Cognitive radio networks for tactical wireless communications

Helen Tang; Susan Watson
DRDC – Ottawa Research Centre

Defence Research and Development Canada
Scientific Report
DRDC-RDDC-2014-R185
December 2014

Cognitive radio networks for tactical wireless communications

Helen Tang; Susan Watson
DRDC – Ottawa Research Centre

Defence Research and Development Canada
Scientific Report
DRDC-RDDC-2014-R185
December 2014

Abstract

The modern battlefield is a demanding environment for tactical radio networks in that in addition to the variation in the wireless propagation environment, the radio must co-exist and contend with a high density of emitters having varying waveforms. Cognitive Radio (CR) is widely considered as a promising technology for providing the mechanisms to mitigate interference, and allow more flexible and dynamic radio resource allocation.

Many nations and organizations have put forward a roadmap for applying Cognitive Radio Networks (CRN) to tactical communications; an overview of these is given in this report. We will also document current Canadian defence Research and Development (R&D) programs in this area, and provide our perspectives and plans for future research. We look at the significance of cognitive radio networks for our future tactical wireless communications, in terms of the benefits, technological challenges, and the implications for security.

CRNs are expected to provide benefits such as Dynamic Spectrum Access for fast network deployment and ease of spectrum congestion, increased communications resilience in dynamic, heterogeneous environments, and may provide the basis for the tactical radio as a multi-functional radio-frequency (RF) unit, capable of supporting intelligent Cyber Electromagnetic (EM) attacks and defences. In our current and future research, we wish to provide solutions which empower the CRN to achieve all of these benefits without compromising security.

Significance to defence and security

Our future tactical wireless communication systems will have elements of the concept known as cognitive radio, but securing the cognitive radio network is an area of current research and development. In this document, we define the scope of the term cognitive radio and we look at its implications for tactical wireless communications in terms of the benefits, technological challenges, and security challenges. We provide an overview of some recent thinking from the international defence scientific community in this area, and describe our own approach to security solutions for cognitive radio networks. Our own roadmap, or outlook is given, which will guide our current and future research into faster, smarter, and more resilient tactical wireless communications.

Résumé

Le champ de bataille moderne est un environnement exigeant pour les réseaux de radiocommunications tactiques, car, en plus des variations dans l'environnement de propagation sans fil, le poste radio doit coexister et composer avec une forte concentration d'émetteurs utilisant diverses formes d'ondes. La radio intelligente (RI) est généralement considérée comme une technologie prometteuse pouvant fournir les mécanismes nécessaires pour réduire les interférences et permettre une affectation souple et dynamique des ressources radio.

De nombreux pays et organismes ont proposé une feuille de route pour utiliser les réseaux de radio intelligente (RRI) pour les communications tactiques, et le présent rapport en donne un aperçu. Nous documenterons aussi les programmes de recherche et développement (R.-D.) en cours de la défense canadienne dans ce domaine, et nous présenterons nos points de vue et nos plans pour les recherches futures. Nous examinons en outre l'importance des réseaux de radio intelligente pour nos communications sans fil tactiques futures, sur le plan des avantages, des défis technologiques et des implications pour la sécurité.

Les RRI devraient offrir des avantages, comme un accès dynamique au spectre pour le déploiement rapide de réseaux et la réduction de l'encombrement du spectre, une résilience accrue des communications dans des environnements hétérogènes dynamiques, en plus de fournir la base pour la radio tactique, comme un poste de radiofréquence (RF) polyvalent pouvant soutenir les attaques cyber-électromagnétiques (ACEM) intelligentes et la défense contre celles-ci. Dans le cadre de nos recherches actuelles et futures, nous désirons fournir des solutions qui permettront au RRI d' offrir tous ces avantages sans compromettre la sécurité.

Importance pour la défense et la sécurité

Nos futurs systèmes de communications sans fil tactiques comporteront des éléments du concept de « radio intelligente », mais la mise en place d'un réseau de radio intelligente fait déjà l'objet de recherche et développement. Dans le présent document, nous définissons la portée du terme « radio intelligente » et examinons ses incidences sur les communications sans fil tactiques du point de vue de ses avantages, de ses défis technologiques et de ses problèmes de sécurité. Nous donnons un aperçu de certaines réflexions récentes à ce sujet tirées de la communauté scientifique internationale de la défense et décrivons notre propre approche des solutions de sécurité aux réseaux de radio intelligente. Notre propre feuille de route, nos points de vue sont présentés, et ceux-ci orienteront nos recherches actuelles et futures de communications sans fil tactiques plus résilientes, intelligentes et rapides.

Table of contents

List of figures

List of tables

1 Introduction

With growing demands for the amount of data transferred in tactical wireless networks, spectrum shortage problems become more imminent. Mechanisms are needed to avoid interference, improve system-wide spectral efficiency and allow more flexible spectrum resource utilization. Cognitive Radio (CR) is widely considered as a promising technology for providing the mechanisms to solve the spectrum resource challenge on the modern battlefield, caused by the current inflexible spectrum allocation policy.

Tactical communications networks are operated in a dynamically changing environment, where interference and sudden changes in the network configuration and radio parameters take place. CRs, which have environment sensing and transmission adaptation capabilities, can address the dynamic nature of the network, offering new possibilities to enhance the performance of a modern tactical communication system [1]. CR communications platforms may be ideal candidates for future tactical networks.

Many nations and organizations have put forward a roadmap for applying Cognitive Radio Networks (CRN) to tactical communications. Some Canadian defence R&D programs exist in this area; however, to date we have not documented our perspectives and plans for future research. We attempt to address this gap.

This document is structured as follows. In this section we review the concept of cognitive radio for military networks. Related work, including that in other nations, is presented in Section 2. In Section 3, we review network architectures for cognitive radio networks. Section 4 provides a discussion of key challenges to the implementation of tactical cognitive radio networks. State-of-the-art security technologies for CRN are given in Section 5, and in Section 6 we provide some scenarios to illustrate the application of CRNs to tactical wireless communications. Finally, in Section 7 we propose a roadmap on how Canada can apply CRN to tactical wireless communications, and conclude in Section 8.

1.1 What is CR and CRN?

The term “Cognitive Radio” (CR) was first coined by Dr. Joseph Mitola in 1999 in a number of publications (e.g., [2], [3]) and his PhD thesis [4]. His broad vision was that CRs are intelligent radios that can autonomously make decisions using gathered information about the RF environment through model-based reasoning, and can also learn and plan according to their past experience.

Today, cognitive radio is an overloaded term with many potential meanings. Simply put, CRs can obtain information about their environment and adapt their operation accordingly to provide required services to end users. The adaptation may result in changes at many layers in the network protocol stack. Regarding spectrum use, CR systems can dynamically access new frequency bands, and at the same time protect higher priority users on the same bands from harmful interference. In addition to the ability to adapt, the concept of CR allows for the radio to “learn” in order to make good performance choices for the user’s objectives.

Along the same lines as Dr. Joseph Mitola, Haykin provided a comprehensive definition for CR [5]:

"Cognitive radio is an intelligent wireless communication system that is aware of its surrounding environment (i.e., outside world), and uses the methodology of understanding by- building to learn from the environment and adapt its internal states to statistical variations in the incoming RF stimuli by making corresponding changes in certain operating parameters (e.g., transmit power, carrier frequency, and modulation strategy) in real-time, with two primary objectives in mind: highly reliable communication whenever and wherever needed; efficient utilization of the radio spectrum."

In 2003, the Federal Communications Commission (FCC) introduced a much narrower definition of CR as "a radio that can change its transmitter parameters based on the environment in which it operates" [6]. Since the FCC's definition was coined, many studies in the literature have focused on this narrower view, whereby many adaptive radio resource access techniques to achieve such frequency agility have been proposed.

A cognitive radio needs knowledge, or awareness of the environment to make decisions. Knowledge can be gathered from policies and rules, sensors, the radio network infrastructure, propagation data, and the like. Knowledge might be gathered by the CR itself, obtained from a central controller (for example, a policy broker), or from peer CRs. Sensing data from other CRs may be gathered and fused locally, or data might be fused by a central controller and distributed in distilled format, for example, as a list of available channels.

Some of the key features that are typically associated with CR [7] are listed below. We can think of these six features in a progressive manner.

1. ***Senses:*** Maintain awareness of surrounding environment and internal state.

2. ***Collaborates*** with other devices to make decisions based on collective observations and knowledge.

3. ***Adapts*** to its environment to meet requirements and goals.

4. ***Reasons*** on observations to adjust adaptation goals.

5. ***Learns*** from previous experiences to recognize conditions and enable faster reaction times.

6. ***Anticipates*** events in support of future decisions.

The community is quite divided on how many of the above six features a radio must possess before it is considered as a CR. And also, the scope of these features is not clearly defined. Some believe that these features are only limited to the physical radio layer, others think of a CR as a device that can exhibit these features across the entire protocol stack.

Cognitive radios shall form cognitive radio networks (CRN) to complete the packet deliveries [8]. A CRN is generally a multi-hop wireless heterogeneous network, meaning it allows peer-to-peer communications and may include different types of radios. When CRs are connected and form a CRN, they may share knowledge, that is, the information gathered at each node, and decisions

may be made in a distributed manner. In an abstract sense, the cognition then becomes a function of the network, rather than the individual radio.

The following discussion aims to clarify some terminologies which are related to cognitive radio.

Cognitive radio and Dynamic Spectrum Access (DSA)

DSA is the real-time adjustment of spectrum utilization in response to changing circumstances and objectives [9]. In particular, DSA allows a group of radios to share spectrum, as a radio may locate vacant frequency bands and occupy them for the duration of a transmission, then release the spectrum resource. When the available spectrum is already licensed for use by a particular set of radios, DSA allows unlicensed (secondary) users to exploit the spectrum in an opportunistic manner, under the condition that the secondary users vacate the spectrum within a predetermined time if the primary user needs it.

A cognitive radio may or may not be capable of DSA. The sufficient aspects for cognitive radio are the context-awareness and decision-making, not a particular algorithm, such as fixed vs. dynamic spectrum access. Conversely, a radio capable of DSA may or may not be cognitive.

Insofar as spectrum access is a fundamental piece in a radio's functioning, a cognitive radio will be more capable if it performs DSA. Thus DSA is viewed as a key component of CR. One issue of concern for military radio users is the ability to guarantee service in a DSA environment where spectrum access is not predictable.

Cognitive radio and Software Defined Radio (SDR)

Software defined radio is a type of radio in which some or all of the physical layer functions (and above) are software defined. This is in contrast to hardware radio, in which changes in communications capabilities may only be achieved through changes to the hardware, or equivalently by software that is programmed once in the factory and cannot be changed due to radio architecture inflexibility. SDR is attractive for many of the same reasons as cognitive radio – it enables adaptation and reconfiguration. Cognitive radio is seen by many as the next step in reconfiguration flexibility, after SDR. It may be more accurate to say that a cognitive radio is in fact, a software defined radio, where the software implements the cognitive functioning of the radio. SDR is not necessary a CR if it lacks cognition. Also an adaptive radio is not necessarily cognitive as it can simply adapt according to some pre-defined algorithm or rule-set.

Tactical CRNs and commercial CRNs

While both the commercial world and the tactical world use the term "cognitive radio", they do not have exactly the same view of what it is. In the commercial world, cognitive radios are radios that use locally available spectrum, which is allocated but unused by the licensed user, in a homogeneous and predictable manner to provide services that would not otherwise be available. An example of this is the Institute of Electronic and Electrical Engineers (IEEE) 802.22 WRAN standard, under development, that aims to reuse vacant Television (TV) bands. There is a clear distinction of primary users and secondary users.

In contrast, the aim of tactical cognitive radios is to use the existing spectral allocations more efficiently and to improve communications support when changing location and network topology to support operations. There may be no clear distinction of primary users and secondary users. Among the military challenges of cognitive radio are not simply finding unused frequencies, but determining how to rank each radio message or data transmission in priority, to find a way for the highest-priority radio message and data traffic to get through first, and to allow lower-priority traffic to wait in line.

Table 1 below compares various aspects of tactical and commercial cognitive radios and CR networks [10]. We focus more on tactical CRN in this paper as we are aiming to apply CRN to tactical wireless communications.

Table 1: *Comparison of tactical and commercial wireless communications.*

Area	Tactical	Commercial
Environment	Hostile, extreme	More peaceful indoor or outdoor environment.
Security requirements	High	Low. Commercial network protocols usually do not address security until the very end.
Survivability requirements	High. Low probability of exploitation is an essential for mission success.	Low. Commercial system has little requirement for low probability of exploitation.
Reliability requirements	High. Mission success depends on reliable communications in contested environments.	Low. Commercial systems are designed to achieve a predictable reliability based on guaranteed access of spectrum. In CR, reliability is not guaranteed, therefore it is likely to be used for non-essential communications which will only be an inconvenience if it fails.
DSA	Military systems may benefit from DSA but also need waveform selection, protocol selection, network topology and other variables instead of just spectrum.	Mostly focussed on DSA.

Area	Tactical	Commercial
Other spectral use	Tactical communications systems are heterogeneous and cover different bands, channel spacing and waveforms.	The other users are licensed, quite predictable in frequency.

1.2 OODA loop for cognitive radio

A useful way to think about the cognition cycle for cognitive radio is to view it as an OODA loop (Figure 1) [12]. The OODA loop refers to the decision cycle of Observe, Orient, Decide, and Act, and is widely used in combat operations processes, often at the strategic level in military operations.

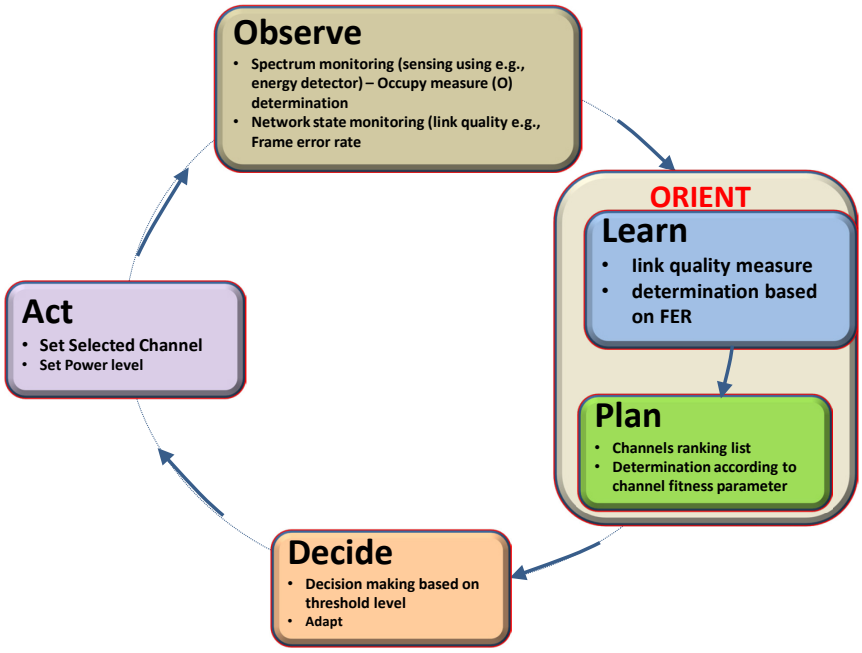

Figure 1: *Simplified cognitive cycle - OODA loop.*

Cognitive radio has the ability to sense the environment in which it is operating, measure the performance it is achieving, and assess whether it is able to perform additional tasks to better accomplish the user's or the network manager's objectives. To use the OODA loop terminology, we refer to the ability of the radio to:

- Observe the electromagnetic environment,

- Orient to the user's objectives, by learning and organizing what has been learnt (planning). Note that the learning could be an evolving process with the CR, which can consider the impact of the previous actions and experiences,
- Decide whether there is an adaption that is possible / practical to enhance performance, and then,
- Act on the decision.

1.3 Expected benefits and challenges of CRN for tactical wireless communications

Now that we have defined cognitive radio and cognitive radio networks, it should be clear that these concepts can enable a broad range of possible outcomes in tactical wireless communications. We wish to focus our efforts on solving the problems that will most benefit the CAF in their missions. The following high-level benefits and associated challenges of CR and CRN are the ones we find to be the most compelling for our tactical networks.

1. Improved spectrum utilisation

The spectrum limitation problem in tactical wireless communications becomes more and more serious as more bandwidth is needed to support more applications such as situational awareness, video sharing, etc. CRN is a promising technology to solve this problem and to meet growing user demands through dynamic spectrum access.

2. Increased communication systems resilience

Tactical communications networks are operated in a dynamically changing environment, where interference and sudden changes in the network configuration and radio parameters take place due to mobility of platforms, and variation in other users of the RF environment. CRNs will need to manage interference and avoid detection, thus increasing security and mission effectiveness.

3. Supporting cyber EM

Cognitive radio for tactical networks opens up new possibilities in merging network defence, network attack and Electronic Warfare (EW) functionality. There is the opportunity to integrate communications and electronic warfare sensors, and through the CR network, to collaboratively obtain a unified view of electronic support measures/tactical SIGINT (ESM) in the area of operation. A CRN may use its accumulated information for its own communication needs together with its unified ESM view to support Cyber EM operations [11].

Along with these benefits of cognitive radio, there are associated challenges and risks, as in Table 2. Some of the challenges of CR will be discussed in more detail in Section 4.

Table 2: *Summary of key benefits, challenges and risks for tactical cognitive radio.*

Benefits	Challenges and Risks
Improve spectrum utilisation: dynamic, operation-adapted spectrum access.	Risk of interference to undetected receivers Security issue resulted from spectrum sharing
Increase communication systems resilience: interference and detection avoidance	Technology challenges on adaptation and optimization
Support Cyber EM: CRN may collaboratively obtain a unified view of ESM in its area of operation	Vulnerability of CR coordination (control) channel Handling of malicious emitters/ EW

2 Related work

We will now review some of the literature from relevant defence research programs, examining what has been accomplished to date. The scope and depth of the papers is broad-ranging – from position papers to simulated results and fully operational demonstrators. Most nations are involved in some aspect of cognitive radio research, and many are involved in collaborative research programs.

2.1 US DARPA WNaN

The US Defence Advanced Research Projects Agency (DARPA) Advanced Wireless Network System (AWNS) / Wireless Network after Next (WNaN) system [12][13] is a mature demonstration of cognitive radio functionality. It was the first defence research program to demonstrate dynamic spectrum access experimentally, and it represents the largest military Mobile Ad hoc Network (MANET) as of today.

The WNaN demonstrator has been described as being cognitive at every layer of the protocol stack. Certainly, the program has produced extensive and valuable results in many areas of relevance to cognitive radio. The program has focussed on several objectives including:

1. Performance optimization in the presence of interference,

2. Resilience and scalability, and

3. Cost effectiveness, and support for periodic technology insertion.

We now elaborate on WNaN contributions to the state of the art in two areas: DSA and adaptive and disruption tolerant networking.

2.1.1 DSA

One approach to MANET frequency channel assignment is to assign a single common frequency to all nodes in a cluster or group, thereby maximizing connectivity. It is noted in [14] that more commonality in frequencies is better for connectivity, but reduces spatial re-use. The WNaN approach is concerned with balancing these two requirements in a dense radio environment. In [12], the author expresses the opinion that the spectrum efficiency of large numbers of users is "the appropriate metric to target in planning for future Cognitive Radio technology."

As such, each WNaN radio is equipped with four transceivers to increase the degrees of freedom in channel selection – a particular node may be connected to two neighbour nodes on two different frequencies. The DSA module of a WNaN radio maintains a list of allowed frequencies, which is a subset of all the possible frequencies. The nodes assign transceivers to each of four frequencies, such that every node can reach every other node in a few hops, according to a distributed frequency assignment algorithm. Radios which are a few hops away can re-use the frequencies, as in cellular radio.

DSA in WNaN is seen as having the ability to mitigate interference. By not building in extra margin for interference, all devices using the spectrum can share it aggressively, with the effect of greater capacity for all nodes.

The DSA module includes a Spectrum Policy Engine that is able to track authorized channels, their frequencies, their corresponding locations and the relevant time windows where these frequencies are authorized. This is very useful when operating in a multi-national situation where various host nation frequency policies may apply. The WNaN system has demonstrated this performance in avoiding interfering with legacy communication networks and other forms of Electromagnetic (EM) interference.

2.1.2 Adaptive and disruption tolerant networking

WNaN tolerates and adapts to the common propagation artifacts of a rapidly changing ad hoc network topology through the use of disruption tolerant networking (DTN) and many other sophisticated network adaption principles.

The WNaN network operates entirely below the IP stack, such that it is seen as an Ethernet device to IP, providing multi-hop services to packets. That way, the IP layer software is not exposed to possibly rapidly changing multi-hop routes, and the WNaN network may be enhanced with mechanisms such as forwarding and caching.

The WNaN network incorporates the following networking features:

- Hazy-sighted Link State (HSLS) routing: limits the scope of link state update dissemination in terms of hop-distance,
- Multi-point Relay (MPR): limits the number of nodes that broadcast the link state updates,
- Epidemic routing in disconnected or disrupted network regions,
- Support for packet routing using a combination of link-state (for connected regions) and epidemic routing (for disconnected regions), and
- Support for multi-cast with two types of dissemination trees.

In addition to scalable routing protocols, the problem of the scalability of MANETs is addressed in WNaN via dynamic spectrum access and interference tolerance. From the analysis in [13], it seems feasible to build multi-channel multi-transceiver MANETs like WNaN that scale to the thousands of nodes for our military networks.

An interesting extension to WNaN is the Advanced Wireless Network System (AWNS) program which aims to develop wireless “cloud computing” applications, such as facial recognition, using the computing power available in the network of radios.

2.2 Cognitive Radio for dynamic Spectrum Management (CORASMA)

The COgnitive RAdio for dynamic Spectrum MAnagement (CORASMA) program [14] is a joint program of research of seven European countries, and managed by the European Defence Agency (EDA). CORASMA is intended as a flexible framework for cognitive radio solutions being developed by a collection of nations. As such, there needed to be a common base of functionality upon which the cognitive radio components were built. Also, these solutions needed to be tested and evaluated in a common environment with enough detail to realistically model the costs and benefits of the cognitive solutions, for example in terms of the extra signaling required, and the sensitivity to a loss of signaling. These needs were met by 1) the basic waveform, which is a non-cognitive, reference waveform for comparison with the cognitive solutions, and 2) the HiFi simulator, which represents in some detail the behaviour of the first three layers of the OSI protocol stack, the physical layer (layer 1) through the network layer (layer 3).

The basic waveform, or common base of functionality which was the starting point for the cognitive solutions, is a clustered ad-hoc network. As there was interest from each of the participating nations in the problem of dynamic frequency allocation (DFA), a basic DFA algorithm was implemented in the basic waveform for comparison against the cognitive solutions. The basic waveform supports a multiple-channel clustered ad-hoc network; each cluster is managed by a clusterhead. The clusterhead must choose the transmit channel in which its cluster must operate, and the power level at which all radio nodes inside the cluster must transmit. The adaptive algorithm which controls this is called Greedy-based Dynamic Channel Assignment (GBDCA) [14, 15]. The GBDCA algorithm assigns channels with a compact pattern for spatial re-use, but has the drawback that it is not based upon interference measurements.

One of the cognitive solutions studied was a learning algorithm for power and frequency allocation in clustered ad-hoc networks [16]. The learning algorithm finds a solution to the optimization problem wherein the clusterheads select cluster frequency channels and transmit powers that minimize the total transmit power of all the clusters. The clusterheads have available information acquired through sensing, and cooperation with other nodes within their cluster. The authors suggest a game theory based solution to the frequency and power assignment problem, based upon trial and error, which consists of a state machine implemented by each player in the game. The players are the clusterheads, and the actions in the game are the set of potential powers and frequencies. A per-player utility function was proposed which evaluates how well the constraints have been satisfied. The original trial and error algorithm was unstable, and the authors have proposed an enhanced version which avoids the problem of repeated channel switching. The algorithm was tested under some fixed and mobile cluster scenarios. The CORASMA HiFi simulator was used to analyze the performance of the algorithm at various layers, such as throughput at the MAC layer and IP layer, which compared favourably with respect to the basic waveform.

2.3 Finnish Ministry of Defence

On the development of burgeoning cognition radio technology for military operations, the Finnish Ministry of Defence provides an assessment in [17]. The authors point out that the features offered by cognitive radio differ according to the point of view of the individual stakeholder. For

example, mobile radio operators wish to optimize their use of the available radio spectrum. For military users, there are many requirements such as highly configurable radios that are easy to use, that may avoid detection and circumvent jamming attacks. Thus, requirements definition which points to military operational requirements is necessary in defining the capabilities and features of military cognitive radio.

Toward this end, the paper identifies fifteen features of cognitive radio, studies the proposed features of the cognitive radio in a military context, and categorizes them in three ways. Firstly the features are classified based upon whether they have arisen from user requirements, system requirements, or design requirements, according to the tenets of systems engineering. Then, to divide or further classify the features, they are sorted into eight categories of system effectiveness (namely performance, availability, adaptability, interoperability, usability, survivability, security, and safety). Finally, the authors study the proposed features according to a soft systems derived technique meant to identify all the stakeholders, in order to meet the needs of all the users of the cognitive radio, for example, military end users and military mid-level management.

The fifteen features of cognitive radio considered in [17] are:

1. Spectrum sensing, signal detection and classification,
2. Awareness, decision making and parameter selection,
3. Geo-location awareness,
4. Enhanced data rate, coverage, capacity, link reliability, quality of service,
5. Spectrum access, policy management,
6. Information sharing,
7. Multiple waveforms, radio resource management,
8. Interference avoidance and rejection,
9. Advanced antennas, beamforming, etc.,
10. Service and traffic prioritization/self-organizing networks,
11. Interoperability/cognitive RF gateways,
12. Reconfiguration, near-zero setup,
13. Security, circumventing hostile jamming, tactical self-protective jamming,
14. Cost, size, battery life, and
15. Spectrum trading, markets, revenue models.

The authors find that much of the effectiveness of the features above is measured in terms of their performance, and metrics like reliability, availability and quality of service. However, it is noted that we need to also think about the new ways that cognitive radio will support mission accomplishment. For example, cognitive radio supports changes in tactics, new ways to deploy radios and forces on the ground, which in turn supports timely mission accomplishment, with fewer casualties. Such considerations may need new metrics to assess how well the cognition is achieving its requirements, for example, situational awareness.

On the subject of the deployment of cognitive radio into operations, the authors note that a single replacement of legacy systems with new cognitive radios would be unreasonable, and that legacy systems will need to operate side by side with new technology. For this reason, interoperability will be important. It is also important that modern iterative development models be used, which enable the development of competencies, understanding, and implemented capabilities in tandem.

Although it is recognized that cognitive radio is an extension of software defined radio, which provides the utmost reconfigurability, the authors assume that the first generation of cognitive radios will be developed to support specific waveforms, and that they will be capable of transferring data traffic from one waveform to another based upon the operational situation.

2.4 Polish Ministry of Defence

The Polish MoD provides a roadmap to tactical cognitive radio in [18]. The focus is on efficient spectrum use, driven by the increasing amount of data generated by tactical wireless networks, including positioning, soldier health, intelligence, and video-monitoring data. The authors state that cognitive radio is the most promising technology available to solve the problem of limited spectrum.

The authors identify four main areas of research in opportunistic spectrum access:

1. Waveforms and protocols:
   - Physical (PHY), MAC, Network (NET) layer protocols, header compression, cross-layer optimization, encryption, network cluster formation, resource allocation, Over-the-air processing,
2. Decision making and learning:
   - Decision making methods (competitive, cooperative, coopetition), optimization algorithms, machine learning, policy definition and management, interference avoidance, primary user protection, maximum spectrum utility, description languages,
3. Sensing:
   - RF sensing, spectrum analysis and detection techniques, spectrum classification and decision making (cooperative, non-cooperative), and
4. Hardware and software platforms:

- RF front ends, radio modem Hardware (HW), Software (SW) architecture, SDR platforms, SW programming and SW/HW testing.

In particular, the authors note that cross-layer optimization will be very important to enable the network to provide various services supported by Over the Air (OTA) processing. Also, game theory is identified as a promising option for global optimization of the available spectrum.

The Polish roadmap refers to the Polish National SDR/CR program, which began in 2013 with two projects: Guarana and Dynamic Spectrum Management. This program would provide the Polish Armed Forces with prototypes of a vehicular SDR implementation, which in turn would provide a basis for the handheld or manpack SDR implementation, including Dynamic Spectrum Management (DSM). Guarana 2 would provide full CR functionality by the end of 2020.

In the area of dynamic spectrum management, the authors present results in two areas: opportunistic (decentralized) spectrum management, and Coordinated Dynamic Spectrum Access (CDSA). The CDSA work presented a hierarchical broker architecture for spectrum management of legacy military wireless networks, and has applications in a multi-national military scenario [19].

A cognitive radio testbed has been developed by the Polish Military University of Technology for the demonstration of new cognitive radio technologies. It is organized in a network of CR nodes comprised of USRP modules. These nodes may be connected via RF switch matrix that models the radio environment as well as the presence of interference, or they may be operated in a real wireless environment.

The Polish roadmap document notes that further research still needs to be done, as the level of standardization in distributed MANET is low, and their behaviour in simulated and real environments still needs examination. In addition, automated decision making, learning and optimization algorithms still require a great deal of computational resources. Finally, the introduction of CR into the military domain is complicated by the need for coexistence of legacy and future wireless network technologies. Cooperation will be required between disparate bodies in industrial and technical, administrative and legislative areas.

2.5 NATO and TTCP activities

NATO has a Research Task Group, IST-077 / RTG-035 on “Cognitive Radio in NATO” which started work in mid-2008. The first activity of that group was to write a report [11] identifying the benefits of CR for NATO purposes. It was agreed at the February 2009 meeting that the focus of the group’s work would be the dynamic coordination of radio networks from a coalition perspective, in particular to address the problem of spectrum scarcity, considering dynamic spectrum access as a possible feature but not limited to it. Later on, there was a follow-on group called IST-104 “Cognitive Radio in NATO II”, which ended in 2014. NATO also organized a symposium in May 2014 on “Cognitive Radio and Future Networks” (IST-123) that highlight various aspects of CRs as well as future networks.

TTCP C3I TP6 held a Cognitive Radio Workshop in 2008 [10]. The objectives of the workshop were to investigate developments in the area of cognitive radio technologies, and assess the

implications of these developments on the military use of the electromagnetic spectrum. In particular, the workshop considered the impact of CR concepts for communications in coalition environments.

Some of the key conclusions of the NATO and TTCP Reports [10] [11] are as follows.

Spectral congestion is a problem affecting current mission effectiveness. Cognitive radio technology has the potential to enhance mission effectiveness, not only by enabling spectrally efficient waveforms, but by supporting data fusion and information management, and efficient networking. Cognitive radio technologies are not limited to Dynamic Spectrum Access, and there is a more general concept of radio and network adaptability. Furthermore, while the term 'cognitive radio' has become synonymous with Dynamic Spectrum Access as it is applied in the commercial domain, military requirements for efficient spectrum use are substantially different than those arising in the commercial domain, due in no small part to the heterogeneous radio environment. That being said, there are expected to be some opportunities to exploit commonality between commercial and military hardware, for example, as software defined radios become sufficiently advanced to support military waveforms in a flexible way.

Cognitive radio networks provide a technological advantage, facilitate coalition interoperability, and could provide information to an RF Common Operating Picture, facilitating the work of battlespace spectrum planners. However, the information transfer and spectrum occupancy requirements need to be identified, to establish the requirements for adaptive radio devices. Along with this analysis, careful consideration should be given to the volume of management traffic that the CRN generates in providing its services, as well as to any new security vulnerabilities that the network parameter adaptability may introduce. Cognitive radio technologies should not be seen as a panacea to the problems of spectral congestion, and cannot replace effective information management in terms of reducing data volume through processing, and in terms of appropriate information handling.

In terms of assessing the capabilities of the cognitive radio network, new modelling, simulation and evaluation capabilities are required. A phased introduction of cognitive radio technologies is anticipated.

2.6 Canadian activities

Communication Research Centre (CRC) made significant contributions to both the NATO working group and the TTCP C3I TP6 Cognitive Radio Workshop listed above. It also completed a Technology Investment Fund (TIF) project entitled "Cognitive radio techniques for assured communications" (2006-2009). The objective of the TIF project was to investigate the potential of advanced radio devices to provide robust and reliable communications in highly congested spectral conditions. It provided a strong direction for continued R&D both in more responsive spectrum management and in advanced adaptive radio technologies. In addition to a review of the state of the art in cognitive radio highlighting the challenges for tactical radio, there were a number of novel technical achievements from the project. Examples include multi-node space-time channel measurements, and a spectrum segmentation method suitable for heterogeneous EM environments such as those expected in operations. There were also innovations in the areas of unaided rendezvous, cluster formation algorithms, signal co-existence

by spectral overlap, selection of cross-layer parameters for different propagation conditions between nodes, and several more areas. Brief descriptions of these, as well as references to publications may be found in [20].

Defence Research and Development Canada – Ottawa (DRDC Ottawa) contributed to the TTCP C3I TP6 Cognitive Radio Workshop and proposed a security framework for CRN [10]. It also presented the work on Security Enhancements for Spectrum Sensing at the NATO Symposium on "Cognitive Radio and Future Networks" [21]. Currently, DRDC Ottawa is leading a project entitled "Cross Layer Security Enhancement for Cognitive Radio Based Mobile Ad-hoc Networks (CR-MANETs) [22] which is a part of the Cyber program project Tactical Network Operations (TNO, 2013-2018). CR can be used in MANETs which enable wireless devices to dynamically manage networks without fixed infrastructure. The convergence of these two technologies, CR-MANETs, could provide powerful self-adaptation capabilities and improved survivability to the mobile forces. However, communications security in the face of both cyber and electronic warfare attack remains a concern for CR-MANETs. The goal for this project is to develop effective security solutions for CR-MANETs by exploring new authentication techniques using various attributes of communication links and novel cross-layer processing to enhance traditional security mechanisms in order to provide security services such as secure routing and attack detection. The potential impact of this project is provisioning of transformative security technologies for future military wireless communications.

3 Architectures of CRN

A Cognitive Radio Network (CRN) is not just an interconnection of cognitive radios – CRNs are composed of various kinds of communication systems and networks, and can be viewed as a sort of heterogeneous network [23]. The heterogeneity exists in wireless access technologies, networks, user terminals, applications, and service providers.

The objective of the design of cognitive radio network architecture is to improve the entire network utilization, rather than just link spectral efficiency. From the users' perspective, efficient network utilization means that they can always fulfill their communications needs anytime and anywhere through accessing CRNs. From the operators' perspective, they can provide better services to mobile users, and allocate radio and network resources to deliver more packets per unit bandwidth in a more efficient way.

The CRNs can be deployed in different architectures, and serve the needs of both licensed and unlicensed applications. The basic components of CRNs are mobile station (MS), base station/access point (BSs/APs) and backbone/core network. These three basic components compose three kinds of network architectures in CRNs: infrastructure-based, ad-hoc and hybrid architectures.

3.1 Infrastructure-based architecture

In this architecture, illustrated in Figure 2, the secondary user network is infrastructure-based, which means that the network consists of cells; each cell is managed through a central Base Station (BS) or Access Point (AP) which controls the medium access and the secondary mobile station (MS). The MSs are synchronized with their BS. The observations and analysis performed by each MS feeds the BS, so that it can make decisions such as how to avoid interfering with primary users. According to the decision, each MS reconfigures its communication parameters.

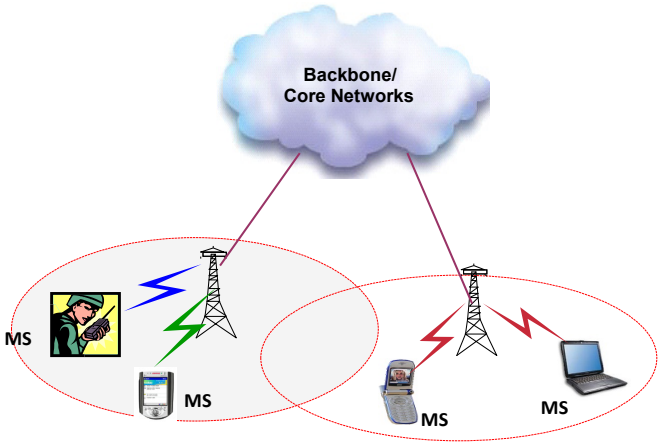

Figure 2: *Infrastructure-based network architecture.*

Each MS connects to a BS/AP with a direct link. MSs in the transmission range of the same BS/AP (one cell) communicate with each other through the BS/AP. Communications between different cells are routed through backbone/core networks. A good example of a cognitive, infrastructure-based network is that of the IEEE 802.22 standard [24] which follows a cellular architecture.

Table 3: *Aspects of infrastructure-based network architecture for CRNs.*

Pros	Central control, central decision making
Cons	Single point of failure, if the BS is down, may take too long time to for MS to communicate. Time consuming to set up the infrastructure.
Possible Remedies	Redundant (back-up) base station
Comments	Suitable for stable secondary spectrum, e.g., IEEE 802.22 is expected to provide broadband wireless access over unused TV bands in rural areas.

3.2 Ad-hoc architecture

In this decentralized architecture, illustrated in Figure 3, there is no central BS to manage the decision making. Each MS needs to have all the CR capabilities and is responsible for determining its actions based on the local observations. Two MSs who are within communication range can exchange their information directory; while those who are not within direct communication range can exchange information over multi-hop relay nodes. To eliminate the limitation of the local observation of each MS, collaborative algorithms [25] are usually used for this type of architecture, where the local observation results are exchanged among the MSs to broaden the knowledge on the network. We call this type of network Cognitive Radio Mobile Ad hoc Networks (CR-MANETs) [25].

Table 4: *Aspects of infrastructure-based network architecture for CRNs.*

Pros	No central control means no single point of failure. Multi-hop communication can be used for expanding the area of the secondary cognitive system. Reducing interference with primary station. Since each terminal transmits the signal with small transmit power, the interference toward the neighbouring terminals are also small. Distributed spectrum sensing and decision making: solve hidden node problem with cooperation of multiple sensing terminals.
Cons	High communication overhead for exchanging sensing data. Decision making may take a longer time. Common Control Channel may be

	needed and could be a single point of failure.
Possible Remedies	Distributed collaborative algorithm for efficient decision making.
Comment	Suitable for tactical environment where there is lots of dynamics and mobility and lack of infrastructure.

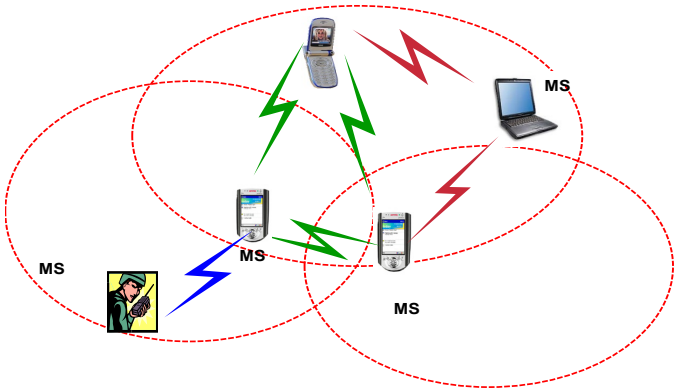

Figure 3: *Ad-hoc network architecture.*

3.2.1 Difference between traditional MANETs and CR-MANETs

Mobile Ad hoc Networks (MANETs) had been around for many years and CR-MANETs can be viewed as a subset of MANETs. All the issues in traditional MANETs (non-cognitive MANETs) in general are still of interest in CR-MANETs. However, some distinct characteristics of CRs introduce new non-trivial issues to CR-MANETs, so it is important to understand their differences. The key is that CR-MANETs are "spectrum aware". Below are some of the main features that set CR-MANETs apart from traditional MANETs:

1. There may be two kinds of users in CR-MANETs: primary users and secondary users, which are classified by their priorities in frequency bands.

2. Choice of transmission spectrum. In CR-MANETs, the available spectrum is dynamic. Traditional MANETs generally operate on a predetermined channel that remains unchanged with time. There is a need for protection of primary users.

3. Topology control: MANETs rely on local coordination to gather topology information as there is no central BS. It is easy in traditional MANETs to obtain the topology information through periodic beacon signals. However, this can be much harder to realize with CR-MANETs, as there may not be available channels for the beacon signals, which could lead to more collisions.

4. Multi-hop/multi-spectrum transmission: CR-MANETs require collaboration between routing and spectrum allocation in multiple hops.

5. CR-MANETs are more reliant on “delay tolerant” routing protocols as the spectrum at the next hop may not be available.

3.3 Hybrid architecture

This architecture, as illustrated in Figure 4, is a combination of the infrastructure and ad-hoc architectures, with wireless connections between the BSs/APs. In this architecture, the BSs/APs work as wireless routers and form a wireless backbone network. The MSs can either access the BSs/APs directly, or use other MSs as multi-hop relay nodes.

Table 5: *Aspects of hybrid network architecture for CRNs.*

Pros	This architecture has the best of both worlds (infrastructure and ad-hoc).
Cons	The need for BSs/APs (vehicle radios may play this role).
Comments	Recommended to heterogeneous networks with different network elements.

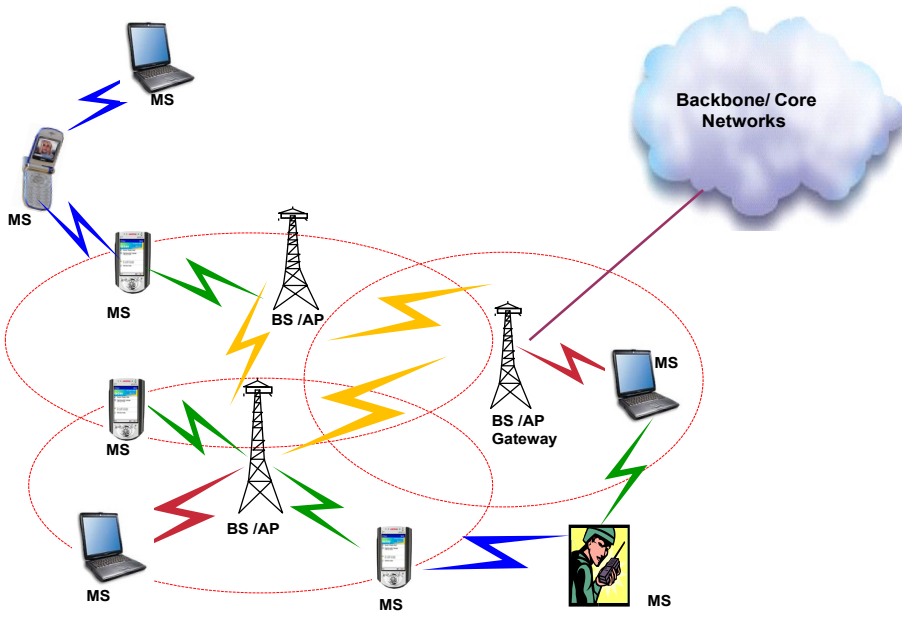

Figure 4: *Hybrid (infrastructure/ad-hoc) network architecture.*

4 Discussion of selected challenges

In this section, we will address in greater depth some of the challenges for realizing the benefits of CRN for tactical wireless communications as listed in Section 1.3.

4.1 Dynamic Spectrum Access (DSA)

As discussed in Section 1.1, cognitive radio is often associated with Dynamic Spectrum Access; the real-time adjustment of spectrum utilization in response to changing circumstances and objectives. Along with the many advantages DSA provides, there are many challenges to its efficient and secure implementation.

One significant challenge to the use of DSA is the implementation of spectrum sensing [26]. Most conceptions of CRNs have some kind of sensing capability, which is seen as a key feature to inform channel selection which avoids legacy radio users. The idea is to avoid interfering with legacy and peer radios, or, since we cannot altogether avoid interfering, how to keep the interference to a minimum.

One reason spectrum sensing is challenging is due to the limitations on conventional signal detection techniques. The classical energy detector for example does not reliably predict the presence of a legacy radio signal when the signal to noise ratio (SNR) of that signal is low, or negative, even when the spectrum is observed for an arbitrarily long time. For higher SNR signals which are detectable with an energy detector, valid spectrum opportunities that exist may still be difficult to observe. For example, the CR may not have the chance to observe a periodic spectral hole in the time domain if the dwell time in any given channel is too short. Or, an average power measurement may be deceptively high, causing the CR to declare the channel as occupied, due to a short burst of spurious interference. Pilot detectors and feature detectors are more reliable methods of spectrum sensing, but they require that features of the signal structure are known in the band of interest.

Another reason spectrum sensing is challenging is the nature of the wireless propagation channel. Of course, only the emitters within range of the sensor may be seen. Deep fades in the wireless channel make the region of detectability around the sensor quite variable. To compensate for this variability and avoid interference, the sensor hardware would have to be far more sensitive than the expected range of the transmitter to be detected. Even so, one can imagine the scenario known as the hidden node problem, where unbeknownst to the first node, a second (hidden) node, out of range of its sensors, is communicating with the same receiving node on the same frequency [26]. Due to the local and variable nature of individual sensor measurements, it is difficult to build an accurate picture of the spectrum occupancy needed to make efficient decisions about spectrum use.

Collaborative sensing is attractive as it allows the CRN to overcome some of the spectrum sensing limitations of the single-sensor approach. But a collaborative sensing strategy means the measurements must be exchanged between neighbours, incurring additional network overhead, and in a hostile environment, raising questions about the authenticity of the measurements received.

The quality of sensing is limited by the quality of the sensor hardware. However, even with a high-quality radio with high dynamic range, a powerful signal in an adjacent frequency channel may cause a less powerful signal to be missed due to adjacent channel interference. Even within a single tactical network, different sensors may have varying measurement qualities, which may need to be taken into account when fusing the sensing data.

It has been suggested that it might be possible to avoid sensing and just monitor one's own received signal quality. This strategy is related to the idea of interference-tolerance in radio networks [27]. For example, some modulation types still work reasonably well when partially overlapped [28]. There are many proponents of a military ISM-like band where interference constraints are not enforced. However, for the first generation of CRNs, we may still need some kind of guidance in the form of spectral use policy on appropriate behaviour. Without a policy for use, the spectrum resource may be unfairly allocated. Policy engines provide guidance for radios to make decisions about which channels are available for which transmissions. While the ideal opportunistic spectrum access scheme would allow access to any band on a non-interference basis, this is highly unlikely to be legally possible. Another challenge presented by DSA is that the multi-channel environment itself provides additional complexity to the network, for example, for routing. If we allow each link to be negotiated on a number of different frequencies, we must ensure that the messages are still deliverable throughout the network within a reasonable number of hops. Also, a coordination strategy will be required to ensure that links can be made between all radios – this process is known as rendezvous. In a military CRN, multi-cast operation must be supported. If the radios reachable by multi-cast are not all listening on the same frequency, the implementation of this feature would be a challenge.

Since in the mobile CRN radio links are made dynamically, if we wish to present a reliable service to upper layers, some cross-layer network management techniques may be required. Finally, although distributed spectrum optimization schemes rely on data exchange between nodes, network delay and traffic overhead in supporting the DSA features of the CRN must be kept to a reasonable level.

4.2 Security

Security is one of the major technical challenges that must be overcome to fully realize the benefits of cognitive radio networks, especially for tactical wireless communication where the operation environment is often hostile. For this reason, we need to explicitly consider security in our research from the beginning rather than as an afterthought.

4.2.1 Difference between traditional wireless network security and CRN security

The same factors that give CRs outstanding potential can be used maliciously to attack CR networks, such as cognition and configurability. For example, locally-collected and exchanged spectrum sensing information is used to construct a perceived environment that will impact CR behaviour. This opens opportunities to malicious attackers. As a result, there are some differences between a traditional wireless network and the CR network in terms of network security [29]:

- The potential of far reaching and long-lasting impact of an attack is higher in CR networks; this is mainly due to the learning and adaptability of CRs. CR uses the experience from the past to reason and anticipate future actions. As a result, attacks can have the opportunity for long-term impact.
- Some simple spectral manipulation, such as generation of signals, can cause a profound effect on network performance and behaviour in CR networks; this is because an attacker can generate signals to influence the perceived environment by the CRs, which can cause effects that propagate through the network.

These factors of CR networks also raise some new topics for security research that have not been studied before, such as: cooperative spectrum sensing, on-demand channel contention, incumbent and self-coexistence mechanisms and spectrum etiquette mechanisms, etc.

In order to provide security services for CRN, it is important to meet the following requirements as identified in [29]:

- The ability to authenticate the local observations that are used to form perceived environments,
- The ability to strongly secure collaboration exchanges between CR elements,
- The ability to authenticate the validity of observations exchanged between CR elements, and
- The ability to perform self-analysis of behaviour.

4.2.2 Three main attack and defence schemes for CRN

An extensive survey on CRN security can be found in [30]. Here we list three main attacks with their characteristics and proposed defence schemes.

1) Incumbent Emulation (IE) attacks: a malicious terminal emits signals that emulate the characteristics of the Incumbent's signal to fool other secondary users and acquire full spectrum use. IE attacks can severely interfere with the spectrum sensing process and significantly reduce the channel resources available to authentic secondary users. This attack is related to the problem of distinguishing primary signals from secondary signals. There are some techniques proposed for "fine/feature" sensing that may be adequate to detect Primary User Emulation (PUE) attacks, such as: verification of signal characteristics through novel physical layer authentication techniques, which incorporates cryptographic and wireless link signatures [31, 32], location integrity checking to decide on the credibility of a user [33].

2) Spectrum Sensing Data Falsification (SSDF) attacks: intruders send false local spectrum sensing resulting in cooperative spectrum sensing decisions by CRs.

   Distributed Spectrum Sensing (DSS) can increase the reliability of the sensing decision. The sensitivity of the CR terminals can be kept moderate to keep cost low. However, cooperative sensing in hostile environments is subject to SSDF attacks. To counter SSDF attacks effectively, [34] proposed a two-level defense. At the first level, all local spectrum sensing results must be authenticated. The purpose of this security measure is to prevent replay attacks or false data injection by entities outside the CR network. The second level of defense

is the deployment of a data fusion scheme that is robust against SSDF attacks. Existing data fusion schemes are vulnerable against SSDF attacks. They can be improved in two ways. One way is to employ a sequential probability ratio test (SPRT), which is a data fusion scheme that supports a variable number of local spectrum sensing results. SPRT has the desirable property of guaranteeing both a bounded false alarm probability and a bounded miss detection probability in a non-adversarial environment. Even if each sensing terminal has low spectrum sensing accuracy, SPRT can provide a guarantee by collecting more local spectrum sensing results. The other way to increase robustness of the data fusion process is to introduce a reputation-based scheme into the DSS process.

We have proposed a consensus-based security mechanism to counter SSDF attacks [35].

The basic idea is for the secondary users to collectively filter out the falsified data inserted by SSDF attacks and make the correct decision about the presence of primary users, which can be viewed as a typical multi-agent coordination situation. Since the algorithms can be constructed based on local communication of neighbouring agents, they have low implementation complexity and good robustness, and the overall system may still function when a local failure occurs.

3) Common Control Channel Jamming (CCCJ) attacks: a Common Control Channel is expected to be present in most CRNs for exchanging the sensing information and reserving the channel before actual data transfer. The provision of Common Control Channel security is essential to ensure any subsequent security among the communicating CR nodes. An attacker can flood the control channel with white/colored noise or forge the MAC frames in multi-hop networks where it is hard to authenticate MAC frames. The jamming signal will increase the received SNR at the local energy detection sensing nodes, which will increase the local false alarm probability, and thus, force the entire CRN to abandon a given sensed channel in the false belief of the presence of primary's signal in that channel. In addition, the learning capability of CRs, while essential in performing cognitive tasks, amplifies the effect of jamming attacks well beyond the instance of attack. For this reason, the Common Control Channel should use a robust spread spectrum coding. The media access scheme should be robust and provide fair access.

   [36] Proposed a framework for a secure common control channel in CRNs, in which two cognitive radio nodes can authenticate each other prior to any confidential channel negotiations to ensure subsequent security against attacks. The framework provides the channel's security by utilising an authentication and confidentiality policy. The transactions in the control channel can only take place once two co-operatively communicating nodes have successfully authenticated each other. After authentication, the encrypted exchange of information ensures confidentiality (integrity can also be achieved by employment of hash functions or message authentication codes).

Many developed and deployed technology has been misused in one way or another. As CRs are deployed, attackers may find ways to compromise the network, and radio developers will have to develop techniques to combat such problems. Our goal is to design CRNs that are resilient to known and unknown attacks. We have conducted research to build resilient CRN such as cross-layer security and a consensus algorithm which will be described in more detail in Section 5.

4.3 Electronic and cyber warfare in CRN

There has been increasing recognition of the fact that Cyber and EW operations need integration and coordination [53], due to the convergence in the technologies supporting these domains, for example, wireless networking technologies and software defined radio. We use the term "Cyber EM" to refer to Cyber Operations that depend on the EMS, rather than a wired network, as the medium. This section will explore some possibilities for the use of a context-aware CR as a technology which can support Cyber EM operations.

Eventually, our wireless networks will require automated intrusion detection systems, similar to those of our wireline networks. However, the courses of action taken in response to a cyber attack will be different, due to the medium being the EM spectrum. Consider the following cyber warfare scenario. Having detected a network intrusion or a jamming event, the CR will know that means there is an adversary radio node within radio range. Using Electronic Support Measures (ESM), the CR may determine this node's geo-location or bearing information. In response to the attack, the CR node has a choice of many possible actions: physically move away from the attacker, switch its channel or modulation, and/or counter-attack the adversary node's communications channel.

This type of scenario is an example of cyber warfare and electronic warfare technology coexisting on the same platform, which has been envisioned in the defence science community and beyond for some time [37]. One can imagine attacks on tactical wireless networks which target any layer of the network protocol stack.

At the physical layer, we can jam particular logical or physical channels of the adversary communications link. A sophisticated jammer may be able to follow an enemy radio signal as it dynamically changes frequency. On the defence side, the CRN may implement anti-spoofing techniques at the PHY layer, such as PHY-layer authentication, which could circumvent replay attacks. In theory, a multi-antenna CRN employs advanced antenna techniques which can enhance transmission security. For example, spatial precoding matrices may be used to degrade unintended third party reception, without affecting the signal quality of the received signal of the intended recipient [38].

At the link layer, we may see attacks on the DSA functioning of the CRN. With primary user emulation, the enemy radio network attempts to occupy the EM space such that wireless access is blocked, seemingly by other friendly nodes' legitimate transmissions. If the enemy CRN were somehow aware of the DSA algorithm or protocol in use by the target CRN, it might be able to block access, or increase network delay, more efficiently by anticipating the channel selection. At the network layer and above, we may see sophisticated covert exploits such as wormhole attacks. We may even see exploits targeting baseband processor vulnerabilities, in which a buffer overload allows access to the target radio software. The more specific the attack, the more information needs to have been gathered beforehand, and the exploit must be injected at the appropriate time and space.

For tactical CRNs, we find that thinking about network defence and the possibilities afforded to us by the CRN naturally leads us to think about network attacks and electronic warfare. Information fusion between communications EW and communications command and control networks has long been seen as beneficial, supporting the concept of an RF Common Operating

Picture (RF CoP) [54]. CRNs provide the opportunity to integrate communications and electronic warfare information in ways that enhance the capabilities of both the communications and EW functionality. One example is that military CRNs may collect spectrum sensing data for the purposes of communicating, which may also be ESM data when viewed from an EW perspective. Another example is that an expeditionary force, being at the battlefront, might be at the best position to launch a covert cyber attack on an adversary network, and so the tactical radio could have a cyber situational awareness and attack capability. In this case, the CR could be thought of as a "multi-functional RF unit" [11].

5 CRN security solutions and research directions

As mentioned in Section 4.2, security is one of the major technical challenges that must be overcome to fully realize the benefits of cognitive radio networks, especially for tactical wireless communications where the operating environment is often hostile and there is no central infrastructure. In this section, we summarize some of our research and describe the technology outlook in this area.

5.1 Cross layer security framework

We believe that applying cross layer design for security can be an efficient solution through information sharing and coordination between layers. Security services are needed at different layers for different functions in CRN. The basic security functions including authentication and intrusion detection can be integrated into a security sub-layer and the results can be used for different layers. This framework may increase some of internal processing within a node, but can greatly reduce the communications between nodes. This is especially beneficial to CRNs in tactical applications where communication bandwidth is precious.

We propose a cross-layer security framework as illustrated in [22]. We see that there is a trust table in the security sub-layer. This trust table is a data fusion centre for security information of all network layers. It is first established based on authentication and then kept updated based on an Intrusion Detection System (IDS). The value of the trust field can be either Boolean (e.g., zero or one) or multi-level (e.g., zero, low, medium, high). We see these values as raw data, and how to utilize it is application dependent [39]. For example, for secure routing, security policy can define if a message can be routed through all available routes or only nodes with a certain trust value. While for spectrum sensing, we can define a security policy that only uses the sensing results from the nodes with a certain trust value.

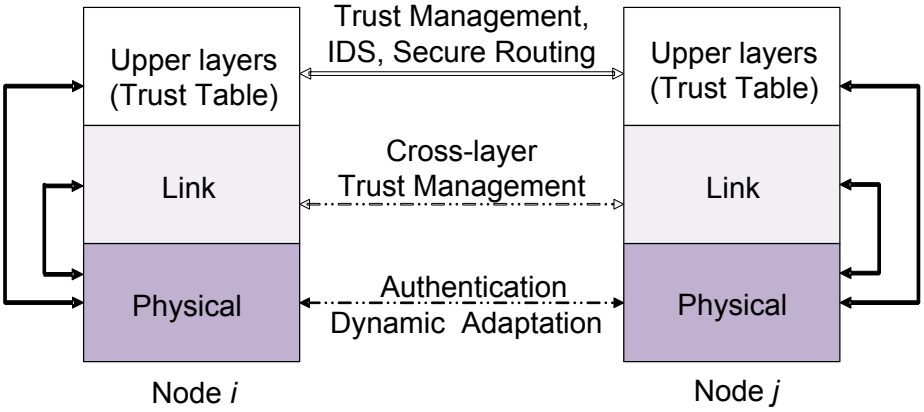

Figure 5: *Illustration of cross layer security framework.*

5.2 Trust-based security schemes

Current network protocols that have been developed implicitly trust all information shared about the state of the nodes and the larger network. Consequently, when the information that is shared among these nodes is tampered with, the network can become unusable. In particular, the protocols that have been developed for CRN require the nodes in the network to coordinate among themselves to manage their resources (e.g., spectrum, time, and power) and also to organize themselves in order to provide the functionality necessary to deliver data efficiently. To meet this objective, the nodes must share information about their state and the state of the world around them without burdening the network with too much system traffic. With the shared information, the network nodes make decisions about configuration details such as which frequencies to use, which node gets to transmit when, and to which node(s) to forward data when a direct path to the destination does not exist.

Trust is an important feature in the design and analysis of secure distribution systems. Trust and Security in Cognitive Radio Networks are always interlinked. They complement each other and are mutually inclusive. Trust-based schemes are considered as effective mechanisms associated with cryptographic techniques for thwarting a variety of attacks, e.g., packet drop attacks. Because of the properties of CR-MANETs, trust establishment needs an intelligent approach to identify attackers' misbehaviour. We can mitigate threats from attackers who deliberately drop and modify packets. We propose a scheme of trust establishment based on Bayesian networks [40], which can effectively perform causal reasoning. Based on this model, other causes, e.g., unreliable wireless connections, which also can result in packet dropping, will be distinguished from maliciousness and thus, a more accurate trust value can be calculated.

5.3 Novel physical layer authentication schemes

In Section 4.2., we have identified that verifying signal characteristics through novel physical layer authentication techniques can help counter Incumbent Emulation (IE) attacks. Currently, the physical properties of the wireless medium are under-utilized to complement and enhance traditional security mechanisms. We propose some new device authentication techniques based on physical layer attributes.

Various physical layer attributes have been explored recently to enhance wireless security [41-43]. It is shown in the literature that the properties of a wireless communication signal from a legitimate user can be used to authenticate subsequent transmissions from that specific user, thereby denying access to any potential spoofer with significant different link properties, including received signal strength or channel state information. However, these existing studies assume a static communication environment, where the impact of communication devices on the communication signals is ignored.

We proposed a comprehensive physical layer security strategy using a novel model-based authentication scheme, which considers the time-varying nature of multiple physical layer attributes, including different attributes of channel impulse response (CIR) and hardware-related device characteristics including carrier frequency offset (CFO) [22]. In addition, a new hypothesis testing for authentication, which combines multiple inputs from these observations, including those indicating the communication environment and those associated with the hardware

characteristics of the communication devices, will be proposed and thoroughly investigated. In addition, other alternatives for wireless device authentication will be explored as well. A new transmitter identification technique using RF fingerprinting/watermarking will be investigated to distinguish different transmitters and enhance traditional identity-based security mechanisms, which could be enabled by RF fingerprinting using an embedded transmitter identification watermark.

5.4 Distributed authentication with threshold cryptography

In this subsection, we describe how distributed authentication can help secure Distributed Spectrum Sensing (DSS) in CRNs.

DSS utilizes not only its own observations as a basis for decision making but also the observations of others. There is an obvious need to authenticate the shared observations. This is particularly true given the distributed and unseen nature of the peer CRs. A CR needs assurance that messages are indeed from whom they claim they are. This is a similar nature to authentication of traffic in any wireless network, and as such is not necessarily unique to the CR paradigm. It is here that benefits can be drawn from distributed authentication in ad-hoc wireless networks.

For security services in a distributed network, threshold cryptography is generally used to let some or all network nodes share a network master key and collaboratively provide security services such as issuing private keys. In a network with N nodes, a group of special n nodes is capable of generating partial certificates using their shares of the certificate signing key. A valid certificate can be obtained by combining k such partial certificate shares, which is called *(k, n)*-threshold cryptography.

In CR-MANETs, identity (ID)-based cryptography with threshold cryptography is a popular approach for the security design because it uses a simple key management scheme compared to Public Key Infrastructure (PKI) [44]. Most previous work for key management in this framework concentrates on the protocols and structures. Consequently, how to optimally conduct node selection in ID-based cryptography with threshold secret sharing is largely ignored. In paper [45], a distributed scheme based on the stochastic multi-arm bandit formulation is proposed. The proposed scheme can select the best nodes and use their partial certificate shares for reconstructing the full secret taking into account the security conditions to minimize the overall threat posed to the network.

5.5 Distributed monitoring and consensus algorithms

In cognitive radio (CR) networks with no central authority, secondary users need to cooperatively sense the spectrum to detect the presence of primary users.

Recently, bio-inspired mechanisms have become important approaches for complex communication networks. An important motivational background of this area is related to the study of complex natural phenomena including flocking of birds, schooling of fish, swarming of ants and honeybees, among others. The investigation of such biological systems has generated fundamental insights into understanding the relation between group decision making at the higher

level and the individual animals' communication at the lower level. These collective animal behaviours have motivated many effective yet simple control algorithms for the coordination of multi-agent systems in engineering. Recently, consensus problems have played a crucial role in distributed control models [46], wireless sensor networks [47], and stochastic consensus seeking with noise measurement [48]. Since these algorithms are usually constructed based on local communication of neighbouring agents, they have low implementation complexity and good robustness, and the overall system may still function when local failure occurs.

We have proposed a fully distributed and scalable cooperative spectrum-sensing scheme based on recent advances in consensus algorithms [49]. In the proposed scheme, there are two main components. The first is "distributed monitoring", in which each of the secondary users maintains coordination based on only local information exchange without a centralized common receiver. The second is the "consensus algorithm", that allows different "views" to be estimated by different local monitors to be combined. Unlike most of the existing decision rules, such as the OR-rule or the 1-out-of-N rule, we use the consensus of secondary users to make the final decision. Secondary users can also collectively filter out falsified data inserted by SSDF attacks and make the correct decision about the presence of primary users, which can be viewed as a typical multi-agent coordination situation. Simulation results show that the proposed consensus scheme can have significant lower missing detection probabilities and false alarm probabilities in CR networks. It is also demonstrated that the proposed scheme not only has proven sensitivity in detecting the primary user's presence but also has robustness in choosing a desirable decision threshold.

5.6 Robust communications and game theory

The history of security has taught us that a perfectly secure system never exists. Instead, security is an evolving process, as we have seen in the context of WLANs and 2G/3G networks. New system vulnerabilities continue to be identified, and new security threats continue to arise. Accordingly new solutions must be developed and integrated into existing systems, which can be likened to a game of "cat and mouse".

We can never fully stop the intruder's actions, however, we hope we can provide tools for the defender to intelligently respond to an intruder and thereby provide robust communication. Game theory provides a good tool to counterattack the dynamic nature of adversaries.

Game theoretic approaches have been proposed to improve network security [18]. Game theory addresses problems in which multiple players with contradictory incentives or goals compete with each other; thus, it can provide a mathematical framework for modelling and analyzing decision problems. In game theory, one player's outcome depends not only on her/his decisions, but also on those of her/his opponents' decisions. Similarly, the success of a security scheme depends not only on the actual defense strategies, but also on the actions taken by the attackers.

Mean field game theory provides a powerful mathematical tool for problems with a large number of players and can be applied for CR-MANET security. Since security defence mechanisms consume precious system resources (e.g., energy), the proposed scheme considers not only the security requirement of MANETs but also the system resources. In addition, each node only needs to know its own state information and the aggregate effect of the other nodes in the

MANET. Therefore, the proposed scheme is a fully distributed scheme. Simulation results are presented to illustrate the effectiveness of the proposed scheme. [50]

5.7 Anti-jamming CR techniques

Like any communications network, cognitive radio networks (CRNs) are vulnerable to jamming attacks, to prevent them from utilizing spectrum opportunities. An intelligent jammer can do spectrum sensing too.

More interference-resilient communications systems need to be designed, for instance to decode the received signals in very low SNR regimes or to detect the primary signal buried in a jammer's signal [30]. Further studies are needed to target specific solutions regarding various jamming attacks within a CRN framework such as common control channel jamming attack. Usage of interference resilient waveforms, such as Spread-Spectrum (SS) techniques, and exploitation of error detection and correction coding are among potential solutions to combat control channel jamming. Due to frequency agility of CR nodes, it might also be possible to switch the control channel of the network from time to time in an attempt to safeguard signaling packets against interferes [30].

6 Scenarios for tactical wireless communications

In this section, we provide two envisioned scenarios in which tactical missions benefit from the capabilities provided by cognitive radio networks. Supporting features of the network which are associated with cognitive radio or security are listed alongside the scenario.

Table 6: Scenario 1 *– Geo-location of an unknown emitter, avoiding jammer interference.*

Scenario description	**Supporting features associated with CR**
1. An allied convoy equipped with CRN is proceeding through an urban conflict zone where there has been a history of IED attacks. Multi-national forces were able to quickly deploy on the mission with no need for extensive spectrum planning, since spectral resources are negotiated on the fly according to policy.	Reconfiguration, near-zero setup, spectrum access, policy management
2. As the convoy moves into the urban area, buildings cause shadowing and a fluctuating decrease in received signal power.	Spectrum sensing
3. Automatic waveform adjustment is performed by the CR system in conformance to the new propagation environment.	Decision making and parameter selection, radio resource management
4. As the convoy approaches the conflict zone, Counter Improvised Explosive Device (CIED) jammers are switched on. The jammer of an independent contractor puts energy into the VHF band, interfering with national military radio. These radios automatically sense the activity on the channel and rendezvous on another channel.	Interference avoidance and rejection
5. The convoy is called to a halt as there are indications of a possible IED in the road ahead. A dismounted force is deployed to investigate the suspected IED. This information is relayed to HQ via the node having the appropriate waveform, security and best connectivity to HQ.	Enhanced connectivity, reliability, security
6. Meanwhile, Electronic Support (ES) has indicated an unknown emitter in the area; via modulation recognition, it is determined that it is a push-to-talk radio. Automatic geo-location indicates that it is not co-located with the suspected IED site ahead.	Signal detection and classification, increased situational awareness
7. The dismounted team determines the road ahead is clear, and the convoy resumes. The new status information is relayed to HQ as the forces move out, via a different relay node than before, as the relative signal quality favours a different link.	Adaptive link establishment

Table 7: Scenario 2 *– CR as a multi-functional RF unit to support Cyber/EW operation.*

Scenario description	**Supporting features associated with CR and security**
1. Our CAF are engaged in a conflict with a military of comparable technological ability. Ground-based forces are to be deployed without connection to a network infrastructure. Prior to mission deployment, each CR is loaded with a set of public keys for all members of its Section; each Section will form a cluster of radios.	Scalable network security in the absence of infrastructure, strong encryption
2. En route to deployment, the soldiers authenticate themselves to their radio devices using biometrics, or two-factor authentication. The radios then find and authenticate themselves to the other radios in their cluster using their pre-loaded keys. Each radio additionally assigns an initial trust value to each of its peer radio nodes, indicating that as of now, each node is trusted. The Section is ready to go.	Authentication, support for secure routing via trust values for each node
3. As the soldiers proceed, their radios adjust their power levels to the minimum necessary, for covertness. A jamming signal begins to affect the spectrum; the cluster of radios moves to a frequency hopping waveform.	Transmission security, waveform agility
4. The Section proceeds to carry out its mission – a coordinated Cyber/EW attack on the adversary's network. Two soldiers proceed as far as possible to the battlefront, and drop 'breadcrumb' radios at strategic locations. These radios will be in contact with the CAF CRN, which EW and Cyber analysts will control and use to launch a covert attack targeting the Dynamic Spectrum Allocation scheme assumed to be in use by the adversary network.	Support for coordinated Cyber/EW operations
5. The soldiers return and join the rest of their Section as they move back into the vicinity of their cluster. Automatically, the monitoring and intrusion detection systems of their peer radios restore the trust values corresponding to the returning soldiers' radios.	Dynamic wireless security

7 Suggested roadmap for Canada

We have identified the expected benefits and challenges of CRN for tactical wireless communications (Section 1.3). Despite the benefits, cognitive radio technology has yet to be adopted by the CAF and its allies even though more than a decade has passed since its inception. We see the need for an evolutionary path to gradually realize the goal of faster, smarter, and more secure communications.

The first step towards each aspect of this path is to understand and address the current heterogeneous network. Tactical wireless communication requires a mixture of wireless communication technologies with different characteristics in terms of bandwidth, range, transmission frequency, and modulation schemes. Each is implemented in a wide range of different equipment, and different security schemes, which has led to a variety of non-interoperable wireless systems. At the very least, the CR needs to have awareness of the range of radio standards, if not to actually provide an implementation, to enable interoperability.

A. Introduce dynamic spectrum access (Fast deployment)

Currently, tactical radio systems require rigorous spectrum management. Spectrum management is a key component of cognitive radio addressing the spectrum scarcity problem as well as the burden of deploying radio networks with detailed spectrum allocation plans for multi-national missions.

We are a proponent of the view suggested in [51] that is espoused by many: military spectrum allocations should include an 'ISM-type' allocation within the military bands to allow for a gradual introduction and proving grounds for newer radio technology. So while we believe that protection of the legacy radio communications is of the utmost importance, we must also make an investment in future radio capabilities if future networks are to meet our growing and changing requirements.

Initially, the need for DSA to be applied in a managed way may be addressed through the use of a centralized spectrum broker entity, or through coordinated dynamic frequency management. Coordinated dynamic frequency management enables coordinated distribution of spectrum in accordance with a defined measure of the benefit to the system of all radio nodes. There is perhaps an analogous progression in the commercial world, with the concept of Licensed Shared Access (LSA) and Authorized Shared Access (ASA) [52]; these concepts allow additional users to use licensed spectrum in accordance with certain sharing rules. The military user will also cede access to the spectrum according to policy.

Ultimately, we see opportunistic decentralized spectrum access, which has maximum flexibility for spectrum access, as the end state. This decentralized spectrum access will allow the most efficient occupation of the spectrum resource without prior spectrum management. That said, we believe that changes to the spectrum occupation of our networks must be made in a deliberate and considered way, in order to preserve our spectrum dominance and information security. More work needs to be done to address the security implications of the decentralized dynamic spectrum access network.

B. Introduce cognition (Smarter communication)

CRNs will implement more advanced waveform adaptation for the purpose of creating more robust waveforms. CRNs will be able to balance various criteria to tune a waveform for a given transmission – such as the need for covertness, the required data rate, and the transmission priority.

CR networks will have continuous monitoring of the spectrum and attempt to make optimal spectrum use decisions based on the observations. CRs can learn and mitigate interference situation. With the trend in military communications is towards denser networks [12], and given that the spectrum is usually quite crowded in a densely populated theater, cognition will eventually be needed.

An overarching concern in the area of communications intelligence is determining how to rank each radio message or data transmission in priority, and finding a way for the highest-priority radio message and data traffic to get through first. Further research is needed in this area.

C. Support cyber EM (More resilient communication)

Modern military communications and EW functions operate in the same electromagnetic spectrum, but sharing of spectrum and EW information within a force and between allied military is difficult. It has long been thought that the increased situational awareness gained by merging EW and communications sensor information would be beneficial [54]. The argument only becomes stronger when considering CRNs, which rely on situational awareness in the spectrum domain, augmented with signal detection and classification, for decision making.

Beyond ESM, when thinking about the CR as a multi-functional RF unit, we envision the CRN as a system with a Cyber defence capability as well as Cyber EM attack capability. CRs are likely to be deployed at the edge of the battlefield, with the dismounted forces, in a good position to perform wireless network detection and network intrusion.

Our future forces will require CRNs that are hardened to attack, and that may intelligently and covertly disable adversarial CR networks.

8 Conclusion

In this report, we have described Cognitive Radio Networks (CRN), and their benefits and challenges for tactical wireless communications. We have summarized related work in the defence community, particularly where our partner nations have described a roadmap towards the adoption of CR technology. We have described our own work in this area, and provided our roadmap or thoughts about the role of CRNs for tactical wireless communications. In particular, we emphasized 1) the need to gradually introduce DSA for fast network deployment and to ease spectrum congestion, 2) the benefit of CRN to increase communication system intelligence in dynamic, heterogeneous environments, and 3) the role of the CR as a multi-functional RF unit, capable of integrating communications and EW information to support coordinated Cyber EM operations.

Modern military communications and EW functions operate in the same electromagnetic spectrum, but sharing of spectrum and EW information within a force and between allied military is difficult. It has long been thought that the increased situational awareness gained by merging EW and communications sensor information would be beneficial.

The argument only becomes stronger when considering CRNs, which rely on situational awareness in the spectrum domain, augmented with signal detection and classification, for their decision making. CRNs can facilitate a unified view of ESM/tactical SIGINT in the area of operations. A CRN may use its accumulated information for its own communications needs together with its unified ESM view to support Cyber EM operations.

The defence scientific community must leverage what has and will be done in industry and academia, to the extent that it meets our objectives. We wish to continue to contribute, through the work described in this document, to the ongoing international efforts through NATO and TTCP. As a group of allied nations contributing to the development of the next generation of tactical wireless communications technology, we stand a better chance of realizing the promise of CRNs to best effect for our national forces.

References

[1] Ari Hulkkonen, Tactical Communications: the future of radio, Geospatial World, Oct., 2013.

[2] J. Mitola III and G. Q. Maguire, "Cognitive radio: making software radios more personal", IEEE Personal Communications, Vol. 6, No. 4, Aug. 1999, pp. 13-18.

[3] J. Mitola III, "Cognitive radio for flexible mobile multimedia communications", IEEE MoMuC'99, Nov. 1999, pp. 3-10 (Best Paper Award).

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

[5] S. Haykin, "Cognitive Radio: Brain-Empowered Wireless Communications", IEEE Journal on Selected Areas in Communications, Vol. 23, NO. 2, Feb. 2005, pp. 201-220.

[6] FCC, Cognitive Radio Technologies Proceeding (CRTP), ET Docket No. 03-108. Available at: http://transition.fcc.gov/oet/cognitiveradio/

[7] Scott Seidel "IEEE 802 Tutorial: Cognitive Radio", Presented at the IEEE 802 Plenary, 18 July 2005.

[8] K.-C. Chen, Y. Peng, N. Prasad, Y. Liang and S. Sun, Cognitive radio network architecture: Part II – trusted network layer structure, Proceedings of the 2nd international conference on Ubiquitous information management and communication ICUIMC '08, Pages 120-124.

[9] IEEE Std 1900.1-2008: IEEE Standard Definitions and Concepts for Dynamic Spectrum Access: Terminology Relating to Emerging Wireless Networks, System Functionality, and Spectrum Management.

[10] Results of the TTCP C3I TP6 Workshop on Cognitive Radio, TTCP Technical Report, July 2009. TR-C3I-4-2009.

[11] NATO report Cognitive Radio in NATO, NATO Final Report of Task Group IST077/RTG-035.

[12] Bruce Fette, "Fourteen Years of Cognitive Radio Development", Proc. of IEEE Milcom 2013.

[13] J. Redi, R. Ramanathan, "The DARPA WNaN Network Architecture", Proc. of IEEE Milcom 2011, 7-10 Nov 2011.

[14] L. Rose, R. Massin, L. Vijayandran, M. Debbah, CORASMA Program on Cognitive Radio for Tactical Networks: High Fidelity Simulator and First Results on Dynamic Frequency Allocation, Proc. of IEEE Milcom 2013.

[15] Rose, L.; Perlaza, S.M.; Le Martret, C.J.; Debbah, M., "Self-Organization in Decentralized Networks: A Trial and Error Learning Approach," Wireless Communications, IEEE Transactions on , vol.13, no.1, pp.268,279, January 2014.

[16] Hou, Ting-Chao; Tsai, Tzu-Jane, "On the cluster based dynamic channel assignment for multihop ad hoc networks," Communications and Networks, Journal of , vol.4, no.1, pp.40,47, March 2002.

[17] Topi Tuukkanen and Jukka Anteroinen, "Initial Assessment Of Proposed Cognitive Radio Features From A Military Perspective", Finnish MoD, 18th ICCRTS.

[18] J. Lopatko, Polish Roadmap to Tactical Cognitive Radio, NATO STO-IST-123 NATO IST Symposium on Cognitive Radio and Future Networks, Amsterdam, Netherlands, May 2014.

[19] M.Suchanski, P. Gajewski, R. Matyszkiel, P. Kaniewski: Dynamic Spectrum Management in Legacy Military Communication Systems, Military CIS Conference MCC'2012.

[20] T.J. Willink, "Cognitive Radio Techniques for Assured Communications", Defence R&D Canada – Ottawa Technical Report, TR 2010-004, January 2010.

[21] Helen Tang, Zhexiong Wei, F. Richard Yu, Peter Mason, Security Enhancements for Spectrum Sensing and Data Transmission in Cognitive Radio Mobile Ad Hoc Networks (CR-MANETs), NATO IST Symposium on Cognitive Radio and Future Networks, Amsterdam, Netherlands, May 2014.

[22] Helen Tang, Peter Mason, Richard Yu, Xianbin Wang and I. Lambadairs, "Cross Layer Security Enhancement for Cognitive Radio Based Mobile Ad-hoc Networks (CR-MANETs)" , TIF project proposal, DRDC Ottawa Internal document.

[23] K.-C. Chen, Y. Peng, N. Prasad, Y. Liang and S. Sun, Cognitive Radio Network Architecture: Part I - General Structure Cognitive Ad Hoc Radio Networks", Proceedings of the 2nd international conference on Ubiquitous information management and communication ICUIMC '08, Pages 114-119.

[24] Carl R. Stevenson, IEEE 802.22: the first cognitive radio wireless regional area network standard, IEEE Communications Magazine, Volume 47 Issue 1, January 2009 Pages 130-138.

[25] F.R. Yu, H. Tang, M. Huang, P. Mason, and Z. Li, "Distributed Consensus-Based Cooperative Spectrum Sensing in Cognitive Radio Mobile Ad Hoc Networks," book chapter in Cognitive Radio Mobile Ad Hoc Networks, Springer, Sept. 2011.

[26] Yucek, T.; Arslan, H., "A survey of spectrum sensing algorithms for cognitive radio applications," Communications Surveys & Tutorials, IEEE , vol.11, no.1, pp.116,130, First Quarter 2009.

[27] Preston Marshall, "Quantitative Analysis of Cognitive Radio and Network Performance", Artech House, 2010.

[28] K.E. Baddour, “Spectrally overlapping coexistence of flexible spectrum access radios”, Communications Research Centre Canada, Technical Report CRC-RP-2012-005.

[29] J. L. Burbank, “Security in cognitive Radio Networks: The required evolution in approaches to wireless network security”, in Proc. Int. Conf. Cogn. Radio Oriented Wireless Netw. Commun., Singapore, May 15–17, 2008, DOI: 10.1109/CROWNCOM.2008.

[30] A. Attar, H. Tang, A. Vasilikos, F.R. Yu, and V.C.M. Leung, “Security Challenges in Cognitive Radio Networks: Solutions and Future Research Directions,” Proceedings of the IEEE, vol. 100, no. 12, pp. 3172-3186, Jan. 2013.

[31] R. Chen, J.-M. Park, and J. Reed, “Defense against primary user emulation attacks in cognitive radio networks,” IEEE J. Sel. Areas Commun., vol. 26, pp. 25–37, Jan. 2008.

[32] Liu, Y., Ning, P., & Dai, H., Authenticating Primary Users’ Signals in Cognitive Radio Networks via Integrated Cryptographic and Wireless Link Signatures. 2010 IEEE Symposium on Security and Privacy, (pp. 286-301).

[33] Morerio, P., Dabcevic, K., Marcenaro, L., & Regazzoni, C. S. (2012). Distributed cognitive radio architecture with automatic frequency switching. IEEE Workshop on Complexity in Engineering, COMPENG2012, (pp. 139-142). Aachen.

[34] R. Chen, J.-M. Park, Y. Hou, and J. Reed, “Toward secure distributed spectrum sensing in cognitive radio networks,” IEEE Comm. Mag., vol. 46, pp. 50–55, Apr. 2008.

[35] H. Tang, F.R. Yu, M. Huang, and Z. Li, “Distributed Consensus-based Security Mechanisms in Cognitive Radio Mobile Ad Hoc Networks,” IET Communications, vol. 6, no. 8, pp. 974-983, May. 2012.

[36] G.A. Safdar; M. O’Neill, “A novel common control channel security framework for cognitive radio networks”, Int. J. of Autonomous and Adaptive Communications Systems, 2012 Vol.5, No.2, pp.125 – 145.

[37] Scott, A.; Hardy, T.J.; Martin, R.K.; Thomas, R.W., “What are the roles of electronic and Cyber Warfare in cognitive radio security?,” Circuits and Systems (MWSCAS), 2011 IEEE 54th International Midwest Symposium on , vol., no., pp.1,4, 7-10 Aug. 2011.

[38] G.W.K. Colman, “Spatial hopping in MIMO systems for impeded signal reception by unintentional receivers”, Communications Research Centre Canada, Technical Report CRC RP 2012-007, November 2012.

[39] H. Tang and M. Salmanian, “Lightweight Integrated Authentication for Tactical MANETs”, Proc. IEEE TrustCom ‘08, Nov. 18-21, 2008.

[40] Zhexiong Wei, Helen Tang, F. Richard Yu, and Peter Mason, Trust Establishment Based on Bayesian Networks for Threat Mitigation in Mobile Ad Hoc Networks, Proc. of IEEE Military Communication Conference (MILCOM) 2014, Baltimore, MD, USA, Oct. 2014.

[41] Y. Liang, H.V. Poor, S. Shamai, “Secure communication over fading channels,” IEEE Trans. Info. Theory, vol. 54, no. 6, pp. 2470-2492, Jun. 2008.

[42] S. Mathur, A. Reznik, C. Ye, R. Mukherjee et.al, “Exploiting the physical layer for enhanced security,” IEEE Wireless Commun., vol.17, no. 5, pp. 63-70, Oct. 2010.

[43] F. Liu, Xianbin Wang and H. Tang “Robust Physical Layer Authentication Using Inherent Properties of Channel Impulse Response”, in Proc. IEEE Military Communications Conference (MILCOM), November 2011.

[44] K.G. Paterson, G. Price, “A comparison between traditional Public Key Infrastructures and Identity-Based Cryptography”, Information Security Technical Report, 8(3):57-72, Elsevier Ltd, 2003.

[45] F.R. Yu and H. Tang, “Distributed Node Selection for Threshold Key Management with Intrusion Detection in Mobile Ad Hoc Networks,” ACM/Springer Wireless Networks, April 2010.

[46] Ren, W., Beard, R.W.: ‘Consensus seeking in multiagent systems under dynamically changing interaction topologies’, IEEE Trans. Autom. Control, 2005, 50, pp. 655–661.

[47] Xiao, L., Boyd, S., Lall, S.: ‘A scheme for robust distributed sensor fusion based on average consensus’. Proc. Fourth Int. Symp. On Information Processing in Sensor Networks IPSN 2005, 2005, pp. 63–70.

[48] Huang, M., Manton, J.: ‘Stochastic consensus seeking with measurement noise: convergence and asymptotic normality’. Proc. American Control Conf.’08, Seattle, WA, June 2008.

[49] H. Tang, F.R. Yu, M. Huang, and Z. Li, “Distributed Consensus-based Security Mechanisms in Cognitive Radio Mobile Ad Hoc Networks,” IET Communications, vol. 6, no. 8, pp. 974-983, May. 2012.

[50] Y. Wang, F.R. Yu, H. Tang, and M. Huang, “A Mean Field Game Theoretic Approach for Security Enhancements in Mobile Ad hoc Networks,” accepted for publication in IEEE Trans. Wireless Comm., Oct. 2013.

[51] Bart Scheers, “Introduction of Dynamic Spectrum Access technology in NATO Europe tactical communications”, Proc. of IEEE Milcom 2013.

[52] GSMA Public Policy Position paper, available http://www.gsma.com/spectrum/wp-content/uploads/2013/04/GSMA-Policy-Position-on-LSA-ASA.pdf.

[53] Technical Report: On the boundaries of Cyber Domain S&T, TTCP TR-C3I-TP3-1-2013.

[54] Requirements for a RF Common Operating Picture: Results of the TTCP Workshop on Spectrum Situation Awareness, DRDC Ottawa and CRC, Canada, 15-17 October 2008, TTCP TR-EWS-AG5-1-2009.

List of symbols/abbreviations/acronyms/initialisms

AP	Access Point
ASA	Authorized Shared Access
AWNS	Advanced Wireless Networking System
BS	Base Station
C3I	Command, Control, Computers and Intelligence
CAF	Canadian Armed Forces
CCCJ	Common Control Channel Jamming
CDSA	Coordinated Dynamic Spectrum Access
CFO	Carrier Frequency Offset
CIED	Counter Improvised Explosive Device
CIR	Channel Impulse Response
COP	Common Operating Picture
CORASMA	Cognitive Radio for Dynamic Spectrum Management
CR	Cognitive Radio
CRN	Cognitive Radio Networks
DARPA	Defence Advanced Research Projects Agency
DFA	Dynamic Frequency Allocation
DRDC	Defence Research and Development Canada
DSA	Dynamic Spectrum Access
DSM	Dynamic Spectrum Management
DSS	Distributed Spectrum Sensing
DTN	Disruption Tolerant Networking
EDA	European Defence Agency
EM	Electromagnetic
ES	Electronic Support
ESM	Electronic Support Measures
EW	Electronic Warfare
FCC	Federal Communications Commission
FER	Frame Error Rate
GBDCA	Greedy-based Dynamic Channel Assignment

HQ	Headquarters
HSLS	Hazy-sighted Link State
HW	Hardware
IDS	Intrusion Detection System
IE	Incumbent Emulation
IED	Improvised Explosive Device
IEEE	Institute of Electronic and Electrical Engineers
IP	Internet Protocol
ISM	Industrial, Scientific and Medical
LSA	Licensed Shared Access
MAC	Media Access Control
MANET	Mobile Ad-Hoc Network
MoD	Ministry of Defence
MPR	Multi-Point Relay
MS	Mobile Station
NATO	North American Treaty Organization
OODA	Observe, Orient, Decide, Act
OSI	Open System Interconnection
OTA	Over the Air
PKI	Public Key Infrastructure
PUE	Primary User Emulation
R&D	Research and Development
RF	Radio Frequency
RTG	Research and Technology Group
SDR	Software Defined Radio
SIGINT	Signals Intelligence
SNR	Signal to Noise Ratio
SPRT	Sequential Probability Ratio Test
SS	Spread-Spectrum
SSDF	Spectrum Sensing Data Falsification
SW	Software
TIF	Technology Investment Fund

TNO	Tactical Network Operations
TP	Technical Panel
TTCP	The Technical Cooperation Program
TV	Television
WNaN	Wireless Network After Next
WRAN	Wireless Regional Area Network

This page intentionally left blank.

DOCUMENT CONTROL DATA

(Security markings for the title, abstract and indexing annotation must be entered when the document is Classified or Designated)

1. ORIGINATOR (The name and address of the organization preparing the document. Organizations for whom the document was prepared, e.g., Centre sponsoring a contractor's report, or tasking agency, are entered in Section 8.)

DRDC – Ottawa Research Centre
Defence Research and Development Canada
3701 Carling Avenue
Ottawa, Ontario K1A 0Z4
Canada

2a. SECURITY MARKING (Overall security marking of the document including special supplemental markings if applicable.)

UNCLASSIFIED

2b. CONTROLLED GOODS

(NON-CONTROLLED GOODS)
DMC A
REVIEW: GCEC DECEMBER 2012

3. TITLE (The complete document title as indicated on the title page. Its classification should be indicated by the appropriate abbreviation (S, C or U) in parentheses after the title.)

Cognitive radio networks for tactical wireless communications

4. AUTHORS (last name, followed by initials – ranks, titles, etc., not to be used)

Tang H.; Watson S.

5. DATE OF PUBLICATION (Month and year of publication of document.)

December 2014

6a. NO. OF PAGES (Total containing information, including Annexes, Appendices, etc.)

56

6b. NO. OF REFS (Total cited in document.)

54

7. DESCRIPTIVE NOTES (The category of the document, e.g., technical report, technical note or memorandum. If appropriate, enter the type of report, e.g., interim, progress, summary, annual or final. Give the inclusive dates when a specific reporting period is covered.)

Scientific Report

8. SPONSORING ACTIVITY (The name of the department project office or laboratory sponsoring the research and development – include address.)

DRDC – Ottawa Research Centre
Defence Research and Development Canada
3701 Carling Avenue
Ottawa, Ontario K1A 0Z4
Canada

9a. PROJECT OR GRANT NO. (If appropriate, the applicable research and development project or grant number under which the document was written. Please specify whether project or grant.)

9b. CONTRACT NO. (If appropriate, the applicable number under which the document was written.)

10a. ORIGINATOR'S DOCUMENT NUMBER (The official document number by which the document is identified by the originating activity. This number must be unique to this document.)

DRDC-RDDC-2014-R185

10b. OTHER DOCUMENT NO(s). (Any other numbers which may be assigned this document either by the originator or by the sponsor.)

11. DOCUMENT AVAILABILITY (Any limitations on further dissemination of the document, other than those imposed by security classification.)

Unlimited

12. DOCUMENT ANNOUNCEMENT (Any limitation to the bibliographic announcement of this document. This will normally correspond to the Document Availability (11). However, where further distribution (beyond the audience specified in (11) is possible, a wider announcement audience may be selected.))

Unlimited

13. ABSTRACT (A brief and factual summary of the document. It may also appear elsewhere in the body of the document itself. It is highly desirable that the abstract of classified documents be unclassified. Each paragraph of the abstract shall begin with an indication of the security classification of the information in the paragraph (unless the document itself is unclassified) represented as (S), (C), (R), or (U). It is not necessary to include here abstracts in both official languages unless the text is bilingual.)

The modern battlefield is a demanding environment for tactical radio networks in that in addition to the variation in the wireless propagation environment, the radio must co-exist and contend with a high density of emitters having varying waveforms. Cognitive Radio (CR) is widely considered as a promising technology for providing the mechanisms to mitigate interference, and allow more flexible and dynamic radio resource allocation.

Many nations and organizations have put forward a roadmap for applying Cognitive Radio Networks (CRN) to tactical communications; an overview of these is given in this report. We will also document current Canadian defence Research and Development (R&D) programs in this area, and provide our perspectives and plans for future research. We look at the significance of cognitive radio networks for our future tactical wireless communications, in terms of the benefits, technological challenges, and the implications for security.

CRNs are expected to provide benefits such as Dynamic Spectrum Access for fast network deployment and ease of spectrum congestion, increased communications resilience in dynamic, heterogeneous environments, and may provide the basis for the tactical radio as a multi-functional radio-frequency (RF) unit, capable of supporting intelligent Cyber Electromagnetic (EM) attacks and defences. In our current and future research, we wish to provide solutions which empower the CRN to achieve all of these benefits without compromising security.

Le champ de bataille moderne est un environnement exigeant pour les réseaux de radiocommunications tactiques, car, en plus des variations dans l'environnement de propagation sans fil, le poste radio doit coexister et composer avec une forte concentration d'émetteurs utilisant diverses formes d'ondes. La radio intelligente (RI) est généralement considérée comme une technologie prometteuse pouvant fournir les mécanismes nécessaires pour réduire les interférences et permettre une affectation souple et dynamique des ressources radio. De nombreux pays et organismes ont proposé une feuille de route pour utiliser les réseaux de radio intelligente (RRI) pour les communications tactiques, et le présent rapport en donne un aperçu. Nous documenterons aussi les programmes de recherche et développement (R.-D.) en cours de la défense canadienne dans ce domaine, et nous présenterons nos points de vue et nos plans pour les recherches futures. Nous examinons en outre l'importance des réseaux de radio intelligente pour nos communications sans fil tactiques futures, sur le plan des avantages, des défis technologiques et des implications pour la sécurité.

Les RRI devraient offrir des avantages, comme un accès dynamique au spectre pour le déploiement rapide de réseaux et la réduction de l'encombrement du spectre, une résilience accrue des communications dans des environnements hétérogènes dynamiques, en plus de fournir la base pour la radio tactique, comme un poste de radiofréquence (RF) polyvalent pouvant soutenir les attaques cyber électromagnétiques (ACEM) intelligentes et la défense contre celles ci. Dans le cadre de nos recherches actuelles et futures, nous désirons fournir des solutions qui permettront au RRI d' offrir tous ces avantages sans compromettre la sécurité.

14. KEYWORDS, DESCRIPTORS or IDENTIFIERS (Technically meaningful terms or short phrases that characterize a document and could be helpful in cataloguing the document. They should be selected so that no security classification is required. Identifiers, such as equipment model designation, trade name, military project code name, geographic location may also be included. If possible keywords should be selected from a published thesaurus, e.g., Thesaurus of Engineering and Scientific Terms (TEST) and that thesaurus identified. If it is not possible to select indexing terms which are Unclassified, the classification of each should be indicated as with the title.)

cognitive radio, cognitive radio networks, dynamic spectrum access, MANETs, software defined radio