Assessment of Cognitive Radio Technology for Public Safety Communications

Working Document WINNF-13-P-0003

Version V1.0.0

13 June 2013

TERMS, CONDITIONS & NOTICES

Table of Contents

Executive Summary

The Wireless Innovation Forum's Public Safety Special Interest Group (SIG) has been studying the potential impact of cognitive radio technology on public safety communications for several years. Previous studies have documented in detail scenarios describing communications occurring at a major incident and a description of how cognitive radio capabilities could enhance user communications directly relevant to effectiveness of the incident response activities. In this report, we define a list of desirable functional capabilities that we derived based on that analysis, an RFI distributed to the industry, and a literature survey. We then identify ongoing research into developing capabilities identified as needed, and assess the maturity of the technology, as well as research gaps.

From the results of the survey and our own analysis, we believe that there is significant ongoing research in Cognitive Radio technologies that can be leveraged to benefit public safety. Software defined radio and cognitive radio technologies have potential to provide important capabilities for public safety communications networks, including enhanced interoperability, coverage improvement, interference mitigation, dynamic spectrum access, more effective management of communications resources, and the ability to configure to meet incident command requirements. There is ongoing research in many of these areas, but additional work will be required to adapt technology developments to meet specific public safety needs. One area in which there is no significant research is the ability to configure to meet incident command requirements, as this is unique to public safety. We recommend appropriate investment in these areas to fully take advantage of software defined radio and cognitive radio capabilities to provide public safety with an effective communications capability.

Contributors

Ihsan Akbar	Harris Corporation
Peter Cook	Peter G. Cook Consultancy
Fred Frantz	Engility Corporation
Phil Harris	Engility Corporation
Stephen Hope	Docobo Ltd.
Ken Klassen	RCMP
Ken Link, Jr.	New Jersey State Police OEM
Stew Potter	Harris Corporation
Al Sadowski	North Carolina Highway Patrol
Rick Taylor	Harris Corporation

Assessment of Cognitive Radio Technologies for Public Safety

1 Overview

The objective of this Cognitive Radio Technology Assessment study is to:

1. Define a set of desirable functional capabilities for public safety communications systems that leverage evolving cognitive radio technology;

2. Survey cognitive radio technology research activities, to identify projects that might facilitate the deployment of desirable capabilities; and

3. Identify research gaps as input to a broad research, development and implementation agenda for consideration by government, academic, and commercial researchers.

This effort follows two previous studies[1,2] published by the Wireless Innovation Forum's Public Safety SIG that identify use cases for advanced communications technology. Each study included an analysis that documented in detail a scenario describing communications occurring at a major incident; a description of how advanced communications capabilities could enhance user communications directly relevant to effectiveness of the incident response activities; and a list of desirable communications capabilities identified by the SIG for each use case. In this report, we map the detailed information in the use cases to a more succinct list of desirable functional capabilities, and then analyze ongoing research into developing these capabilities, and assess the maturity of the technology as well as research gaps. We solicited input on the status of ongoing research activities through a published Request for Information (RFI), which provided useful summary information. To supplement that data, we surveyed recent published academic and trade literature to assess the state of ongoing research.

Based on the analysis, we draw the following conclusions:

1. We identified more ongoing research work in the area of interoperability than any of the other topic areas. We attribute this to the high visibility that interoperability issues have been given over the past several years. Various approaches have been developed to achieve interoperability[3], including common waveforms, gateways, and standards. Software-defined multiband radios provide new options for achieving interoperability by

[1] Wireless Innovation Forum, Use Cases for Cognitive Applications in Public Safety Communications Systems - Volume 1: Review of the 7 July Bombing of the London Underground, Report No. SDRF-07-P-0019-V1.0.0, available at http://groups.winnforum.org/d/do/1565.
[2] Wireless Innovation Forum, Use Cases for Cognitive Applications in Public Safety Communications Systems Volume 2: Chemical Plant Explosion Scenario, Report No. WINNF-09-P-0015-V1.0.0, available at http://groups.winnforum.org/d/do/2325.
[3] We define interoperability from the public safety standpoint as the ability of first responders to communicate (voice and/or data) even if they are from different agencies, utilize radios that operate on different frequency bands and/or different protocols and modulation types, and so on.

allowing devices to operate on networks using different frequency bands. Significant progress has been made in both technical and non-technical aspects of interoperability; while we encourage this work to continue, the accomplishments to date in this area mean that resources can be better used on other areas such as resource management and better linkage of communications capabilities to incident command. (See Section 4.1 for a more detailed discussion of desirable capabilities for interoperability based on cognitive radio technology, and Section 5.1 for an assessment of the maturity of research in enhancing interoperability.)

2. There is significant research and development ongoing in the areas of coverage enhancement. Some development may be necessary to adapt the technology to specific public safety requirements, but much of the needed capability will be inherent in commercial products and capabilities, particularly in wireless broadband data networks. (See Section 4.2 for a more detailed discussion of desirable capabilities for coverage enhancement based on cognitive radio technology, and Section 5.2 for an assessment of the maturity of research in coverage enhancement.)

3. There is significant research and development ongoing in the areas of spectrum utilization optimization and dynamic spectrum access. Some development will be necessary to adapt the technology to specific public safety requirements, since some of the ongoing research is focused on unlicensed spectrum utilization and spectrum sharing, which would have specific requirements in a public safety context. (See Section 4.3 for a more detailed discussion of desirable capabilities for spectrum utilization optimization and dynamic spectrum access based on cognitive radio technology, and Section 5.3 for an assessment of the maturity of research in spectrum utilization optimization and dynamic spectrum access.)

4. Research work in communication of reconfiguration information is generally specific to implementation of a broader capability (e.g., dynamic spectrum access, network optimization), rather than being addressed as a separate research topic. (See Section 4.4 for a more detailed discussion of desirable capabilities for communication of reconfiguration information, and Section 5.4 for an assessment of the status of research in this area.)

5. Ongoing research in cognitive-based management of communications resources has potential for more effective public safety communications, but will need adaptation to apply to public safety networks. For example, there are a number of capabilities defined in LTE and LTE-A (see Section 5.5) that can provide a mechanism for cognitive-based resource management. Additional effort will be required to most effectively tailor the capability to public safety requirements, due to differences in commercial and public safety objectives.[4] For example, while LTE provides capabilities for dynamic prioritization, additional effort is required to provide the tools to exploit network data and incident command decisions to effectively utilize the dynamic prioritization feature of

[4] For a discussion of difference and commercial and public safety objectives, see “Utilization of Software Defined Radio Technology for the 700 MHz Public/Private Partnership,” Document SDRF-08-P-0004-V1.0.0, 19 June 2008, Available at http://groups.winnforum.org/d/do/1564.

LTE. (See Section 4.5 for a more detailed discussion of desirable capabilities for management of communications resources based on cognitive radio technology, and Section 5.5 for an assessment of the maturity of research in communications resource management.)

6. We found little research on tying emerging communications capabilities to the support of incident command. This topic is unique to public safety, which may account for the lack of ongoing work, but as noted in the desirable capabilities, leveraging emerging communications capabilities and providing appropriate tools for incident command can provide more effective and efficient communications for public safety. (See Section 4.6 for a more detailed discussion of desirable capabilities for supporting incident command based on cognitive radio technology, and Section 5.6 for an assessment of the maturity of research in supporting incident command.)

7. Our previous use case that addresses rolling back, at the end of an incident, communication system changes to their previous state is being addressed by current development and ongoing research in technology to manage communications resources. (See Section 4.7 for a more detailed discussion of desirable capabilities for configuration rollback based on cognitive radio technology, and Section 5.7 for an assessment of the maturity of research in configuration rollback.)

8. Finally, we note that public safety adoption of commercial wireless broadband standards such as LTE may yield improvements in system performance. Discussion of the role of LTE, particularly in evolving capabilities for resource management, is included in Section 5.5. We also identify potential for incorporating technologies developed for LTE systems into existing land mobile radio (LMR) systems in Section 5.2, which could also facilitate convergence of broadband data and voice capabilities.

The remainder of this document provides details on desirable functional capabilities, an assessment of ongoing research with respect to the capabilities, and the research gaps. We provide a brief summation of the motivation and objective of this report in Section 2 and methodology in Section 3. Section 4 includes the listing of the desirable functional capabilities derived from the use case documents, and in Section 5 we present a summary of the assessment of the research from both the RFI responses and our own analysis. Our conclusions are presented in Section 6.

2 Motivation

Cognitive radio technology is rapidly evolving in both military and commercial domains. While certain aspects of today's public safety radio systems incorporate some level of cognitive capabilities (e.g., it can be argued that trunked public safety radio systems and roaming capabilities meet the definition of "cognitive radio"[5]), there is significant potential for much

[5] The term "cognitive radio" has been defined in a variety of ways. For definitional purposes, we use the definition published in IEEE 1900.1: "a) A type of **radio** in which communication systems are aware of their environment and internal state and can make decisions about their radio operating behavior based on that information and predefined objectives.
b) Cognitive radio [as defined in item a)] that uses **software-defined radio**, **adaptive radio**, and other technologies to adjust automatically its behavior or operations to achieve desired objectives." A more detailed analysis of various definitions of

broader application of cognitive radio technology to enhance public safety communications systems. While Dynamic Spectrum Access (DSA) is often identified as the key objective for cognitive radios, there are additional potential applications of cognitive radio technology that the Public Safety SIG identified in the two detailed studies referenced above.

As noted above, the Wireless Innovation Forum has identified a number of areas in which cognitive radio technology could significantly enhance public safety communications. The analysis on which these conclusions were based did not address the feasibility or maturity of technology to implement the proposed concepts, instead focusing on the requirements for such functionality. The feasibility aspect of the study was deferred to this report, which involves assessing the state of research into these specific technologies, assessing the maturity of technology to understand near-term opportunities for technology insertion as well as longer-term research projects, and identifying research gaps for which additional investment may be recommended.

Data within this report will help provide public safety community leadership, researchers, product developers, regulatory, and standards developers with information that:

- Helps public safety agencies plan communications system life cycles
- Informs public safety standards and regulatory bodies regarding evolving systems capabilities
- "De-mystifies" cognitive radio for public safety leaders and users,
- Identifies technology gaps and dependencies for researchers, and
- Supports roadmap development efforts of the Wireless Innovation Forum.

In addition, the identification of research gaps will be helpful to federal and other research agencies in planning and prioritizing research programs.

3 Summary of process/methodology

The initial studies (the Use Case documents referenced in footnotes 1 and 2) identified twelve (12) use cases and over sixty functional capabilities. The first step of the follow-on study discussed herein was to compile and organize these functional capabilities, combine similar capabilities, and organize them into broad categories. The results of this step, presented in Section 4, provide a concise summarization of desirable cognitive radio capabilities for public safety communications.

Next, to solicit input from the research community at large, the Forum published a Request for Information (RFI) to solicit input on research activities applicable to the desired capabilities listed in Section 4. The RFI was published as both a written request and as a survey that could be completed on-line. To provide a more comprehensive picture of the state of research, we

cognitive radio and similar terms can be found in *Cognitive Radio Definitions and Nomenclature,* Document SDRF-06-P-0009-v1.0.0.

augmented the data that we received by reviewing a comprehensive analysis of cognitive radio research published by the Wireless Innovation Forum[6], and then more recent papers from relevant conferences of the past two years, including the Wireless Innovation Forum (WInnComm), IEEE MILCOM, IEEE GLOBECOMM, and IEEE Dynamic Spectrum Access Networks (DySPAN) conferences.

In addition, we reviewed a number of other journals and magazines, and followed up with personal conversations. We identified papers that addressed the above research topics, and have summarized the overall perspective in the discussion in Section 5.

4 Desired cognitive radio capabilities for public safety

The aforementioned use case reports were developed by analyzing major incident scenarios (one actual, the July 2005 bombing of the London underground, and one hypothetical based on an explosion at a chemical plant resulting in onsite fatalities and release of hazardous chemicals). In the analysis, the Public Safety SIG reviewed scenario events and postulated cognitive radio technologies that could have improved the communications element of the incident response. Using a scenario-based approach ensured that the proposed functions, or functional capabilities, were grounded in real needs identified by public safety.

The analysis resulted in definition of twelve (12) use cases; each use case included a set of cognitive radio-based functional capabilities that could have improved the communications, and were thus identified as desired functional capabilities. As part of developing this report, we analyzed these functional capabilities, combined similar or overlapping capabilities, and organized the capabilities into major groupings. The result is the summary of desired cognitive radio capabilities, as described in the following sections.

4.1 Interoperability for Public Safety

It is common during major incidents that first responder support will come from locations other than the one with primary jurisdiction. Numerous issues arise as personnel from other organizations arrive; they are assigned roles in the incident command structure, join newly established command nets, bring the situation under control, and ultimately revert to routine operations.

A number of technological and operational issues exist for voice and data systems that may impede the emergency responders' ability to interoperate because of incompatible systems. Current technological solutions for providing voice interoperability through disparate systems range from console audio patches to cross-band repeaters to audio switches and other network-based solutions. Such implementations facilitate interoperability, but they typically require a layer of additional equipment external to the core communications systems. Bridge devices require the same transmission to be concurrently broadcast over multiple radio systems and frequencies within the same geographic area, thereby requiring additional system capacity and

[6] Wireless Innovation Forum, "Quantifying the Benefits of Cognitive Radio," Document WINNF-09-P-0012, 2 december 2010, available at http://groups.winnforum.org/d/do/3839.

spectrum. Deployable repeaters and switches require time to mobilize, and once on site need additional time to configure and activate.

Another logistical issue that arises with the deployment of this technology into use to support Public Safety incidents, is whether they are pre-planned or events that evolve in real-time: A the need for trained and technically competent operational staff to install, maintain and monitor these devices, systems, networks, and other configurations during an incident or event. One of the key requirements for interoperable solutions is to make the Incident Commander's job manageable by allowing the seamless communication of agencies with disparate systems, and the ability to perform these tasks while not causing any additional escalation of the event. When properly trained personnel in the role of Communications Unit Leader (COML) or the Communications Technician (COMT) are on an incident scene overseeing this interoperable technology exchange, risks are minimized as communication deficiencies arise.

Desired innovations include those that will improve end user radio equipment and systems, minimizing or eliminating dependence upon an overlay of specialized interoperability equipment. Examples of such innovations include the following:

- "Smarter" gateway devices between legacy technologies to enable voice and/or data communications
- Advanced interoperability concepts utilizing multiband radio technology (at both the end-user and infrastructure levels).
- Innovations for voice interoperability between P25 and other standards (e.g., non-P25 systems)
- Innovations for enhanced data interoperability (e.g., interoperability among disparate mix of broadband through low speed data systems)
- Interoperability between new and legacy technology (e.g., voice interoperability with broadband network
- Innovations that standardize procedures to facilitate the ability of "visiting" responders to appropriately access local communications capabilities (such as a "meeting point")
- Creation of a "Virtual System" from multiple disparate systems

As with interoperability between public safety agency users, the Use Case documents identify a significant requirement for interoperability between first responders and non-public safety communications systems. For example, communications may be required between first responders, emergency management users, and users from other organizations such civilian government authorities (e.g., public health, public works, transportations), organizations supporting critical infrastructure (e.g., utilities), tow truck and bus drivers, National Guard, Department of Defense units. In some cases it also may be beneficial to allow more seamless communications capabilities between users with selected cell phones and public safety network users, with appropriate restrictions. This need can arise during major disasters and events as well as daily operations of public safety agencies.

Innovations that will enhance communication capabilities between non-public safety resources and public safety users are also of interest. Examples of such innovations include prioritization of access and throughput, store-and-forward capabilities, integration of temporary capabilities in support of incident command (IC) structure operations, and maintaining the security and integrity of public safety communications.

4.2 Coverage Improvement

System coverage, i.e. providing radio access to voice and data system resources, is an important requirement in a public safety communications system. The ideal solution for a public safety communications system would provide access to all services at all location where a first responder may be needed (or need assistance), at all times, with perfectly understandable voice quality and ensured data delivery at acceptable data rates. This would include access within traditionally difficult locations such as basements, stairwells, tunnels, and buildings where users often experience well over 30 dB RF signal penetration loss. Cost-benefit trade-offs made when procuring and designing public safety communications systems (as well as immutable factors such as the laws of physics) result in systems that do not meet the ideal solution of ubiquitous access. Also, in recent real-world cases like the London Bombing and Katrina disasters, system access was further (and severely) compromised by loss of key supporting infrastructure, such as radio network base stations, radio towers, and tunnel coverage devices. Thus there is a continuing need to develop cost-effective means for improving system coverage in general, as well as provide capabilities to rapidly adjust to the loss of infrastructure that impacts coverage.

Examples of such solutions may include the following:

- Reconfiguration of responders' radios, to create an ad-hoc extension to an existing network. Such network extension would allow transmissions to be passed back and forth from the incident site through a network of individual responder radios operating in peer-to-peer mode effectively extending coverage of the main radio system/network.
- Use of adaptive beamforming antennas to maximize gain in the direction of the desired communication path and possibly also minimize gain (create a null) in the direction of a known interfering signal.
- Standards for interfacing "smart antennas" with cognitive radios (to define parameters such as band, power capability, direction, null direction, polarization, and so on).
- Adaptive modulation and data rate adjustment for modifying the link budget and interference generation (on transmit) or suppression (on receive).
- "Smart" frequency control to increase frequency separation between interference sources and the desired radio signal.
- Adaptively reconfigure receiver filter characteristics to provide improved rejection of an interfering adjacent signal (e.g., by narrowing the receiver filter bandwidth) or improved sensitivity when interference isn't limiting coverage.
- Enhanced and/or adaptive channel coding algorithms
- MIMO techniques

- Adaptive receive processors

As another means for enhancing coverage, access to non-public safety network resources may be a viable option for public safety. For example, additional data bandwidth may be operationally required even in areas where voice coverage and capacity meet user requirements. Broadband services provided via TV spectrum whitespace, or access to commercial services via cellular provider data facilities may be exploited as a supplemental, or fallback, resources. Access to supplemental resources would require appropriate wireless communications equipment in vehicles, and appropriate policies must be formulated and implemented, defining when such links could be activated.

4.3 Spectrum Utilization Optimization and Dynamic Spectrum Access

One of the critical issues faced by the public safety community is limited availability of RF spectrum to address current and emerging requirements for mission-critical communications. Increasing public safety reliance on bandwidth-intensive data such as video, paired with limitations on the number of available narrowband voice channels when responding to large scale complex incidents, creates increasing pressure for spectrum resources. Cognitive radio technology provides promise as a technological path for addressing this issue. Specific capabilities include those that:

- Identify and optimize network capacity and loading. For example,
  - prioritize transmissions;
  - control access priority, per subscriber unit;
  - adjust network operations to accommodate significant changes in traffic volume;
  - accommodate direct communication between first responders and non-first responders;
  - re-allocate spectrum used by public safety users as incident response communications demands decline; and
  - identify and mitigate capacity issues with wireless or wireline backhaul components of the network.

- Dynamically access additional spectrum resources in the most effective manner, consistent with regulations and policy. For example,
  - identify situations, and associated threshold criteria, whereby dynamic spectrum access can be initiated;
  - identify available spectrum resources that can be utilized (sensing and policy limited);
  - exploit all available spectrum resources as needed, and integrate additional spectrum resources into existing communications capabilities, including disparate frequency bands and protocols;
  - adjust spectrum utilization based on defined regulations and policy (e.g., a network sharing agreement); and
  - aggregate multiple radio networks to provide improved data rate, coverage and redundancy.

4.4 Communicate Reconfiguration Information

Public safety communications are generally provided through a network consisting of infrastructure accessed by number of end-user (subscriber) devices. Thus system reconfiguration decisions cannot occur independently, and must be coordinated through all network components. Decisions must be based on knowledge of the current configuration of all nodes that are part of the network, and reconfiguration commands must be transmitted to affected nodes securely and reliably.

Most public safety land mobile radio infrastructure network configurations are static, based on a pre-planned configuration. Some networks have a limited ability to communicate reconfiguration information to end user devices, using technology such as over-the-air programming (OTAP), typically through narrowband channels, or distribute encryption keys and re-key end user devices via over the air re-keying (OTAR) technologies.

Key capabilities include the following:

- Standard methods for query and exchange of information among the network infrastructure and end user radios. Examples of information include vendor, network/end user radio type, and capabilities (e.g., available modes, version numbers, reconfiguration capability, etc.)
- Identify and communicate accessible spectrum resources that can be utilized to offload some calls based on real-time identification of available spectrum.
- Reconfigure subscriber and/or network radios and antennas to access additional spectrum resources when required.
- Rapidly adjust air interface transmit power, waveforms, frequencies, filtering, and receiver attenuation based on network and end user radio commands.
- Specify and reconfigure air interface transmit and receive parameters, for either a single transmission or a message sequence.
- Reconfigure/reprogram radios over the air with ensured integrity

4.5 Manage Communications Resources

Real-time management of network resources is critical, particularly when specific situations in which incident communications requirements exceed system capacity, creating a need for more effective network resource management tools than those that are commonly available today. The likelihood of the occurrence of such situations will increase as bandwidth-intensive applications such as video become more prevalent in incident response. Optimizing public safety spectrum use in critical situations and assessing available spectrum resources in support of the most critical operational needs on a real-time basis, is essential for ensuring that effective in communication capabilities are maintained for future incident, responders. The required innovations are needed for both public safety-only networks and public-private networks.

Technologies of interest include those that can manage communications resources. Examples of possible related innovations include the following:

- Monitor network resource allocation and associated issues, including anticipating network resource allocation issues, providing an effective display of current conditions, and generating appropriate notifications and alarms.
- Provide information about the RF environment at a user's location.
- Geolocate network nodes.
- Predict signal and interference levels at any potential subscriber location.
- Seamlessly integrate additional communications resources with existing networks.[7]
- Communicate in a standardized way the status of communications assets to support network utilization and Comm Unit Leader[8] functions and tools

4.6 Support Incident Command

Typical public safety mutual assistance activities involve personnel responding from multiple agencies and arriving on scene as part of a large incident response. Given the scope of such incidents, responders may be from jurisdictions for which there are no standing mutual aid agreements and when in place are not equipped to support pre-planned communications interoperability plans. Upon arrival at the incident, end user wireless devices may not be directly interoperable with local communications systems being used to manage incident response. A desired technological capability is that such wireless devices can be dynamically reconfigured to support the in-operation pre-defined incident response, and also support the arriving responders' role within the incident response structure.

For example, often the capability that an arriving public safety responder needs (and therefore his/her wireless device should support) support is defined by the role that the responder is performing—for example, supervisors in the incident command structure require capabilities that responders in other roles do not. This concept provides the incident response management team greater control of communications resources, ensuring that ubiquitous interoperability does not result in "everyone talking to everyone at once on the same frequency." After arrival on scene, following device reconfiguration to support a specific role, mechanisms must also be in place to ensure that device reconfiguration was successfully executed.

Reconfiguration of wireless devices to meet requirements of the incident response often means modification of their operating parameters, or verification of current configuration. It is also essential that provisions be in place to restore device configurations to their pre-response state in support of ongoing normal operations.

[7] For example, in a disaster scenario in which existing infrastructure is partially, but not totally disabled, and as parts of damaged/destroyed infrastructure are gradually brought on-line, temporarily deployed resources should adjust seamlessly.
[8] Comm Unit Leader is a specific function defined in the National Incident Management System (NIMS) adopted as a standard in the United States for incident response. Other incident management systems/procedures are assumed to have comparable functions.

In today's public safety environment, unlike devices in commercial cellular networks, reconfigurations are typically manual in nature, complicated, and require a responder to report to an incident staging area equipped to make device modifications. In addition, land mobile radio configuration templates are often based on static definition of day-to-day communications capabilities, independent of the actual role that the responder has in supporting the incident command structure.

Examples of possible related innovations include the following:

- Identify an over-the-air "meeting point" for incoming responders to register and receive configuration information.
- Associate users, radios, radio capabilities, and user roles (e.g., roles within a NIMS construct). For example,
    - Define explicitly (i.e., in a machine-interpretable form) user roles within an incident response structure.
    - Store in a machine-interpretable form a user's credentials.
    - Authenticate a specific user as qualified for a specific role.
    - Define appropriate radio capabilities in support of a specific user's role.
- Dynamically reconfigure communications device capabilities (both subscriber and network capabilities) using criteria based on both the user's current role, and incident policy, mitigating how dynamic reconfiguration negatively impacts ongoing communications and minimize bandwidth required to support over the air transmittal of device reconfiguration information.

4.7 Rollback Configuration Changes

Given the capability to reconfigure communications capabilities in near-real-time, there must also be a capability to undo, or roll back, configuration changes if they result in unintended consequences, otherwise degrade communications, or to simply restore a communications device to a pre-incident configuration. For the situation in which a reconfiguration needs to be rolled back, networks and subscriber devices may maintain a configuration history that allows previous configurations to be restored. However, rolling back a configuration change that involves the network and subscriber equipment is not typically automated in current systems. Thus changes that turn out to have a negative impact on communication usually can only be reversed by manually resetting subscriber equipment software configurations.

In the case of restoring default or home agency configurations as a responder is released from an incident, the most significant shortfall is associated with radios that cannot be reconfigured over the air. Reprogramming many legacy radios that must be tethered/cabled to programming hardware can require a significant amount of time (days or weeks) due to the logistics of transporting radios to a reprogramming point to manually loading configuration software updates. Radio security is not specifically addressed here, but some LMR manufacturers require use of special hardware or software keys prior to accessing radio configuration functions, creating additional logistical challenges.

Example capabilities include:

- Storing previous device configuration information.
- Recognizing when a device reconfiguration results in a degraded capability.
- Restoring or rolling back the device capabilities to a previous configuration.
- Rapidly restoring a default configuration and/or the configuration of the device prior to the incident.

5 Conclusions on research activities and research gaps

The initial level of information that we obtained from the RFI was a distribution of the responses in the seven topic areas outlined in Section 3. The number and percentage of responses by topic area is shown in Table 1.

Table 1, Distribution of Responses by Topic Area

Topic Area	Responses	Percent
1 - Interoperability for Public Safety	28	54%
2- Coverage Improvement	2	4%
3- Spectrum Utilization Optimization and Dynamic Spectrum Access	14	27%
4- Communicate Reconfiguration Information	3	6%
5- Manage Communication Resources	3	6%
6- Support Incident Command	2	4%
7- Rollback Configuration Changes	0	0%
Total	52	100%

We observe that over half of the responses addressed the topic of interoperability. This is consistent with the emphasis that has been placed on interoperability, particularly within the public safety community, in the last decade.[9,10] In addition, there have been a number of high profile events such as the 9/11 terrorist attacks in the U.S., the bombing of the London underground in 2005, and Hurricane Katrina in which interoperability issues impacted the effectiveness of the response. While there has been significant progress in both the technology and operational aspects of interoperability, the responses indicate that an active area of research is to develop faster, cheaper, more efficient, more effective, and more robust technical solutions

[9] "Why Can't We Talk?", National Institute of Justice, February, 2005, available at https://www.ncjrs.gov/pdffiles1/nij/204348.pdf (last accessed November 13, 2012.

[10] The U.S. Department of Homeland Security established a program (SAFECOM) specifically focused on improving interoperable communications among public safety agencies. (http://www.safecomprogram.gov/).

for interoperability. We attribute the large percentage of responses in this area to the fact that interoperability has been highlighted for an extended period of time as a critical issue for public safety.

The topic that received the second highest number of responses was "Spectrum Utilization Optimization and Dynamic Spectrum Access". While this is a broad technical area which may have contributed to the high number of responses, we recognize that this is an active research area with numerous applications including public safety. Thus there is a significant amount of research that, while not specific to public safety, could be adapted to enhance public safety communications. For example, one of the areas within this topic that is receiving extensive research is use of TV White Space—which could be adapted for public safety communications as an alternative spectrum resource during the high bandwidth demand of a major incident. A recent report of the President's Council of Advisors on Science and Technology (PCAST) also highlighted the potential of spectrum sharing technology and called for additional research and development.[11]

The remaining topics, even taken together, represent less than 20% of the responses. Perhaps most surprising was the lack of responses in the area of "Wireless Coverage Improvement", as we believed that the quantity of responses would be commensurate with the high degree of importance of coverage to public safety users.

We do not believe that in this case the lack of responses is indicative of lack of research in regards to the general topic of "wireless coverage", as evidenced by substantial advances made by commercial cellular systems in regards to self-optimization, maintenance of link budget and reduction of interference. Research within the commercial cellular community has indeed led to them using techniques often more advanced than typically deployed in public safety LMR radio systems. LTE is a good example of this, with its utilization of power control, adaptive spectrum utilization, adaptive modulations, MIMO, and other techniques for enhancement of both coverage and data throughput. In essence, LTE employs numerous techniques that arguably could be categorized as "cognitive".

Even though commercial cellular systems are not usually required to meet the more stringent coverage requirements and guarantees associated with public safety LMR, we feel that more research is needed in applying the commercial techniques used by systems such as LTE to public safety system LMR requirements. We recognize that the user community is justifiably not amenable to high risk in implementing new concepts until they are fully proven, so deployment of new coverage technologies must be done in small increments, using studies of the effectiveness and reliability of these techniques in deployed commercial cellular systems for partial proof of concept.

We can generally conclude that there is little ongoing research in the other four topic areas (Communicate Reconfiguration Information, Manage Communication Resources, Support Incident Command, Rollback Configuration Changes). In general, these topics areas are either unique to public safety (Support Incident Command) or at least unique to centrally managed

[11] *Realizing the Full Potential of Government-Held Spectrum to Spur Economic Growth,* Executive Office of the President, President's Council of Advisors on Science and Technology, July, 2012.

networks that are fundamental to public safety communications. Outside of public safety, we observe that the majority of research in cognitive radio tends to be applied to situations of spectrum sharing and/or opportunistic secondary spectrum use, rather than cognitive radio applications to resource management within a network. (We also recognize that research on resource management within a network can be accomplished by a single organization focused on proprietary technology that would not be reported or visible through our methodology. The adoption of LTE for broadband networks, for example, provides mechanisms for resource management, as described in more detail in Section 5.4.)

5.1 Interoperability

While significant progress has been made over the past decade, incompatible communications equipment for voice and data systems still impede the emergency responders' ability to interoperate. The fact that interoperability has been recognized as a critical issue for public safety for a number of years is reflected in the responses to the RFI, of which over half cited Interoperability as the area of research in SDR/CR technology.

- Interoperability technology enablers include the following:
  - Interoperability via common waveforms (everyone speaks the same language at the physical layer)
  - Interoperability gateways (a "translator")
  - Interoperability via standard interface definitions (commonality at higher levels in the stack)

There are several variations on each of the above, but interoperability research is generally based on one of these approaches.

5.1.1 Interoperability via Common Waveform

One method of achieving interoperability is to ensure that all radios that need to communicate over the air are using the same waveform—including the same frequencies, modes, modulations, protocols, and so on.

Much of the early work in Software Defined Radios was in response to the U.S. military's inventory of specialized radios that did not interoperate with other radios. "Specific deficiencies of current systems include … [radios that] operate on a single frequency band and employ a single waveform. They can inter-operate only with like radios, mandating multiple radios with different waveforms to support weapons platforms and command and control nodes."[12] As a consequence, the military incurred the expense of developing and maintaining a large number of different radios, and the physical challenge of fitting multiple radios into the constrained space of an aircraft or tank. The Joint Tactical Radio System (JTRS) program was initiated in response to these challenges, to develop a single radio system technology that would facilitate the ability for a single device to host multiple waveforms (increasing the circumstances in which two radios

[12] "Mission Needs Statement for the Joint Tactical Radio (JTR)," 21 August 1997.

had a common waveform), and for waveforms to be easily ported across different radio platforms, so that military radios with otherwise different requirements could operate the same waveform and therefore be interoperable. Extensive research and development resulted in the Software Communications Architecture (SCA), which provides a standardized interface between a waveform and the operating environment of the radio. As the JTRS program has matured and some SCA-based military radios have been fielded, research has turned to expanding the types of waveforms that can run with the SCA[13] and extension of the concepts to public safety applications.[14,15]

The SDR technology incorporated into the JTRS products is mature, has been fielded, and has been adopted to support other needs, beyond those defined via the JTRS program. The European Secure Software Radio (ESSOR) Programme[16] has leveraged SDR technology to achieve interoperability among the radios of six different participating states (PSs), also using the SCA as the key for porting a common waveform to multiple radios. A similar effort is underway involving nine different participating states to develop a waveform to pass secure voice, video, and data among coalition partners, called the Coalition Wideband Networking Waveform (COALWNW). Like the ESSOR program, the objective is to develop a common waveform that can be implemented on multiple hardware devices to achieve interoperability. Efforts are now underway to harmonize the ESSOR and COALWNW to achieve interoperability across both systems.[17]

In the U.S., there are defined standard waveforms (e.g., P25, LTE); however, there has never been a standard equivalent to the SCA defined for the interface between a waveform and the operating environment of the radio. Thus rather than a common, portable waveform, radio manufacturers have each integrated the waveform into their radio operating environment in their own way. The Wireless Innovation Forum has previously analyzed the advantages and disadvantages of an SCA, and concluded that introduction of an interface definition such as the SCA "between" the waveform and the operating environment of a radio was "a radical departure from the current development models of public safety radios."[18] The question at that time was whether the advantages of such an approach outweighed the disadvantages.

Recently two research initiatives have begun to implement PHY-layer characteristics within P25 protocols into a radio architecture based on the SCA. Researchers at the University of

---

[13] Turner & Dingman, "Developing SCA Based Wideband Networking Waveforms," *SDR '11 WInnComm,* Washington, DC, November, 2011.
[14] Christopher Rezendes, "Situational Awareness & Wireless in Military & Public Safety," *SDR '10 WInnComm,* Washington, DC, November, 2010.
[15] Zhongren Cao et al, "SCA-Compatible Public Safety P25-FM3TR-VoIP Bridge," *SDR '10 WInnComm,* Washington, DC, November, 2010.
[16] Margot, "The ESSOR Programme: Status and way to Standardisation," presentation at *SDR '11 WInnComm,* Washington, DC, November, 2011.
[17] Zammariello, C., and Lorelli, A., "Towards SDR standardisation for military applications," January 11, 2012, http://www.eda.europa.eu/News/12-01-11/Towards_SDR_standardisation_for_military_applications, (last visited May 15, 2012).
[18] *Software Defined Radio Technology for Public Safety,* Wireless Innovation Forum Report No. SDRF-06-A-0001-V0.0, 14 April 2006, available at www.wirelessinnovation.org.

California—San Diego (UCSD)[19] have demonstrated a Phase 1 P25 Common Air Interface waveform operating on a Universal Software Radio Peripheral (USRP) platform running the Linux operating system and OSSIE environment, which is an open-source SDR core framework based on the JTRS SCA. Researchers at the Communications Research Centre Canada (CRC) have demonstrated a P25 CAI waveform running on Android smart phones utilizing an SCA architecture[20]. These projects are both in the development stage and have progressed to prototype laboratory demonstrations.

The EULER project also investigated the application SCA-based architecture for public protection and disaster response (PPDR)[21]. EULER, a European Commission Seventh Framework Programme project, resulted in the definition of a system architecture and functional blocks (based on the SCA) designed specifically to facilitate interoperability among various European member states using various radio access techniques in PPDR activities. In addition, EULER also included development of a security framework that would support interoperability as well. As with the ESSOR program, the approach included development of an EULER waveform (EWF) that was then ported to various devices. The EWF provides a high-speed broadband radio access technique but also interfaces to legacy systems (e.g., TETRA, WiMAX, satcom).

While an SCA-based architecture has not been adopted by manufacturers supporting the public safety market, recent evolution of multiband land mobile radios represents an approach in which end-user devices (subscriber radios) support multiple public safety frequency bands using common "waveforms" promoting interoperability via the end user device. Multiband software defined radios have reached the market and provide another solution to interoperability by providing equipment that is not limited to operations on a single frequency band. These radios incorporate "flexible waveforms" by implementing multiple frequency bands(e.g., VHF, UHF, 700/800 MHz), allowing radios to interoperate with many more systems than single band radios. (Note that interoperability also required a common higher level protocol, such as P25—a multiband P25 radio would not be able to operate on a network that used a single other protocol, such as TETRA.) This technology is mature, and there are now multiple vendors who have fielded such radios.

One respondent to the RFI noted that while this technology is available today, some multiband radios are more expensive than single-band radios, and users require additional training (Additional licensing may also be required depending on spectrum use.)

---

[19] Cao, Z., Cuenco, J., Nwokafor, A., Johansson, P., Hodgkiss, "Development of Low-Cost Public Safety P25 Waveform in an OSSIE Environment with USRP," *SDR '11 WInnComm,* Washington, DC, November, 2011.
[20] CRC Announces SCA Applications Running on Android™, Communications Research Centre, http://www.crc.gc.ca/en/html/crc/home/mediazone/whatsnew/nov29-dec2_1, (last visited 1 May 2012).
[21] Baldini, G., Picchi, O., Luise, M., Sturman, T., Vergari, F., Moy, C., Bräysy, T., Dopico, R., "The EULER Project: Application of Software Defined Radio in Joint Security Operations," *IEEE Communications*, October, 2011.

5.1.2 Interoperability via Gateways

The second type of interoperability noted above is required when interoperability is required between incompatible devices/networks, e.g., where there is no common "waveform" on the devices used to communicate. Current technological solutions for providing voice interoperability through incompatible systems run the gamut from console audio patches to cross-band repeaters and network based IP-audio switches. Such solutions facilitate interoperability, but they typically require a layer of additional equipment external to the core communications systems. Gateway devices typically require the same transmission to be concurrently broadcast over multiple radio systems and frequencies within the same geographic area, thereby consuming additional system capacity and spectrum. Deployable repeaters and switches often require time to mobilize, and once deployed often require significant manual configuration and may require someone to physically connect land mobile radio devices compatible with each of the local LMR systems and/or enable device capabilities. As a result, in many cases additional time and manpower is required to configure and activate such capabilities. Even more advanced interconnect devices with a large number of modifiable parameters require expert operators to optimize performance, and even after initial setup, changes in the RF environment, the radios and networks being interconnected, and so on, can require retuning and/or resetting of a gateway.[22]

The DARPA Mobile Ad hoc Interoperability Networking GATEway (MAINGATE) program is an example of research into achieving interoperability via gateways. According to Raytheon, MAINGATE developer, the vehicular soldier radio system has 10 megabits capacity and is scalable to 128 nodes.[23]

As an alternative approach, Virginia Tech demonstrated software defined radio technology to create reconfigurable radios that can function as a handheld gateway, employing cognitive radio technology to discover key waveform parameters of public safety signals.[24] Funded by the National Institute of Justice and the National Science Foundation, this project addresses the (voice) interoperability problem by producing an affordable all-band all-mode software defined radio that can scan the public safety bands, identify target waveforms, and configure itself to operate in any authorized network selected by its operator (subject to standard operating procedures, command and control issues, etc.). With one click the operator can configure the radio to provide an audio gateway between two incompatible land mobile radios. Alternatively the radio can serve as a repeater for a public safety network.

5.1.3 The role of standards

The third approach to interoperability noted above is to achieve interoperability at higher levels of the communications protocol stack using standards. In each case a standard is defined for the interpretation of signals, control data, and/or data payload. Since both transmitter and receiver

---

[22] http://www.nij.gov/nij/topics/technology/communication/gateways.htm (last visited May 1, 2012).
[23] "Raytheon's vehicular soldier radio system links 37 different types of US, coalition radios," Press Release, July 11, 2012, available at http://raytheon.mediaroom.com/index.php?s=43&item=2133, last accessed March 12, 2013.
[24] Hasan, S.M., "Academic Research in Public Safety Communications," *Public Safety Communications Workshop, SDR' 10 WInnComm,* Washington, DC, November 2010.

are interpreting the signals and data in the same manner, the control data, and air interface, of these systems are interoperable at multiple levels. (Note that interoperability can be achieved at one level but not another level. For example, video data can be successfully transmitted through an LTE network, but if the application level of a transmitter is using H.264 data compression protocol and the receiver is expecting VC-2 protocol, the end-to-end path will not be interoperable at the application level. Similarly, because difference frequencies are used, a P25 VHF radio is not interoperable (over the air) with a P25 UHF radio even though they both use the same protocols defined by the P25 common air interface standards. .

Standards in public safety communications have a significant role in enhancing interoperability. P25 and TETRA standards facilitate interoperability between different vendors' land mobile radio equipment and systems, and LTE has been selected by both U.S.[25] and Canadian public safety for future wireless broadband data networks in large part to have a standard interface in place to ensure interoperability among public safety network users. LTE offers a number of capabilities that will benefit public safety, including some that can be enhanced with cognitive radio technology as described in sections below. Where standards are in place, fully adopted and deployed, interoperability can be achieved without cognitive radio technology. However, the reality is that "fully adopted and deployed" is rarely achieved in practice. P25 radios are generally more expensive[26], so that there remain a significant number of non-P25 land mobile radio systems in the United States. The proposed U.S. National Public Safety Broadband Network (NPSBN) may never be fully built out, particularly in some rural areas. Even among cellular carriers, there is an open debate (and FCC proceeding[27]) on whether interoperability among carriers utilizing 700 MHz frequencies should be mandated. Even though LTE is based on 3GPP standards, deployment decisions of features defined by those standards are not mandatory, so they are based on network operator choice. Standards also continuously evolve, and while typically backwards compatible they are not guaranteed to be. Existing interoperability may be compromised, therefore, when one entity deploys an updated version of a standard. Thus, even when standards are generally in place, the cognitive radio capabilities discussed above in Sections 3.1, 3.2, and 3.3 will be useful from a technical perspective in achieving end to end interoperability.[28]

As a final thought on standards for interoperability, a respondent to the RFI drew an interesting comparison between interoperability and the development of standards for email exchange.

"What you are seeing was paralleled by product developments with electronic mail about two decades ago. Several non-interoperable implementations entered the market. To get e-mail interoperability we saw:

[25] FCC 11-6, January 25, 2011, Third Report & Order and Fourth Notice of Proposed Rule Making, in the Matter of Implementing a Nationwide, Broadband, Interoperable Public Safety Network in the 700 MHz Band.
[26] "The hope and reality of Project 25," *Urgent Communications*, May 1, 2007.
[27] FCC 12-31, March 21, 2012, Notice of Proposed Rule Making in the Matter of Promoting Interoperability in the 700 MHz.
[28] The extent of cognitive radio technology deployment is such cases will depend on the business case and the cost-benefit tradeoffs of using the technology to address the situations in which the standards are not fully adopted and deployed.

1) Bilateral translators (such as you are describing). The problem is a familiar 'n^2' one -- the number of pair-wise patches increases proportional to the square of the number of e-mail systems.

2) Esperanto. Everything translates (just once) to a commonly agreed upon. The problem here was that the formal standards exercise picked the wrong one (CCITT X.400) while the commercial world got SMTP/S/MIME right.

3) As Esperanto took hold, most e-mail implementations either left the marketplace or became 'native Esperanto'

In the world of e-mail applications, the Esperanto is SMTP/S/MIME; in the world of voice applications, it is VOIP."

5.1.4 Other Interoperability Issues

While significant progress has been made over the past ten years on interoperability, including technology solutions, there are still some open research questions:

- Innovations for enhanced data interoperability (e.g., interoperability among disparate mix of broadband through low speed data systems);
- Interoperability between new and legacy capabilities (e.g., voice interoperability with broadband network);
- Innovations that standardize procedures to facilitate the ability of two radios to establish a communications link when no link has been pre-defined (a "meeting point");
- Creation of a "Virtual System" from multiple disparate system;
- Exchange of data from NextGen 9-1-1 systems;
- Interoperability with non-first responders;
- Preserving integrity/security of public safety communications in interoperability scenarios;
- LTE direct mode in the absence of infrastructure;
- Native one-to-many capability (e.g., dispatch) capability within LTE (i.e., LTE native, not via over the top, or OTT applications).
- Hybrid terminal (commercial / public safety LTE); and
- Interoperability of machine-to-machine communication.

5.2 Coverage and Performance Improvement Techniques

As stated previously, we received only two responses to the topic of Coverage, and neither identified research into coverage technologies. Therefore, this section discusses data gleaned from additional research by the SIG into coverage technologies for augmenting the little information that we received.

Adaptive beamforming has been used in radar systems for over 30 years for achieving agile antenna patterns that direct high gain to desired areas and minimize gain toward interference sources. However, there were no responders to the RFI to discuss adaptive beamforming for public safety. A major complication for using adaptive *transmit* beamforming in public safety base station transmit antennas is the fact that most communications, being group calls, are transmitting to several receivers simultaneously, requiring complicated transmit beamforming using several degrees of freedom, as well as knowledge of the angular position of all terminal receivers relative to the transmit antenna. Terminals transmitting to the base station are typically one at a time per frequency, even for group calls. Today's processing devices (FPGAs, DSPs, GP computers, etc.) are fast enough to rapidly adapt to the direction of arrival of the signal to increase *Grs* for that particular terminal-frequency pair.

"Multiple In Multiple Out" (MIMO) techniques are used extensively for cellular systems, but there was no response to the RFI for this topic applied to LMR systems. Public safety's new LTE broadband systems in Band 14 of the 700 MHz band use MIMO, typically employing 2 X 2 polarization diversity (2 TX polarizations, 2 RX polarizations) on its downlink from its ENodeB transmitter to its UE handheld or mobile terminals. Several companies have announced advances in MIMO antennas, particularly tunable multiband antennas for LTE devices, including SkyCross and Antenova. Other techniques such as adaptive polarization techniques are being developed to improve performance by mitigating interference.[29]

Source coding techniques use error correction and/or interleaving to mitigate errors introduced in the channel by noise, interference, fading, and other factors. In essence, these techniques increase the communication range by reducing the signal to noise ratio that is required to achieve a given quality of service (e.g., voice quality for digital voice communications) of the communication. Although public safety waveforms such as P25 and legacy manufacturers' waveforms such as EDACS Provoice use source coding, there were no RFI responses that relate to source coding,

A classic coverage problem in public safety is the so-called "near-far problem". An example would be where a radio that is transmitting at full power in close proximity to a radio receiver causes sufficient interference to the receiver so that it cannot communicate with a radio with a weak signal on another channel. This situation can be alleviated if the interfering radio does not use full power when it doesn't need to, i.e., controls its power to be the minimum necessary to achieve a desired quality of service. Such is common for cellular radio communications, including LTE broadband, but this technique was not mentioned in any RFI response.

MANET network extension would allow transmissions to be passed back and forth from the incident site through a network of individual responder radios operating in peer-to-peer mode

[29] For example, Eigen Wireless has developed smart antenna technology based on adaptive polarization (personal communication). See United States Patent no. 8,203,500 for a "Compact Circularly Polarized Omni-Directional Antenna", and Patent Application 20120329416 for An Adaptive Polarization Array (APA) Algorithm for adjusting the polarization orientation of antennas, such as Dual-polarized array antennas. The APA Algorithm searches to find a polarization state that maximizes a signal quality of a received signal in the presence of interfering signals and noise. The search facilitates adjustment of a polarization state of, for example, receive antennas to maximize a signal quality metric. A proxy metric having no local maxima other than the global maximum is used to search the polarization search domain to find a best polarization state.

effectively extending coverage of the main radio system/network. This concept for coverage extension was also noted in a report on desirable propertied of a national public safety network, published by the Visiting Committee on Advanced Technology (VCAT) of the National Institute of Standards and Technology[30]. Key research issues include impact on power use, throughput issues, and the extent to which current MANET routing algorithms accommodate public safety communications patterns.

As another means for enhancing coverage, access to non-traditional network resources may be a viable option for public safety. For example, additional data bandwidth may be operationally required even in areas where voice coverage and capacity meet user requirements. Broadband services provided via TV whitespace spectrum, or access to commercial services via cellular provider data facilities may be exploited as supplemental, or fallback, resources. For example, commercial coverage might be available in a tunnel where specific public safety systems are not. Access to supplemental resources would require appropriate wireless communications equipment in vehicles, and appropriate policies must be formulated and implemented, defining when such links could be activated.

While most of this report addresses technology development, we also note that some coverage issues can be mitigated through non-technology approaches. For example, addressing in-building and degraded area coverage has become almost a normality during the specification phase of a potential system deployment for Public Safety. Jurisdictions across the country have already forged forward with partnerships in the building construction and standards community by getting in-building codes submitted and approved at local levels. The traction of "in-building" ordinances and resolutions approved at the governance level have been extremely popular and entities such as fire departments that rely on critical fireground communications on these networks in-building have supported it wholeheartedly and even have performed several tests in accordance with the building owners to meet or exceed the required coverage parameters.

5.3 Spectrum Utilization Optimization and Dynamic Spectrum Access

The overall research area of spectrum utilization and dynamic spectrum access was identified by a number of survey respondents, more respondents than any other area except interoperability. While this may in part be due to the breadth of the topic area, we also note that this is a very active research area in general. Conferences such as the IEEE Dynamic Spectrum Access Networks (DySPAN) have a primary focus in this area. Many of the proposed innovations being investigated by the research community are independent of a specific domain (such as public safety).

Research topics include techniques to utilize TV White Space (TVWS), share spectrum with incumbent users such as the military, and operations as licensed or unlicensed secondary users. For public safety, where spectrum is allocated on a generally exclusive basis, technology developments in this area may seem to be relevant; however, the ability to meet the surge

[30] *Desirable Properties of a National Public Safety Network,"* Report and Recommendations of the Visiting Committee on Advanced Technology of the National Institute of Standards and Technology, 21 November 2011., available at http://www.nist.gov/director/vcat/upload/vcat-public-safety-subcommitte.pdf, last accessed 26 November 2012.

capacity requirements associated with major incidents may require the ability to identify and access spectrum outside allocated frequencies (e.g., TVWS) or access other spectrum under some pre-defined agreement. Thus some aspects of this work, in support of the use cases described in Section 4.3, are relevant research.

Carriers are already implementing one form of this technology in offloading traffic to WiFi systems, so there is significant baseline capability in this accessing additional spectrum outside allocated frequencies. Reliably deploying systems that exploit unlicensed spectrum, in which current FCC rules say all deployed devices, to include public safety devices, cannot create interference, while accepting all interference, is a major operational challenge; particularly since this operating mode is embedded into the firmware of hundreds of millions of FCC authorized consumer grade wireless broadband devices, in addition to a plethora of non-wireless broadband wireless technologies. Accessing non-public safety deployed wireless systems operating in the unlicensed bands is another challenge.

InterDigital announced the rollout of a suite of technologies at the 2013 Mobile World Congress that leverage cognitive radio technologies to address a number of the desired capabilities listed in Section 4.3. According to the InterDigital website, their Dynamic Spectrum Management™ product set includes capabilities to:

- Allocation and aggregation of contiguous and non-contiguous licensed, unlicensed, and TVWS frequency channels;
- Policy-based channel management on infrastructure or terminal;
- Channel selection assisted by database access; and
- Channel quality sensing;[31]

At the time this report was authored, open FCC proceedings were underway, through which they were requesting comments on, among other topics, the use of cognitive radio technology to enhance spectrum sharing in unlicensed or lightly licensed spectrum. The results of these proceedings could influence the perception of unlicensed technology reliability by public safety, through mandated use of priority of access mechanisms, defined classes of users. This change may facilitate broader public safety acceptance/use of additional unlicensed or lightly licensed spectrum. Expansion of the 5GHz unlicensed band (in Notice of Proposed Rulemaking FCC 13-22), if successful, will create a regulatory framework that changes the use of sharing unlicensed spectrum significantly; one in which multiple cognitive techniques, and a priority of use regime may be established. In addition, the Notice of Proposed Rulemaking and Order (FCC 12-148) on the 3.5 GHz band lays out concepts that could give government and public safety priority access for small cell use in specific locations.

[31] A full set of capabilities and business partners is included in a Press Release entitled, "Intelligent Harvesting of TV Whitespace and Other Underutilized Spectrum Provides a Forward-thinking Solution to the Impending Bandwidth Crunch," 26 February 2013, available at: http://ir.interdigital.com/common/mobile/iphone/releasedetail.cfm?ReleaseID=651535&CompanyID=IDCC&mobileid=, last accessed 1 March 2013.

Geolocation databases are currently being developed as one approach to implementing Dynamic Spectrum Access capabilities. This approach to DSA works particularly where spectrum is licensed to fixed transmitters, and devices can determine what spectrum is potential available by checking a database that identifies available spectrum for a given location. This is the principle on which TV White Space spectrum utilization is being deployed in the United States. A near-term opportunity for public safety is to exploit TV White Spaces in situations when additional spectrum is needed for adequate incident response. InterDigital, for example, also demonstrated LTE over TVWS capabilities at the 2012 IEEE DySPAN conference.

A significant amount of research has been in spectrum sensing, to allow opportunistic secondary spectrum users to identify potential used spectrum; however, there are a number of challenges to bringing this technology to commercial viability. Given the real-time critical nature of public safety communications and the need for highly controlled communication, this approach may only be applicable in some specific public safety scenarios. One such scenario was briefed to the FCC in September, 2012, in which cognitive radio technology including spectrum sensing was demonstrated as a potential solution as part of a Deployable Aerial Communications Architecture.[32]

5.4 Communicate Reconfiguration Information

In our original analysis of Use Cases, it was apparent that communicating reconfiguration information among the nodes in a network was a key capability to exploit the flexibility of SDRs and the adaptability of cognitive radios in a public safety network. However, in our analysis of ongoing research activity, it appears that there is little ongoing research on this topic as an independent activity. Instead, much of the ongoing activity is in conjunction with standards and specific broader capabilities. Evolving LTE standards include the specifications for communicating information as needed to implement network functionality. Also, the IEEE P1900.4.1 project is developing a "Standard for Interfaces and Protocols Enabling Distributed Decision Making for Optimized Radio Resource Usage in Heterogeneous Wireless Networks". While this research is not specific to public safety networks, we anticipate that results will be incorporated into networks that support public safety communications.

5.5 Manage Communications Resources

Real-time management of network resources is critical, particularly when specific situations in which incident communications requirements exceed system capacity, creating a need for more effective network resource management tools than those that are commonly available today. One area of research is focused on dynamic allocation of bandwidth, typically among secondary users; this research could be relevant in public safety networks in which both primary and secondary users are public safety users, but primary users are transmitting mission critical information. Different approaches are currently being developed based on techniques such as,

[32] xMax for Public Safety, Homeland Security and DACA Applications, presentation to the FCC, included in *ex parte* filing, 1 October 2012, accessible at http://apps.fcc.gov/ecfs/document/view;jsessionid=YPhpQrnNhTynMfDvZyj8LLSLHFSYV3J3T45VHQKHzY0gDLvypnF3!-224088840!NONE?id=7022026210, last accessed 24 February 2013.

but not limited to, cooperative learning,[33] approaches based on grade of service for heterogeneous traffic,[34] and opportunistic traffic scheduling.[35] These approaches all focus on leveraging information about the nature of data to be transmitted, the required quality of grade of service, to allocated communications resources to optimize some objective (such as throughput). This research could provide a baseline for sophisticated tools for public safety, although some additional adaptation may be required. For example, research that focuses on optimization metric of throughput may not be as useful to public safety as an algorithm that balances criticality, timeliness, and bandwidth to optimize network performance against mission or incident requirements rather than simply throughput.

Much of the research in this area is still in the early algorithm development stage, and will require further development, test, and evaluation before adaption to public safety specific applications will be possible.

We also recognize that there is ongoing internal research by commercial carriers that addresses this area as well, particularly in the deployment of LTE systems.[36] For example, Alcatel-Lucent has filed relevant patents for capabilities that can be leveraged for resource management. The first, US20110305137A1, Admission Control for a Shared LTE Network defines a method to facilitate access priority, and call preemption, for UE network access at an eNodeB. Note that according to the application text, this process falls outside the 3GPP standards. This application specifically addresses public safety versus consumer access and associated call pre-emption. The second application US20110305240A1, Call Admission Preemption for Multiple Bit-Rate Applications, was referred to in the body of the access control application. This application covers call admission control for multiple bit-rate applications (e.g., a streaming video with multiple specified bit rates) through the EPC, and allowing the call on a congested network at one of the specified rates and enabling the system to control it (e.g., roll these rates back) or simply preempt lower priority calls to accommodate higher priority calls.

Incremental releases of 3GPP Long Term Evolution, or LTE (including LTE-Advanced, or LTE-A), include features that can be considered “cognitive” in nature. LTE, as a 3G technology, or LTE-A as a 4G technology are very complex. These technologies, along with 3GPP sister technologies like HSPA+ are quickly becoming the dominant commercial service platform for delivery of wireless data and multimedia services worldwide, and in the next year or two, will become a dominant platform for cellular telephony, displacing previous generations of circuit-switched technology currently used by commercial carriers.

LTE technology, in the context of the commercial world, is primarily focused on making available network assets (spectrum, radio access infrastructure, network core infrastructure) and

---

[33] Di Felice, M., Chowdhury, K., and L. Bononi, “Learning with the Bandit: A Cooperative Spectrum Selection Scheme for Cognitive Radio Networks,” IEEE GLOBECOM 2011, December 2011.

[34] Yu, L., Jiang, T., Guo, P., Qu, D., and P. Gao, “Improving Achievable Traffic Load of Secondary Users Under GoS Constraints in Cognitive Wireless Networks,” IEEE GLOBECOM 2011, December 2011.

[35] Paul, U., Buddhikot, M., and S. Das, “Opportunistic Traffic Scheduling in Cellular Data Networks,” 2012 IEEE International Symposium on Dynamic Spectrum Access Networks, October, 2012.

[36] An excellent overview of LTE for public safety can be found in the following article:
Doumi, T., M. M. Dolan, S. Tatesh, A. Casati, G. Tsirtsis, K. Anchan, and D. Flore, “LTE for Public Networks,” *IEEE Communications*, Vol. 51, No. 2, February 2013, pp. 90-95.

end user equipment more efficient and more cost effective, and therefore more profitable. The environment in which commercial networks based on 3GPP standards currently operate is conducive to development of cognitive technologies that make the network operators more effective "within their specific pre-defined spectrum environment". Unlike many other systems, commercial cellular networks generally operate in an interference limited environment walled in by specific spectrum allocations. Commercial network operators are embracing technologies like carrier aggregation and offload functionality (e.g., Wi-Fi) but these are geared towards optimization and use of well-defined network components; not by using opportunistic technologies exploiting randomly available spectrum resources acquired via dynamic spectrum access technology. Nevertheless, there are many aspects of current commercial networks that can be considered to be "cognitive" in nature, enabling the network to self-optimize, and interact with end user equipment to learn about its operating environment.

The ongoing evolution of LTE technology is significant to the public safety community, particularly in the U.S., because this technology has been mandated as the core transport technology for a National Public Safety Broadband Network (NPSBN) that will be deployed over the next few years. Cognitive features within 3GPP standards may be especially significant for the public safety users. For example when, and where, temporary tactical networks are deployed to support short-term incident operations or to ensure RAN access priority and heightened QOS through a shared network backbone.

The list below describes certain LTE/LTE-A features in a generic sense as described by 3GPP. This is a living list, and not intended to be exhaustive. The functional details of these features are out of scope for this document, but details can be found in publicly available 3GPP standards. Some of the items noted are on the 3GPP development roadmap for LTE Advanced. Another point should be made: The 3GPP standards upon which these networks are built provide a foundation. These standards, like many other standards describe functionality at architecture reference points and describe desired functionality. How network technology manufacturers implement these functions (i.e., within the undefined architectural areas between standard interface/reference points) is based on individual manufacturer and network operator choice; this is where equipment vendor and network competition takes place. It's where the "secret-sauce" resides. Utilization of specific features and implementation choices within specific carrier network architectures remain a network operator choice, perhaps the cognitive mechanisms noted below may not be realized of as universal features in LTE networks. Some of the features described will also require evolutional changes in future generations of end-user equipment.

- Base Station Self-Configuration
- Automatic Neighbor Relation (ANR)
- Load Balancing
- Mobility Robustness / Handover
- RACH (Random Access Channel) Optimization
- Inter Cell Interference Coordination
- Energy Savings

- Cell Outage Detection And Compensation
- Modification Of Antenna Tilts
- Minimization Of Drive Tests
- SON Interactions With Distributed Antenna Systems
- SON With Picos/Femtos/Relays
- SON With Picos/Femtos/Relays

The main areas of interest within 3GPP standards specifically applicable to LTE, and cognitive in nature, fall within the category of "Self Optimizing Networks" or SON[37]. There are a number of SON items within the 3GPP standards starting with 3GPP LTE Release 8, becoming increasingly more comprehensive in subsequent LTE releases 9 to 11. Further, the 3GPP development roadmap, including future Release 12 and beyond, becomes increasingly more cognitive in nature as network operations become more and more automated from plug & play deployment.

5.6 Support Incident Command

In both the responses to the survey and in our literature searches we found very little research that specifically looks to adapt communications capabilities to the requirements of an evolving incident. We attribute this to the limited market for public safety specific incident command support tools, and that the research community has little or no understanding of incident command. We consider this a significant research gap, as the vision outlined in Section 4.6 will not be achieved without investment in this area.

5.7 Rollback Configuration Changes

The concept of rolling back configuration changes was not identified by any respondents to the survey. Over-the-air reprovisioning is currently a feature of commercial cellular systems, and likely will be adopted by public safety broadband data systems. Thus the need for this capability is truly unique to public safety LMR radio systems. Since this is not an issue for commercial systems, there is little outside research that can be leveraged for public safety. However, there is ongoing research in over-the-air reprogramming via broadband networks specifically targeted for public safety LMR that is reaching maturity. Thus we conclude that from a research perspective, additional research on technology for the basic functional capability is not needed. We do note that the focus of further developments in this area should be on standardization of the reprogramming process across public safety manufacturers and equipment. As a final note, research providing real-time feedback on the impact of any configuration changes, addressed as a subset of the tools for managing communications resources, would be useful in ensuring that configuration changes generate the desired results.

[37] •4G Americas, *Self-Optimizing Networks: the Benefits of SON in LTE*, July 2011, available at http://www.4gamericas.org/documents/Self-Optimizing%20Networks-Benefits%20of%20SON%20in%20LTE-July%202011.pdf, last accessed on December 3, 2012.

6 Conclusions and Recommendations

Cognitive radio technology has been identified as having potential to provide important improvements for public safety communications networks, including enhanced interoperability, coverage improvement, interference mitigation, dynamic spectrum access, more effective management of communications resources, and the ability to configure to meet incident command requirements. There is ongoing research in many of these areas, but additional work will be required to adapt ongoing technology development to meet specific public safety requirements.

One notable area in which current research is inadequate is the ability to configure communications capabilities to meet evolving incident command requirements, a requirement is unique to public safety. Particularly in the case of large-scale events involving many days and multiple jurisdictions, more effort is needed to most effectively utilize advanced communications technologies.

Incident command is the process of providing commanders with tools to organize on-site resources, communicate with them effectively, and have access to on-site and off-site data relevant to the incident. Automated acquisition and analysis of a wide variety of data sources can provide the command structure with information to improve their decision-making process and improve the efficiency with which decisions are disseminated to through the incident command hierarchy.

We have identified a number of areas of ongoing research, and noted gaps that need attention. Technologies new to public safety, including broadband networks and big data offer exciting opportunities. As always with the public safety community, there is a challenge in getting new developments into the hands of first responders. We trust this report is helpful in meeting that challenge.

Appendix 1 Additional Information on the Wireless Innovation Forum and Public Safety Special Interest Group

The Wireless Innovation Forum™ is a non-profit "mutual benefit corporation" dedicated driving technology innovation in commercial, civil, and defense communications around the world. Forum members bring a broad base of experience in Software Defined Radio (SDR), Cognitive Radio(CR) and Dynamic Spectrum Access (DSA) technologies in diverse markets and at all levels of the wireless value chain to address emerging wireless communications requirements through enhanced value, reduced total life cost of ownership, and accelerated deployment of standardized families of products, technologies, and services. The PS SIG is an organization within the Wireless Innovation Forum that provides a focus for activities in which the public safety community has an interest. Goals of the PS SIG are to interface with both communications users and commercial vendors associated with the public safety community with a goal of increasing awareness of SDR related issues, publicize activities of the Forum that address those issues, and increase participation by the public safety community in Forum activities. The PS SIG also interacts with other forum committees and working groups to ensure that the public safety community's inputs are addressed in other publications and initiatives undertaken by the Forum.

The public safety community, as defined by the PS SIG, includes all first responders (e.g., emergency medical services, fire services, police/law enforcement. It also includes secondary responders (e.g., civil government, emergency management, environment health personnel, civil protection/homeland security/homeland defense units, search and rescue units, hospitals, relief organizations, public utilities, transportation), and other elements of the criminal justice system.

Appendix 2 Key Concepts/Issues for Public Safety Communications

One of the most important fundamental requirements associated with public safety communication needs is the ability for first responders to communicate as needed, regardless of technological differences in communications equipment (e.g., different frequency bands, different protocols, different modes, manufacturer specific capabilities, different versions of hardware and software). Most of the effort in recent years has been focused on enabling "mission-critical" voice communications. There are still open challenges related to achieving ubiquitous voice interoperability, although concerted efforts in development of technology, governance, standards, have led to vast improvements. Gateway devices and multiprotocol land mobile radios are common and multiband radios are beginning to penetrate the market. However, even today many current interoperability approaches do not utilize spectrum in the most efficient manner.

As significant progress is being made to address the challenges associated with interoperability, public technological advances that drive commercial thirst for spectrum also provide the foundation for public safety applications that also require increasing access to spectrum. These applications provide a wealth of information to public safety users such as the ability to download security video to a police car, devices that monitor firefighter biometrics and equipment safety and are turning attention to other equally challenging issues. Spectrum availability is an issue for all wireless systems, including those for the public safety community in that spectrum resources currently allocated to public safety users are limited. Mission critical information such as status and real-time access to hazardous material information is resulting in increasing data transfer through wired and wireless networks in addition to voice traffic. The resulting information volume has the potential to overwhelm communication network resources and capabilities as well as the ability of responders to process information.

In response to the continuing growth in data volume, U.S. public safety user groups have endorsed LTE as the protocol of choice for 700 MHz broadband data (as a national option) and the FCC has identified this technology as a requirement for use in 700Mz public safety broadband spectrum.

An increasing reliance on resources and capabilities enabled through wireless broadband data technology has created new interoperability challenges associated with:

- multiple networks and wireless data networking technologies;
- multiple frequency bands;
- multiple protocols and varying protocol implementations;
- constantly evolving wireless technology standards
- multiple encryption approaches
- increased complexity of data
- migration of voice services onto data networks.

Current proposals for a national broadband network in the 700 MHz frequency band present a significant opportunity for public safety to have a dedicated network built from the ground up following standard protocols. However, we strongly believe that there is a significant role for evolving cognitive radio technology. Spectrum efficiency will continue to be a critical aspect of a nationwide network. Efficient management of resources will be critical, as will exploitation of additional spectrum when requirements surpass existing resources (e.g., leveraging 700MHz, 4.9 GHz, unlicensed, and white space spectrum in a major emergency). Other issues will include graceful upgrade of product software, graceful migration to evolving technologies, logistics associated with provisioning and support, leveraging commercial hardware and software development, improved efforts while addressing unique public safety needs, maintaining ease of use, and reducing life cycle costs. Maintaining robust and reliable communications in the face of intentional or ambient interference will continue to be an issue. Costs, extended lifecycle timeframes and affordability have traditionally been limiting factors limiting the extent to which the public safety community has been able to refresh and deploy new technologies.

Future public safety communications platforms will likely be implemented as a system of systems reliant upon on a variety of networks. They will involve emerging network technologies, standards, protocols, and frequency bands, and differing implementation choices made by network operators in support of local user needs. These networks must support services ranging from short-range communication capabilities such as those provided by personal area networks, to long haul communication at a national or international level. We believe software defined and cognitive radio technologies can provide capabilities that exploit all available communications resources to facilitate interoperability and support seamless “virtual” communications capabilities to public safety users.

Appendix 3 Related Efforts

The there are several, concurrent, ongoing commercial and government efforts focused on addressing the needs of public safety personnel and agencies. This RFI effort, undertaken by the Public Safety Special Interest Group, is intended to build upon, and complement, these efforts.

The following list is not exhaustive, and focuses on government initiatives that also address the overall issue of leveraging evolving technology for public safety. Technology research activities are not included in this list, but rather are the types of information that we are soliciting through this RFI.

The National Institute of Justice (NIJ): NIJ conducts research and development on technologies for state, local, and tribal law enforcement and criminal justice needs. NIJ's communications portfolio includes research, development, test, and evaluation activities that include development of cognitive radio technologies developed in response to identified public safety needs. NIJ is currently funding research into a number of software defined and cognitive radio topics, such as:

- Automated discovery of public safety networks
- Reconfigurable radios
- Intelligent, handheld land mobile radio network bridging
- Steerable directional antennas
- Smart power management
- Network switching to avoid disruption
- Channel/path bonding

The Department of Commerce: The Department of Commerce Public Safety Communications Research (PSCR) program acts as an objective technical advisor and laboratory to DHS/OIC and the response community to accelerate the adoption and implementation of only the most critical public safety communication standards and technologies. PSCR examines public Safety Requirements, Specifications/Standards, Test and Evaluation, and records Lessons Learned. PSCR support includes technology research in support of the following:

- Radio over Wireless Broadband,
- Project 25 support (i.e., P25 compliance assessment, P25 standards development, P25 Security, P25 ISSI),
- Public Safety Voice over IP and
- Research in support of public safety Audio and video quality.

The Public Safety Communications Research (PSCR) program is deeply involved in the rapidly progressing topic of Public Safety 700 MHz Broadband (e.g., Public Safety LTE test and demonstration network as well as LTE PS standards support). To help move forward broadband technology for public safety communications, PSCR is building a national public safety broadband demonstration network and providing technical advocacy for the public safety community through requirements gathering and standards development. More details can be found at www.PSCR.gov.

The Department of Homeland Security (DHS) SAFECOM is a public safety-driven communications program, managed by the Office of Emergency Communications and the Office for Interoperability and Compatibility (OIC) of the U.S. Department of Homeland Security. SAFECOM works to build partnerships between all levels of government, linking the strategic planning and implementation needs of the emergency response community with Federal, State, local, and tribal governments to improve emergency response through more effective and efficient interoperable wireless communications. Under the SAFECOM program, public safety communications Statement of Requirements and Architecture Framework documents have been published. More details can be found at http://www.safecomprogram.gov/SAFECOM/.

The National science Foundation (NSF) is sponsoring a research & development program entitled Enhancing Access to the Radio Spectrum (EARS). The EARS program "… targets innovative and potentially transformational research that carefully considers the interplay of science, engineering, technology, applications, economics, social sciences, and public policy on spectrum efficiency and access."[38]

The European Telecommunications Standards Institute (ETSI): The ETSI Technical Committee on Reconfigurable Radio Systems (RRS) has a Working Group specifically focusing on the application of software defined radio and cognitive radio technology to public safety.

The Federal Communications Commission (FCC) is addressing regulatory aspects of DSA technology (including proceedings that are asking specific questions regarding the regulatory considerations of deploying DSA in public safety communications.

This RFI effort undertaken by the Public Safety Special Interest Group is intended to build upon, and complement, these efforts.

[38] http://www.nsf.gov/funding/pgm_summ.jsp?pims_id=503480, accessed 28 February 2011.