138–144.

Du, X., Liu, F., 17-19 Sept. 2010 2010. Industrial wireless networks wia-pa cross-layer design research. In: 2010 Proceedings of the 2nd IEEE International Conference on Information and Financial Engineering (ICIFE). pp. 344–347.

Evans-Pughe, C., 2003. Bzzzz zzz [zigbee wireless standard]. IEE Rev. 49 (3), 28–31.

Feng, W., Cao, J., Zhang, C., Liu, C., 2009. Joint optimization of spectrum handoff scheduling and routing in multi-hop multi-radio cognitive networks, 85–92.

Firdaus, Nugroho, E., Sahroni, A., 26-30 Nov. 2014 2014. Zigbee and wifi network interface on wireless sensor networks. In: Proceeding of the 2014 Makassar International Conference on Electrical Engineering and Informatics (MICEEI). pp. 54–58.

Gungor, V.C., Hancke, G.P., 2009. Industrial wireless sensor networks: challenges, design principles, and technical approaches. IEEE Trans. Ind. Electron. 56 (10), 4258–4265.

Guo, P., Cao, J., Zhang, K., Liu, X., April 27, 2014-May 2, 2014 2014. Enhancing zigbee throughput under wifi interference using real-time adaptive coding. In: IEEE INFOCOM 2014 - IEEE Conference on Computer Communications. pp. 2858–2866.

Gupta, A., Jha, R.K., 2015. A survey of 5g network: architecture and emerging technologies. IEEE Access 3, 1206–1232.

Hancke, G.P., Mbuya, C.F., 1-4 June 2014 2014. Dynamic spectrum allocation for smart meter networks and wsns in the presence of household consumer networks. In: 2014 IEEE Proceedings of the 23rd International Symposium on Industrial Electronics (ISIE). pp. 1459–1462.

Heng, W., Jian, Y., Ping, W., Zhiyong, L., Kim, K.C., 20-22 Aug. 2010 2010. An adaptive deterministic scheduling scheme for wia-pa industrial wireless networks. In: 2010 Proceedings of the 3rd International Conference on Advanced Computer Theory and Engineering(ICACTE). Vol. 2. pp. V2–332–V2–336.

Hu, H., Min, Y., Xie, X., Wang, F., Yuan, J., 2008. Distributed cooperative dynamic spectrum management schemes for industrial wireless sensor networks. In: Proceedings of the Second International Conference on Future Generation Communication and Networking, 2008. FGCN'08. vol. 2. IEEE, pp. 381–386.

Hua, W., Feng, L., Yang, S., 11-13 Dec. 2009 2009. A design method of industrial wireless networks based on wia-pa. In: Proceedings of the International Conference on Computational Intelligence and Software Engineering, 2009. CiSE 2009. pp. 1–4.

Islam, S.M.R., Kwak, D., Kabir, M.H., Hossain, M., Kwak, K.S., 2015. The internet of things for health care: a comprehensive survey. IEEE Access 3, 678–708.

J, x00C, kerberg, Gidlund, M., Bj, M., x00F, rkman, 26-29 July 2011 2011. Future research challenges in wireless sensor and actuator networks targeting industrial automation. In: 2011 Proceedings of the 9th IEEE International Conference on Industrial Informatics. pp. 410–415.

Jaber, M., Imran, M.A., Tafazolli, R., Tukmanov, A., 2016. 5g backhaul challenges and emerging research directions: a survey. IEEE Access 4, 1743–1766.

Jiang, T., Wang, Z., Cao, Y., 2015. Cognitive Radio Networks: Efficient Resource Allocation in Cooperative Sensing, Cellular Communications, High-Speed Vehicles, and Smart Grid. CRC Press.

Jindal, V., Verma, A. K., 15-17 Aug. 2015 2015. The underlying technologies in wsns: Zigbee vs. wireless hart. In: 2015 Proceedings of the 12th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD). pp. 2208–2213.

Juncheng, J., Weihua, Z., 10-15 April 2011 2011. Capacity of multi-hop wireless network with frequency agile software defined radio. In: Proceedings of the 2011 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS). pp. 41–46.

Kaur, P., Udin, M., Khosla, A., 10-12 Dec. 2009 2009. An efficient spectrum mobility management strategy in cognitive radio networks. In: 2009 Proceedings of the First UK-India International Workshop on Cognitive Wireless Systems (UKIWCWS). pp. 1–6.

Kruger, C.P., Abu-Mahfouz, A.M., Hancke, G.P., 17-19 March 2015 2015. Rapid prototyping of a wireless sensor network gateway for the internet of things using off-the-shelf components. In: 2015 IEEE International Conference on Industrial Technology (ICIT). pp. 1926–1931.

Kumar, A., Hancke, G.P., 2014. An energy-efficient smart comfort sensing system based on the ieee 1451 standard for green buildings. IEEE Sens. J. 14 (12), 4245–4252.

Kumar, S., Ovsthus, A.A., Kristensen, L. M, K., 2014. An industrial perspective on wireless sensor networks; a survey of requirements, protocols, and challenges. IEEE Commun. Surv. Tutor. 16 (3), 1391–1412.

Lertsinsrubtavee, A., Malouch, N., Fdida, S., 5-7 Oct. 2011 2011. Spectrum handoff strategy using cumulative probability in cognitive radio networks. In: 2011 3rd International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT). pp. 1–7.

Li, M., Jiang, T., Tong, L., 21-22 Dec. 2013 2013. Spectrum handoff scheme for prioritized multimedia services in cognitive radio network with finite buffer. In: 2013 IEEE Proceedings of the 11th International Conference on Dependable, Autonomic and Secure Computing (DASC). pp. 410–415.

Liang, W., Zhang, X., Xiao, Y., Wang, F., Zeng, P., Yu, H., 2011. Survey and experiments of wiaâpa specification of industrial wireless network. Wirel. Commun. Mob. Comput. 11 (8), 1197–1212.

Liu, H.J., Wang, Z.X., Li, S.F., Yi, M., 19–21 Nov. 2008 2008. Study on the performance of spectrum mobility in cognitive wireless network. In: Proceedings of the 11th IEEE Singapore International Conference on Communication Systems, 2008. ICCS 2008. pp. 1010–1014.

Maheshwari, P., Singh, A. K., 27-29 Nov. 2014 2014. A survey on spectrum handoff techniques in cognitive radio networks. In: Proceedings of the 2014 International Conference on Contemporary Computing and Informatics (IC3I). pp. 996–1001.

Maia, A.M., Vieira, D., de Castro, M.F., Ghamri-Doudane, Y., 2016. A fair qos-aware dynamic lte scheduler for machine-to-machine communication. Comput. Commun. 89, 75–86.

Miao, Y., Wei, L., Weijie, X., 7-9 July 2010 2010. Design and implementation of industrial wireless network system based on wia-pa. In: Proceedings of the 2010 8th World Congress on Intelligent Control and Automation (WCICA). pp. 6799–6803.

Muhammad Faisal, A., Aslam, B., Zou, C. C., 11-14 Jan. 2013 2013. Transparent cross-layer solutions for throughput boost in cognitive radio networks. In: 2013 IEEE Proceedings of the 10th Consumer Communications and Networking Conference (CCNC). pp. 580–586.

Mukherjee, T., Nath, A., 2015. Issues and challenges in spectrum management in cognitive radio networks. management 6, 7.

Nagarajan, R., Dhanasekaran, R., 2-4 April 2015 2015. Optimization of power in wireless industrial automation networks. In: Proceedings of the 2015 International Conference on Communications and Signal Processing (ICCSP). pp. 0680–0684.

Nejatian, S., Syed-Yusof, S.K., Latiff, N.M.A., Asadpour, V., 2014. Push: Proactive unified spectrum handoff in cr-manets, 33–40.

Nellore, K., Hancke, G., 2016a. A survey on urban traffic management system using wireless sensor networks. Sensors 16 (2), 157.

Nellore, K., Hancke, G., 2016b. Traffic management for emergency vehicle priority based on visual sensing. Sensors 16 (11), 1892.

Nobre, M., Silva, I., Guedes, L.A., 27-30 July 2014 2014. Reliability evaluation of wirelesshart under faulty link scenarios. In: 2014 Proceedings of the 12th IEEE International Conference on Industrial Informatics (INDIN). pp. 676–682.

Nomura, K., Sato, F., 10-12 Sept. 2014 2014. A performance study of zigbee network under wi-fi interference. In: 2014 Proceedings of the 17th International Conference on Network-Based Information Systems. pp. 201–207.

Oloyede, M.O., Hancke, G.P., 2016. Unimodal and multimodal biometric sensing systems: a review. IEEE Access 4, 7532–7555.

Oo, T. Z., Hong, C. S., Lee, S., 28-30 Jan. 2013 2013. Alternating renewal framework for estimation in spectrum sensing policy and proactive spectrum handoff. In: The International Conference on Information Networking 2013 (ICOIN).pp. 330–335.

Opperman, C.A., Hancke, G. P., 13-15 Sept. 2011 2011. Using nfc-enabled phones for remote data acquisition and digital control. In: AFRICON, 2011. pp. 1–6.

Oualha, N., Olivereau, A., Wehner, M., Bartzsch, T., Burggraf, D., Zeisberg, S., Gheorghe, L.C., Lusanschi, E., Tudose, D., 2012. Aaa-based infrastructure for industrial wireless sensor networks. In: Future Network & Mobile Summit (FutureNetw), 2012. IEEE, pp. 1–8.

Papadopoulos, G., 14-18 June 2015 2015. Challenges in the design and implementation of wireless sensor networks: A holistic approach-development and planning tools, middleware, power efficiency, interoperability. In: 2015 Proceedings of the 4th Mediterranean Conference on Embedded Computing (MECO). pp. 1–3.

Perera, C., Liu, C.H., Jayawardena, S., Chen, M., 2014. A survey on internet of things from industrial market perspective. IEEE Access 2, 1660–1679.

Petersen, S., Carlsen, S., 2011. Wirelesshart versus isa100.11a: the format war hits the factory floor. IEEE Ind. Electron. Mag. 5 (4), 23–34.

Phala, K.S.E., Kumar, A., Hancke, G.P., 2016. Air quality monitoring system based on iso/iec/ieee 21451 standards. IEEE Sens. J. 16 (12), 5037–5045.

Pham, T.N., Tsai, M.F., Nguyen, D.B., Dow, C.R., Deng, D.J., 2015. A cloud-based smart-parking system based on internet-of-things technologies. IEEE Access 3, 1581–1591.

Potdar, S.M., Patil, K.P., 8-10 Aug. 2013 2013. Efficient spectrum handoff in cr network based on mobility, qos and priority using fuzzy logic and neural network. In: 2013 Proceedings of the Sixth International Conference on Contemporary Computing (IC3). pp. 53–58.

Potter, C.H., Hancke, G.P., Silva, B.J., 25-28 Feb. 2013 2013. Machine-to-machine: Possible applications in industrial networks. In: 2013 IEEE International Conference on Industrial Technology (ICIT). pp. 1321–1326.

Qianbin, C., Jiao, C., Rong, C., 14-16 Aug. 2013 2013. A unified framework for secondary user accessing/handoff in cognitive heterogeneous network. In: 2013 Proceedings of the 8th International ICST Conference on Communications and Networking in China (CHINACOM). pp. 212–217.

Rappaport, T.S., Sun, S., Mayzus, R., Zhao, H., Azar, Y., Wang, K., Wong, G.N., Schulz, J.K., Samimi, M., Gutierrez, F., 2013. Millimeter wave mobile communications for 5g cellular: it will work!. IEEE Access 1, 335–349.

Rawat, D. B., Amin, T., Song, M., April 26, 2015-May 1, 2015 2015. The impact of secondary user mobility and primary user activity on spectrum sensing in cognitive vehicular networks. In: Proceedings of the 2015 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS). pp. 588–593.

Ray, A., J, x00C, kerberg, Gidlund, M., Bj, M., x00F, rkman, 25-28 Feb. 2013 2013. Initial key distribution for industrial wireless sensor networks. In: Proceedings of the 2013 IEEE International Conference on Industrial Technology (ICIT). pp. 1309–1314.

Reinhold, R., Kays, R., 13-15 Nov. 2013 2013. Improvement of ieee 802.15.4a ir-uwb for time-critical industrial wireless sensor networks. In: Wireless Days (WD), 2013 IFIP. pp. 1–4.

Rezaeirad, M., Mazloom, S., Iqbal, M.A., Perkins, D., Bayoumi, M., 13-15 Aug. 2014 2014. Investigating the feasibility of leap; in zigbee specification. In: 2014 IEEE Proceedings of the 15th International Conference on Information Reuse and Integration (IRI). pp. 406–412.

Riaz, F., Niazi, M.A., 2015. Spectrum mobility in cognitive radio-based vehicular cyber physical networks: A fuzzy emotion-inspired scheme, 264–270.

Rodriguez, P.M., Val, I., Lizeaga, A., Mendicute, M., 27-29 May 2015 2015. Evaluation of cognitive radio for mission-critical and time-critical wsan in industrial environments under interference. In: Proceedings of the 2015 IEEE World Conference on Factory Communication Systems (WFCS). pp. 1–4.

Sarijari, M.A., Abdullah, M.S., Lo, A., Rashid, R.A., 8-11 Sept. 2014 2014. Experimental studies of the zigbee frequency agility mechanism in home area networks. In: 2014

IEEE Proceedings of the 39th Conference on Local Computer Networks Workshops (LCN Workshops). pp. 711–717.

Sgora, A., Vergados, D.D., 2009. Handoff prioritization and decision schemes in wireless cellular networks: a survey. IEEE Commun. Surv. Tutor. 11 (4), 57–77.

Sheng, Z., Mahapatra, C., Zhu, C., Leung, V.C.M., 2015. Recent advances in industrial wireless sensor networks toward efficient management in iot. IEEE Access 3, 622–637.

Sikorski, J.J., Haughton, J., Kraft, M., 2017. Blockchain technology in the chemical industry: machinetomachine electricity market. Appl. Energy 195, 234–246, 2017/06/01.

Silva, B., Fisher, R.M., Kumar, A., Hancke, G.P., 2015. Experimental link quality characterization of wireless sensor networks for underground monitoring. IEEE Trans. Ind. Inform. 11 (5), 1099–1110.

Silva, B., Hancke, G.P., 2016. Ir-uwb-based non-line-of-sight identification in harsh environments: principles and challenges. IEEE Trans. Ind. Inform. 12 (3), 1188–1195.

Son Duc, N., Tung-Linh, P., Kim, D.S., 29-31 July 2013 2013. Dynamic spectrum handoff for industrial cognitive wireless sensor networks. In: 2013 Proceedings of the 11th IEEE International Conference on Industrial Informatics (INDIN). pp. 92–97.

Song, J., Han, S., Mok, A., Chen, D., Lucas, M., Nixon, M., Pratt, W., 22-24 April 2008 2008. Wirelesshart: Applying wireless technology in real-time industrial process control. In: Real-Time and Embedded Technology and Applications Symposium, 2008. RTAS '08. IEEE. pp. 377–386.

Song, Y., Xie, J., 6-10 Dec. 2010 2010a. Common hopping based proactive spectrum handoff in cognitive radio ad hoc networks. In: Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE. pp. 1–5.

Song, Y., Xie, J., 15-19 March 2010 2010b. Proactive spectrum handoff in cognitive radio ad hoc networks based on common hopping coordination. In: INFOCOM IEEE Conference on Computer Communications Workshops, 2010. pp. 1–2.

Song, Y., Xie, J., 2012. Prospect: a proactive spectrum handoff framework for cognitive radio ad hoc networks without common control channel. IEEE Trans. Mob. Comput. 11 (7), 1127–1139.

Soto, V.S., Muller, I., Pereira, J.M.W.C.E., Netto, J.C., 3-7 Nov. 2014 2014. Control over wirelesshart network through a host application: A wirelesshart network control proposal. In: 2014 Brazilian Symposium on Computing Systems Engineering. pp. 91–96.

Southwell, R., Huang, J., Liu, X., 25-30 March 2012 2012. Spectrum mobility games. In: INFOCOM, 2012 Proceedings IEEE. pp. 37–45.

Sun, Y., Song, H., Jara, A.J., Bie, R., 2016. Internet of things and big data analytics for smart and connected communities. IEEE Access 4, 766–773.

Tang, Z., Mei, Z., Zeng, P., Wang, H., 25-27 June 2010 2010. Industrial wireless communication protocol wia-pa and its interoperation with foundation fieldbus. In: Proceedings of the 2010 International Conference on Computer Design and Applications (ICCDA), vol. 4. pp. V4-370-V4-374.

Tran, M.P., Minh, T.P.T., Hea-Min, L., Kim, D.S., 8-11 Sept. 2015 2015. Effective spectrum handoff for cognitive uwb industrial networks. In: 2015 IEEE Proceedings of the 20th Conference on Emerging Technologies & Factory Automation (ETFA). pp. 1–4.

Trigui, E., Esseghir, M., Boulahia, L. M., 8-11 Sept. 2013 2013. Cognitive radio spectrum assignment and handoff decision. In: 2013 IEEE Proceedings of the 24th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC). pp. 2881–2886.

Verma, P.K., Verma, R., Prakash, A., Agrawal, A., Naik, K., Tripathi, R., Alsabaan, M., Khalifa, T., Abdelkader, T., Abogharaf, A., 2016. Machine-to-machine (m2m) communications: a survey. J. Netw. Comput. Appl. 66, 83–105, 2016/05/01.

VrabiÄ, R., Kozjek, D., Butala, P., 2017/04/28/ 2017. Knowledge elicitation for fault diagnostics in plastic injection moulding: A case for machine-to-machine communication. CIRP Annals - Manufacturing Technology.

Wagner, R.S., Barton, R.J., 3-10 March 2012 2012. Performance comparison of wireless sensor network standard protocols in an aerospace environment: Isa100.11a and zigbee pro. In: Aerospace Conference, 2012 IEEE. pp. 1–14.

Wang, C.-W., Wang, L.-C., 2012. Analysis of reactive spectrum handoff in cognitive radio networks. IEEE J. Sel. Areas Commun. 30 (10), 2016–2028.

Wang, L.C., Wang, C.W., 7-9 Dec. 2008 2008. Spectrum handoff for cognitive radio networks: Reactive-sensing or proactive-sensins? In: Proceedings of the 2008 IEEE International Performance, Computing and Communications Conference. pp. 343–348.

Wang, S., Cao, F., Fan, Z., 9-13 June 2013 2013. Periodic partial soft sensing and spectrum handoff in cognitive relay networks. In: Proceedings of the 2013 IEEE International Conference on Communications (ICC). pp. 2683–2688.

Won-Yeol, L., Akyildiz, I.F., 2012. Spectrum-aware mobility management in cognitive radio cellular networks. IEEE Trans. Mob. Comput. 11 (4), 529–542.

Wu, Q., Ding, G., Du, Z., Sun, Y., Jo, M., Vasilakos, A.V., 2016. A cloud-based architecture for the internet of spectrum devices over future wireless networks. IEEE Access 4, 2854–2862.

Wyglinski, A.M., Nekovee, M., Hou, Y.T., 2008. Cognitive radio communications and networks. IEEE Commun. Mag. 46 (4), 30–31.

Xin, G., Zhang, X., Song, G., 12-14 Oct. 2011 2011. Design and implementation of wia-pa data link layer. In: Proceedings of the 2011 International Workshop on Open-Source Software for Scientific Computation (OSSC). pp. 47–51.

Xu, Q., Ren, P., Song, H., Du, Q., 2016. Security enhancement for iot communications exposed to eavesdroppers with uncertain locations. IEEE Access 4, 2840–2853.

Yan, Y., Yang, P., Li, X.Y., Zhang, Y., Lu, J., You, L., Wang, J., Han, J., Xiong, Y., 2015. Wizbee: wise zigbee coexistence via interference cancellation with single antenna. IEEE Trans. Mob. Comput. 14 (12), 2590–2603.

Yang, W., Dong-Seong, K., 14-16 Oct. 2013 2013. A self-stabilized firefly synchronization method for the isa100.11a network. In: Proceedings of the 2013 International Conference on ICT Convergence (ICTC). pp. 881–886.

Yang, Z., Song, Y., Wang, D., 16-19 Feb. 2015 2015a. An optimal operating frequency selection scheme in spectrum handoff for cognitive radio networks. In: Proceedings of the 2015 International Conference on Computing, Networking and Communications (ICNC). pp. 1066–1070.

Yang, Z., Song, Y., Wang, D., 16-19 Feb. 2015 2015b. An optimal operating frequency selection scheme in spectrum handoff for cognitive radio networks. In: Proceedings of the 2015 International Conference on Computing, Networking and Communications (ICNC). pp. 1066–1070.

Yau, K.L.A., Komisarczuk, P., Teal, P.D., 20-23 Oct. 2009 2009. Cognitive radio-based wireless sensor networks: Conceptual design and open issues. In: 2009 IEEE Proceedings of the 34th Conference on Local Computer Networks. pp. 955–962.

Yu, K., Gidlund, M., Akerbergy, J., Bjorkman, M., 2013. Low jitter scheduling for industrial wireless sensor and actuator networks. In: Industrial Electronics Society, IECON 2013-Proceedings of the 39th Annual Conference of the IEEE. IEEE, pp. 5594–5599.

Yunhuan, L., Cailian, C., Honghua, X., Baoqing, Y., Xinping, G., 25-27 July 2012 2012. A cognitive radio based reliability optimization for industrial wireless dsss/ch transmission links. In: Control Conference (CCC), 2012 31st Chinese. pp. 5542–5547.

Zahed, S., Awan, I., Min, G., 2012. Prioritized proactive scheme for spectrum handoff decision in cognitive radio networks, 335–341.

Zhang, Y., Zheng, J., Chen, H.-H., 2016. Cognitive Radio Networks: Architectures, Protocols, and Standards. CRC Press.

Zheng, T., Qin, Y., Zhang, H., Kuo, S.-Y., 2012. A self-configurable power control algorithm for cognitive radio-based industrial wireless sensor networks with interference constraints. In: Proceedings of the 2012 IEEE International Conference on Communications (ICC). IEEE, pp. 98–103.

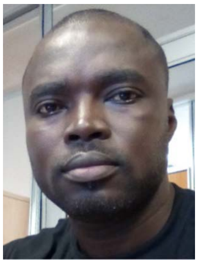
Zhi-jin, Z., Lu-ping, Z., Hai-quan, W., 2015. Spectrum handoff based on adaptive weights adjustment. IET Commun. 9 (5), 674–680.

Zhu, C., Leung, V.C.M., Shu, L., Ngai, E.C.H., 2015. Green internet of things for smart world. IEEE Access 3, 2151–2162.

Zhu, X., Dong, W., Mok, A.K., Han, S., Song, J., Chen, D., Nixon, M., 24-26 Aug. 2009 2009. A location-determination application in wirelesshart. In: 2009 Proceedings of the 15th IEEE International Conference on Embedded and Real-Time Computing Systems and Applications. pp. 263–270.

Zhuo, S., Shokri-Ghadikolaei, H., Fischione, C., Wang, Z., 2015a. Adaptive congestion control in cognitive industrial wireless sensor networks. In: 2015 IEEE Proceedings of the 13th International Conference on Industrial Informatics (INDIN). IEEE, pp. 900–907.

Zhuo, S., Shokri-Ghadikolaei, H., Fischione, C., Wang, Z., 22-24 July 2015 2015b. Adaptive congestion control in cognitive industrial wireless sensor networks. In: 2015 IEEE Proceedings of the 13th International Conference on Industrial Informatics (INDIN). pp. 900–907.



S. S. Oyewobi, is a PhD student in the department of Electrical Electronic and Computer Engineering, Advanced Sensor Network Group, University of Pretoria. South Africa. He obtained B.Eng Electrical and Computer Engineering in 2003, and M.Eng Electrical Engineering (Telecommunication Option) in 2013 from Federal University of Technology, Minna, Nigeria respectively. His research interest including, Advanced sensor Networks, Energy Managements for network nodes, Industrial wireless Sensors, and internet of things.

G. P. Hancke is an Assistant Professor with the City University of Hong Kong (Hong Kong SAR). His research interests are system security, embedded platforms and distributed sensing applications. He obtained B.Eng and M.Eng degrees from the University of Pretoria (South Africa) in 2002 and 2003, and a PhD in Computer Science with the Security Group at the University of Cambridge's Computer Laboratory in 2008.