Trends in Survivable/Secure Cognitive Networks

Erik Blasch  
Air Force Research Lab  
Rome, NY 13441  
erik.blasch@rl.af.mil

Timothy Busch  
SUNY-IT  
Utica, NY 13502  
Timothy.Busch@sunyit.edu

Sunil Kumar  
San Diego State University  
San Diego, CA 92182  
skumar@mail.sdsu.edu

Khanh Pham  
Air Force Research Lab.  
Kirtland, NM, 87117  
khanh.pham@kirtland.af.mil

Abstract— Recent developments in cognitive radio networks have enabled intelligent spectrum management, dynamic message traffic patterns, and adaptive platform configuration. However, as these developments extend from the software-defined radio, there are numerous research questions that require further analysis over the user, network, and application quality of service considerations. In this position paper, we develop the key tenets of cognitive networking that enable future survivable, secure, and trusted networks that meet measures of performance and measures of effectiveness capabilities for future communication systems.

Keywords: Cognitive Radio, Data Preparation, Dynamic Spectrum Management, Cogniton Cycle, Obersve-Orient-Decide-Act.

I. INTRODUCTION

Cognitive Radio (CR) developments have recently been debated through the IEEE 1900 series standards from which definitions, recommended practices, applications, and polices have been vetted in the community [1]. These definitions serve to bring together various conceptualizations of the distinctions between intelligence (e.g. cognitive) and applications (e.g. radio). Numerous communities have contributed elements such as dynamic spectrum access, networking, software defined radio, and quality of service (QoS) to the concept of a cognitive radio network. These elements (and others) are formalized in the IEEE 1900 series standards.

CR is an emerging technology which uses intelligent strategies to allow a radio terminal to automatically sense, recognize, and adapt to use of any available radio frequency spectrum at a given time [2]. CR can be viewed as an extension to software defined radio (SDR) where SDR has a predefined frequency band; whereas CR scans a wide range of frequency spectra before deciding which band to use, as shown in Fig. 1. CR opportunistically uses the available (i.e., idle) frequency spectrum for the exchange of information for secondary users (i.e., low priority) and stops using the frequency band at the instant the primary user (i.e., high-priority) needs to use the band. CR seeks to not infringe upon or interfere with the rights of licensed users [3]. Recently, Kaur et. al. [4] overview various CR definitions, with a focus on spectrum sensing, management, allocation/mobility, and sharing.

While IEEE 1900 provides a basis for standard implementations, there are still open questions to be answered. Since the Federal Communications Commission (FCC) [5] opened the industrial, scientific and medical (ISM) bands for commercial applications, there have been many developments which have accelerated in the last decade [6] especially with regard to CR. CR can viewed from both hardware and software perspectives and the definition is dependent on the communications community exploring the topic. For the hardware radio frequency (RF) antenna community, CR is an extension of SDR. For researchers in physical layer communications, CR is closely related to dynamic spectrum sharing (DSS) [7] and dynamic spectrum access (DSA). For example, Jouini et. al. [6] defined DSA into exclusive use (i.e., property rights, allocation), open sharing, and hierarchal use (e.g., spectrum underlay (ultra-wideband) and overlay (opportunistic)).

CR can also be viewed from a software perspective. For the artificial intelligence (AI) community, CR implies methods of learning and adaption. For network and protocol designers, CR implies devices with cross-layer optimization. As a final example, information theorists view CR as channels with side information from which to utilize network capacity.

In addition to these explorations, there is a need to also address QoS attributes such as network survivability and trustworthiness. A survivable network is based on QoS secure communications of confidentiality, integrity, availability, and access control [8]. Survivability is related to the jamming resistance of a network. CR can provide a means to utilize the spectrum to mitigate source-level jamming [9, 10]. As another example of effectiveness, CR would need to address the trustworthiness in delivering sustained, maintainable, and consistent QoS parameters. While survivability and trustworthiness are not the only measures of effectiveness (MOEs) needed, future CR definitions and protocols would
need to be established over measures of performance (MOPs) (e.g., time delay, probability of error, throughput) to standardize the CR community.

The purpose of this paper is to highlight the emerging trends in survivable networks. Section II presents the CR standards and Section III discusses cognition of a network. Section IV presents the trends from a panel discussion on secure aerial networks and Section V presents a way forward, with Section VI providing conclusions.

II. COGNITIVE RADIO DEFINITIONS

IEEE is currently standardizing CR developments [1]:

- **P1900.X**: IEEE Standard Series on Next Generation Radio and Spectrum Management. [In 2010, the committee was renamed as the IEEE DySPAN Standards Committee (DySPAN-SC)]
- **P1900.2**: Recommended Practice for Interference and Coexistence Analysis
- **P1900.3**: Recommended Practice for Conformance Evaluation of Software Defined Radio (SDR) Software Modules [The working group has been disbanded, but included in the list]
- **P1900.4**: Architectural Building Blocks Enabling Network-Device Distributed Decision Making for Optimized Radio Resource Usage in Heterogeneous Wireless Access Networks
- **P1900.5**: Policy Language and Policy Architectures for Managing Cognitive Radio for Dynamic Spectrum Access Applications

Developments in CR are available through the IEEE working groups [12]; however what is missing from the list of evolving standards is elements of survivable and secure networking. These preliminary definitions will lead to standards for survivable networks for such applications as space [9, 10] and air-ground communications [13]. Space communications has unique factors of time delays and predictable orbital patterns which make these systems vulnerable to latency, interference, and jamming effects. Methods of transponder grooming and open-loop spectrum hopping can be used for uplink/downlink jamming mitigation; however cognitive spectrum awareness has yet to be included. For aerial networks, the terminal position is moving, the spectrum is limited for frequency reuse, and data transmission (i.e., video) can be large. The IEEE standards can serve as the basis for developing CR standards over unique space and aerial applications which requires an extended definition of the cognition of a network.

III. COGNITION OF A NETWORK

Cognition for spectrum management seeks to utilize elements of the static allocated spectrum for increased communications. Mitola [14] proposed Cognitive Radios (CR) for the opportunistic allocation of the under-utilized portions of the spectrum. Multiple CRs form a CR Network (CRN). Mitola's original idea is adapted from Boyd's Observe-Orient-Decide-Act (OODA) control loop [15], shown in Fig. 3.

![Figure 3 – The Extended OODA Loop.](image)

Mitola [14] presents six areas of cognition to include planning and learning with OODA characteristics and CR extensions from SDR. The cognition cycle learns from the environment for intelligent control. The cognition cycle follows the trends in human performance analysis such as the cognitive OODA (C-OODA) [16]. The six methods, shown in Fig. 4, are:

- **Observe**: Know the information of operating environment through sensing and signaling mechanisms.
- **Orient**: Evaluate this information to determine its significance and relevance.
- **Plan**: Based on this evaluation, the radio determines its options or alternatives for resource optimization.
- **Decide**: An alternative is chosen that evaluates more favorably than other options, including the current ongoing action.
- **Act**: The radio implements the decisions taken for resource optimization where changes are reflected in the interference profile presented by the CR in the outside world.
- **Learn**: Throughout the process, the radio uses its observations and decisions to improve its own operation, creating new modeling states and alternatives.

![Figure 4 – Cognition Cycle [adapted from Mitola, 14]](image)
The cognition cycle brings in planning and adaption to the control cycle. Some issues of the original model are based on the definitions, such as the continual learning of the network; however, the learning is not adapted within the OODA loop as per Boyd’s model where the orient phase presents adaptive learning. Jouini et. al. [6], presents the orient phase as establishing normal priority and plan generation to help the decision phase to allocate resources. In order to establish secure communications, planning has to learn from the capabilities and utilize such notions as game theory to determine or decide if an action is appropriate. To update the model towards secure networks, the system would have to learn before action, as shown in Fig. 5.

Figure 5 – Learning in Cognition Cycle

CRs devices sense the spectrum and use its free portions in an opportunistic manner, but must also address threats. The notion of a primary user (i.e., band of frequencies assigned to at a particular time and specific geographic location, and not being utilized) only supports a potential opportunity. Since a CR device observes its environment, it can use a variety of spectrum sensing methods (e.g., energy detection [17], filter matching, cyclostationary detection), and spectrum management decision techniques (e.g., Bayesian, evidential, cooperative, distributed, etc.) [18].

In addition to spectral awareness, the cognitive radio network needs to be aware of the applications that are using it and the network topology. The kinds of sensors, priority of data, and general information management, lead to requirements on the quality of service (QoS) that the system must support and are communicated to the CR through the applications. Threats to successful communication from noise, interference, and malicious activities must be taken into consideration [6, 19]. For example, QoS metrics for distributed networks could be used to detect threats and network diversity might be used to mitigate them [20]. In the spectral domain, threat awareness comes from a combination of power and interference analysis [21]. To provoke discussion and determine issues that are needed to ensure a survivable CRN, a group of panelists formulated a set of emerging trends at the Cyber and Information Challenge Conference, held at SUNY-IT, in June 2012.

IV. TRENDS IN COGNITIVE RADIO

To frame the current CR needs, we map the trends to the OODA cycle, which was inherently designed to describe the MOPs of timeliness and efficiency in human-decision making. However, there are elements of MOEs of survivability and availability that are needed to fully execute a CR network. The recent panel discussion brought together experts to identify current trends and future research. The focus of the discussion was on aerial networks.

A. Issues for Secure Aerial Networks

The discussions were wide ranging and included topics on:

- Legacy techniques embedded in existing systems;
- Compression to accommodate aerial platforms;
- Next generation waveforms-- chaotic waveforms, quantum communications;
- Network management - tools and metrics to determine operational effectiveness;
- Effects of security on cross layer methods;
- User community - QOS and value of data issues; and
- Trust (secure) complicated by ad hoc implementations.

From these topics, there was further discussion on systems-level designs that incorporate CR methods. The design process must be modified to accommodate problems (recognizing them and fixing them) from the use of CR methods.

Hardware
- Supporting legacy systems;
- Spectrum sharing over cross functional applications (communications, radar, navigation, etc.);
- Data preparation over different types of formats;
- Policy design in a machine accessible protocol; and
- Resolving resource conflicts (e.g., languages for expressing strategies, market driven policies, etc.).

Software
- Using security techniques (e.g. immune systems; reputation; biomimetics for user verification);
- Creating cognitive capabilities at all levels;
- Measuring of value of information for decision; and
- Understanding the vulnerability space for action.

The system design issues related to CR technology, resulted in a list of the top trends needed for secure and survivable (aerial) communication. Two recent examples include data sharing in ultra wideband (UWB) systems and data preparation for multimedia applications. UWB is a radio technology for low energy, short-range, high-bandwidth communications using a large portion of the radio spectrum [22, 23, 24]. UWB applications include non-cooperative radar imaging, sensor data collection, precision locating, and target tracking. UWB has unique hardware CR issue of antenna design, energy detection [25], overhead protocol analysis [26], distributed network sensing [27], distributed routing analysis [28], waveform design [29], and compressive sensing [30, 31, 32]. The emergence of UWB requires pragmatic inclusion of threat and situation awareness in spectrum sensing and spectrum data sharing.

Another closely related example presented was UWB multimedia applications [33]. Multimedia (e.g. video) requires
intelligent methods for data preparation. From different types of data, prioritization [34], routing [35, 36], and error protection [37] are needed. Future secure and survivable networks will require data preparation for processing, exploitation, and dissemination of information such as multisource video applications [38, 39, 40, 41].

B. Top Trends in Secure CR methods

Given the many issues of CR developments, we first had to define CR and the domain of interest such as aerial networks. Then a listing of existing issues in system design initiated the discussion. Through the UWB and multimedia examples, the top trends were formulated. Our current list of trends includes the standard classifications, but delineated into the application, information, network, and joint optimization categories:

TYPE OF NETWORK
- Spectrum Sensing for classification of networks
- Spectrum Sharing for cross-functional determination

TYPE OF INFORMATION
- Dynamic spectrum management over different data types
- Data preparation for multimedia content prioritization

TYPE OF APPLICATION/SENSOR
- Antenna pattern control (e.g. MIMO, cognitive radar)
- Operation and legacy system coordination

JOINT OPTIMIZATION
- Dynamic routing over sparse networks
- Dynamic cross-layer optimization

From the “cognitive” aspect of networking, we utilize concepts from decision-making to determine who, what, where, when, and how to transfer information based on the business, operational, and collaborative needs of people, organizations, and missions. The cognitive decision-making for situation awareness requires needs and capabilities that extend CR networks for these issues:

- Mission-driven bandwidth optimization: robust operations over different situations;
- Resource analysis: market-driven language of expression;
- Policies: user and network QOS reconfiguration;
- Information value: metrics for network control [42]; and

Using Fig. 5, the areas of research trends can be placed in the cognitive cycle. From Fig. 6, the cycle includes the application and type of sensors as the operation and priori states for the antenna patterns. Spectrum sensing and spectrum sharing result from a standard OODA analysis as discussed in the definitions of CR. Key to future secure networks is the type of network and information. Applications must consider legacy systems and hardware in addition to intelligent adversaries [43]. Data preparation and dynamic spectrum management afford orientation and action, respectively. Finally, the techniques for survivable networks include elements from learning (new states) of for dynamic routing and cross-layer optimization.

![Figure 6 – Emerging Trends as applied to the Cognition Cycle](image)

V. WAY FORWARD

Mapping these trends into the six-step cognition cycle model can extend the efficiency of CR networks were all information and users are of equal value. Also, effectiveness of operations over the various information needs, network types, and applications can be accommodated for joint optimization and survivability. The application issues include:

- **Sense**: Observe the network type and need;
- **Orient**: Policy determination and market costs;
- **Plan**: Management across the available spectrum;
- **Learn**: Cross-functional optimization and sensing;
- **Decide**: Allocation based on value of information; and
- **Act**: Dynamic routing based on security needs.

Like Boyd’s original model, Fig. 3, future CR techniques will revolve around the orient phase such as FCC policies. An emerging example is cloud computing [44], from which CR will receive and send network message traffic which can be aided with intelligent CR decision making.

VI. CONCLUSIONS

Based on the recent issues presented in papers that cover the CR network issues [2-4, 6-7], the next decade must focus on the unequal considerations of users, information, and networks to truly enable an intelligent cognitive-based approach to dissemination of information. These trends include the spectrum sharing and prioritization, dynamic spectrum management through data preparation, adaptive configuration based on sensors and hardware considerations, and dynamic cross-layer optimization over missions, policies, information values, and network classifications.

ACKNOWLEDGMENT

The authors recognize the many participants at the Cyber and Information Challenge Conference that contributed to the forum to discuss the current trends in secure CR networks.

REFERENCES
