NIST Public Safety Broadband Radio Network

In response to National Institute of Standards and Technology Docket No.: 110727437-1433-01
Soliciting Input on Research and Development for Desirable Features of a Nationwide Public Safety Broadband Network

Joseph Gaeddert (jgaedder@vt.edu),
Jeffrey H. Reed (reedjh@vt.edu),
Bob McGwier (rwmcgwi@vt.edu),
Tamal Bose (bose.vt@gmail.com),
Charles Clancy (tcc@vt.edu),
Haris I. Volos (hvolos@vt.edu)

Wireless@Virginia Tech
Bradley Department of Electrical and Computer Engineering, Virginia Tech
432 Durham Hall, MS 0350, Blacksburg, VA 24061, USA

October 12, 2011

1 Introduction

Interoperable emergency radio communications is integral for the success of first response, public health, and national security communities. The need to effectively undertake action in the field has been emphasized by a series of events caused by terrorists and by natural disasters. Disparate protocols and varying frequency bands between public safety agencies make interoperability difficult in disaster situations. Furthermore the resiliency of radio communications is imperative in catastrophic events where mission-critical infrastructure is disabled, damaged, destroyed, or otherwise non-existent. In particular maintaining secure and reliable communications links is a crucial factor in preserving mission integrity to both disaster prevention and initial reaction. In these environments governments are strained to take necessary actions to protect citizens, critical infrastructures, and information. Consequently the ability of a public safety network to maintain resiliency even when infrastructure is unavailable is crucial. The particular limitations of modern radios in adaptive environments have been exposed by first response teams unable to communicate in heterogeneous wireless networks [1]. Accordingly the public safety office has proposed the migration to commercial LTE infrastructure and 4G technologies in order to leverage inexpensive hardware and existing networks [2, 3]. However the reliance of such systems on infrastructure is a critical weakness during disasters when outages occur.

In such scenarios networks will require reconfigurable wireless communications implementations which can intelligently adapt to unforeseen scenarios. This includes spectrum coexistence (e.g. with radar), ad-hoc network deployment, self-organizing ad-hoc networking, security countermeasures in cyber attacks, and adaptive radio link optimization. These capabilities are enabled by software-defined and cognitive radios which can augment existing commercial handsets to complement protocol support and enhance the resilience of radio communications links. Furthermore if a security threat of a particular waveform is detected (such as a breach of security in encryption or even a physical layer vulnerability) the waveform can be immediately upgraded in the field with a software download. These upgrades can only be supported on a reconfigurable platform, and can be accomplished autonomously and completely transparently from the user. This provides a significant advantage to first response teams who rely on communications equipment to provide a high quality of service even when valuable infrastructure has been compromised. Finally these systems must be validated through deployment in a wide-area testbed to gain insight into how real-world environments, unforeseeable factors, and dynamic spectrum access technologies stress the system.

2 Software-Defined Radio Handsets

With this growing demand for wireless connectivity comes the need to adapt to quickly-changing standards. Software-defined radio (SDR) is heralded in the wireless engineering community as the future of standards implementation as radio hardware can be "future-proofed" by permitting on-the-fly reconfiguration. Defining the radio's physical and network layers in software provides a powerful tool for enhancing the functionality of the communications layer at a reduced cost. This technology can support compatibility with commercial infrastructure, including numerous protocols such as P25, FM voice, GSM [4], and numerous cellular standards. Furthermore, software-defined transceivers can add support for emerging standards to augment existing infrastructure. This re-

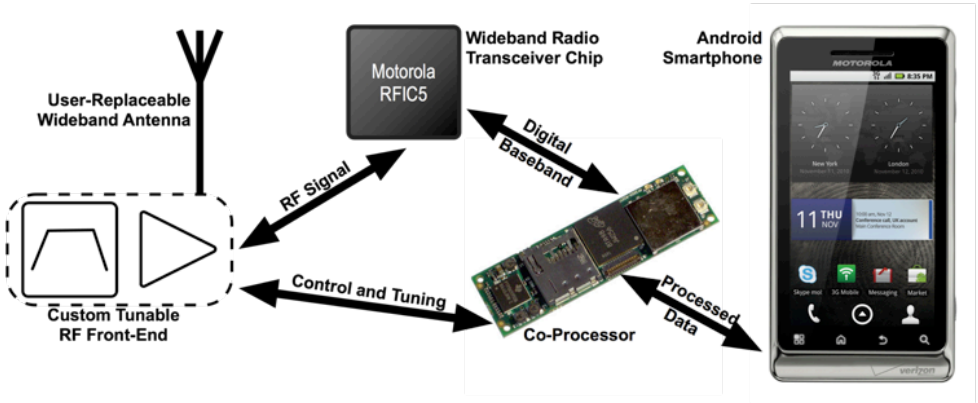

Figure 1: Block diagram of Virginia Tech Wideband Mobile Radio.

duces the time between first responders in the field giving feedback and when they see the changes actually made; there is no need to re-design the hardware, just a software download. This methodology permits incremental changes to be made to the communications platform, as components can be easily upgraded as new technologies are rolled out. For example, voice quality won't suffer as a result of locking the transceiver into old audio codecs with poor quality [5]. Additionally, the recent push for free and open-source SDR software [6, 7] has paved the way for a significant cost reductions in development platforms. Furthermore the rapid prototyping capabilities of such software platforms permits a significant reduction in testing and grants developers to identify and isolate key trouble areas in emerging standards.

Currently the nation's public safety groups have agreed to move forward and use LTE in the 700 MHz band to deliver mobile broadband applications to first responders [2, 3]. The high capacity, low latency, and inexpensive commercially available handsets makes LTE an attractive solution and an improvement in land-mobile public safety communications. However LTE has several significant limitations in its applications for reliable land-mobile communications. Vulnerabilities in the physical layer in LTE make reliability an issue with malicious attacks (see Section 4). Furthermore in catastrophic events where the cellular infrastructure is disabled, the handsets will have no way to communicate with one another. Unlike other standards which employ symmetric air interfaces (e.g. 802.11a), the uplink and down-link protocols for LTE are very different and inhibit the ability for mobile handsets to communicate directly to one another. The bottom line is that regardless of the standard, any system relying on commercial infrastructure is susceptible to malicious attacks, severe outages, and loss of communications links.

By augmenting an inexpensive commercial handset (e.g. an Android smart phone with a touch screen interface) with a software radio platform, the first responder effectively gets the best of both worlds: a fast data connection with commercial infrastructure when available, and a reliable communications platform otherwise. The SDR platform can take the form factor of a sleeve for the handset so the entire unit wouldn't be considerably larger than existing hardware (see Figure 1). The operating system itself can be customized to include specific applications for first response units, including locations of teams, status reports, and graphical information such as criminal history and medical records. Software-defined radios can be deployed with a variety of services

to support compatibility with existing commercial infrastructure. This is a vital to public safety networks as the availability of particular services aren't necessarily known at the time of a catastrophic event. Furthermore, it isn't feasible to know before an event what services are required, what frequency bands are available, or the state of the infrastructure. Having an arsenal of communications protocols within the capabilities of a single handheld device is a powerful tool and a large step in the direction of enabling reliable and resilient communications in unknown environments. In this fashion the full platform can ride on the success of commercial development yet still provide functionality for reliable communications even during outage periods.

An enabling technology to reduce the size, weight, and power requirements of the flexible radio transceiver is to convert the desired RF signal to baseband for processing. The Motorola RFIC5 is a direct-conversion transceiver on a chip that can tune to any carrier frequency between 10 MHz and 6 GHz, and down-convert channels as wide as 20 MHz to baseband [8]. The chip also includes high-speed analog/digital converters, which further simplifies radio design. With this hardware, a simple Android smart phone or tablet can instantly communicate with two-way radios in any band using any modulation technique. It can serve as a bridge between the cellular network and the two-way radio network. The same phone/tablet can receive broadcast signals, talk to white space devices, work with military hardware, and even implement application-specific custom protocols for industrial use. Since an Android phone is at the core of the radio, it will also be able to support Android applications.

3 Cognitive Radio Network Capabilities

As mentioned in the previous section, software-defined radio platforms can significantly augment the capabilities of existing standards by enabling communication using any standard necessary. By complementing a commercial platform which already includes hardware for existing standards (LTE, GSM, CDMA, WiFi, BlueTooth, GPS, etc.) the SDR platform can provide additional support for other existing and future protocols. However the full benefits of software-defined radios are visible through cognition; permitting the radio to be aware of its surroundings and react accordingly. By employing a self-adapting engine, cognitive radios use goal-driven autonomous operation to improve link performance and reliability, all while acting completely transparently to the mobile operator. For example, in a catastrophic event where the main infrastructure is disabled, the radios could adapt by establishing an ad-hoc network completely autonomously. This promotes heterogeneous radio link coexistence: supporting multiple standards within a single network. Furthermore, a radio with cognitive capabilities can act as a bridge to link two completely different standards and promote interoperability between separate groups.

In a catastrophic event where many first responders are dispatched, there are often not enough physical radio channels to support the communications demands of the teams. As with many existing commercial cellular protocols, current public safety networks are limited in the number of physical channels available at any particular time. This restriction can have deleterious effects on the success of the mission and can significantly hinder the ability of response teams to complete necessary tasks. One of the true benefits of cognitive radio is with dynamic spectrum access: the ability to seek underused and available frequency bands and utilize them for communications, particularly

in emergency situations. This is particularly relevant in the recently re-farmed television bands in which public safety spectrum currently resides. By enabling the radio to act autonomously and gain access to spectrum "white space," the capacity and reliability of the network can be greatly enhanced. Dynamic spectrum access capabilities can only be enabled on a radio platform with a flexible RF front end, which is why software-defined radios are particularly tractable for such applications.

Finally, cognitive radio technologies have demonstrated further benefits to network reliability through intelligent adaptive link adaptation. With its ability to modify its behavior based on external conditions and experience, cognitive radio can decide the best operational mode and parameter settings for a given situation. This includes reducing transmit power to save battery life (and reduce interference to neighboring networks) when the link quality is good, and switching to more reliable modes when the link quality is poor. Because the radio can act in an unsupervised manner, its actions are transparent to the operator. This enables higher-level functionality as well, such as facilitating self-organizing ad-hoc networks which can support reliable infrastructure-less communications in times of need.

4 Enhanced Security in the Physical Layer

Current public safety equipment employs a degree of security through obscurity and anti-tampering measures; however these measures can always be breached with enough time and effort. For example, Glass *et al.* recently demonstrated in [9] how an inexpensive software-defined receiver could examine and manipulate P25 data traffic at both the physical and data link layers of the protocols stack, exposing flaws in the design, implement countermeasure attacks, reverse-engineer protocols, and crack the encryption keys securing the underlying data. Furthermore Clark *et al.* in [10] demonstrated that the particular framing structure of the APCO P25 protocol allows a careful jammer to attack only the *Network Identifier* sub-field of voice traffic to effectively has more than 14 dB of an average power advantage over the legitimate transmitter. Even the LTE air interface reserves the center 62 subcarriers (930 kHz) on the down-link for primary synchronization and acquisition by the mobile handset. A malicious attacker could easily jam just this acquisition signal (or even just the pilot subcarriers) to prevent the mobile devices from initial synchronization, bringing the entire cell down.

By deploying anti-jamming countermeasures in the physical layer, public safety communications can remain stable and resilient even in the presence of malicious RF attacks. Spread spectrum communications are widely considered to be the most interference-resistant mechanisms available today, and have seen wide success in commercial systems such as direct sequence spread spectrum and frequency hopping. These protocols are designed to withstand strong levels of interference and have proven successful even in hostile RF environments. With a software-defined radio these security levels are available at the physical layer and enhances the security of the communications links. Furthermore the addition of cognition into the radio promotes an added layer of resiliency to the network.

5 Enhanced Networking Security and Capabilities

Any radio communications system is to some degree susceptible to physical layer vulnerabilities such as denial of service (DoS) attacks; however the severe vulnerability of current systems to such attacks is particularly notable. For example, it was shown in [9] that anti-theft mechanism built into P25 devices could be easily used against the network as a special "inhibit" command could be sent unencrypted from a malicious party to "stun" valid radios and bring the network down. Public safety communications system need to be capable of operating in a variety of modes to enhance network security and harden communications links. This includes the following scenarios:

1. *Several nodes are outside the range of the base station but within range of several nodes within the network.* Radio nodes can operate in gateway mode, by which a single mobile with connection to the network can act as a relay for other nearby nodes outside the range of the infrastructure. This effectively extends the range of the network at the cost of end-to-end latency and battery life of the relay node.

2. *Legacy radios are to communicate with modern infrastructure.* As described in Section 2, if the relay node as software-defined radio capabilities, it can translate protocols for end-to-end voice transparency. For example, if the end node is equipped only with an FRS radio, the relay node could bridge the network's encrypted digital signal into analog FM.

3. *The base station is operational, but the back-haul link to the outside network is unavailable.* The network must support in-network calling without relying on external connections. For example, LTE supports user authentication but this functionality resides outside the base station in the mobility management entity. Without authentication the handsets cannot connect to the base station. As such, public safety radio infrastructure must be capable of handling temporary authentication for scenarios in which the local network is disconnected from the public mobile network.

4. *The base station is unavailable.* In such a scenario, the mobile devices must be capable of direct mode operation in which they can communicate without the use of a master tower. This implies that not only must the devices be capable of communicating directly to each other (e.g. "walkie talkie" mode) but also be able to negotiate cryptographic key exchanges without a supervising agent. The lack of this particular functionality is a known security flaw in the APCO P25 system which requires either manual or over-the-air re-keying through a key distribution center [11].

Consequently public safety radios will need to operate in a variety of modes (such as trunked point-to-point, broadcast, ad-hoc networking, etc.) to ensure resilient communications. These capabilities are facilitated by mobile software-defined radio transceivers and are hardened by cognitive radio technologies. Furthermore, with the ability for radio handsets to detect attacks comes reliable, "always-on" communications links, and permits the network to stay a step ahead of malicious attackers by reporting the problem to the dispatcher and alerting the radios in the rest of the network to act accordingly.

Testing the functionality of such a system requires a mature full-scale network testbed with software-defined radio transceivers, such as Virginia Tech's cognitive radio network (CORNET) [12, 13]. Such

a testbed can identify key vulnerabilities in the system design and instantly accommodate improvements through software updates. Furthermore an improved area-wide testbed would help spur the development of cutting-edge wireless technologies and advance public safety communications even faster.

6 Enhanced Data Security

Recently a number of vulnerabilities and security flaws have been discovered and exploited for several existing world public safety standards including P25 [10, 9] and TETRA [14] in terms of authentication and data encryption. Protection of confidential information in a mobile environment is extremely difficult because of the heighten risk profile of mobile devices. Additionally, public safety is seeking to leverage commercial mobile broadband technology which was never designed to meet the security requirements of a non-commercial set of users. Significant research is required into how public safety can effectively, robustly, reliably, and securely leverage this infrastructure. In particular, end-to-end encryption is necessary that protects data from the handset all the way through the network to the end point. This encryption must be provisioned in such a way that a lost or stole devices does not expose the entire network to authentication and authorization attack vectors.

One area of research is implementation of voice and data communications protocols for smartphones that meet NIST FIPS 140-2 cryptographic requirements for end-to-end security. Taking it a step further for military and defense application would be implementation of Suite B ciphersuites including Elliptic Curve Cryptography to protect classified data.

Ultimately the security of the devices themselves is the critical link. Physical access to a device will result in total compromise unless cryptographic material can be adequately protected, and externally-installed applications are sufficiently isolated from sensitive operating system functions of the device.

7 Coexistence with Radar

Over the next ten years, President Obama's National Broadband Plan seeks to free up 500 MHz of spectrum for commercial broadband carriers to deploy the next generation of mobile broadband, and DOD radar spectrum is a prime candidate because it is often perceived as underutilized. To cope with potential loss of both radar and communications spectrum, the US Navy is investigating how heterogeneous technologies can coexist and operate simultaneously without causing interference to one another. Virginia Tech has proposed the application of machine learning and cognitive radio techniques that would allow a radar to survey its spectral environment, characterize the channel access behaviors of the devices in its environment, and develop a frequency hopping pattern than simultaneously minimizes mutual interference while maximizing radar mission objectives. The system will predict when and where spectrum access opportunities will occur, and schedule radar pulses in those predicted slots. Our overall goal is to leverage all spectral, spatial, and temporal resources available to achieve coexistence. Over the past 10 years the field of spectral dynamic

spectrum access has matured to the point of commercial and military deployment. This will be a key enabler of our approach, but is expected to be insufficient in crowded spectral environments. Research into temporal interleaving of signals [15] has received some academic interest but so far there has been no market for commercial development because the commercial sector has a fundamentally different business model. Cognitive MIMO techniques [16, 17, 18], using machine learning and reasoning-based algorithms and protocols, and real time spectrum coordination and transmission scheduling will also be leveraged to achieve spectrum coexistence between military radars, military communications, and commercial communications. If successful, both governmental and commercial radar programs can apply the resulting technology to a broad class of spectrum sharing applications.

This is particularly relevant to public safety networks radar bands offer quality spectrum for such applications. This is particularly relevant for civilian bands (e.g. aviation, weather) which are not being fully utilized. Specifically, TD-LTE is a prime candidate as an air interface as it is both an emerging standard and does not require paired spectrum bands but operates in a time-duplexed manner. The Wireless Innovation Forum has a working group [19] to specifically address TD-LTE in television white space; as this technology could be tailored specifically to the radar bands, capable systems could offer additional spectrum resources to public safety networks. Furthermore the future of radar might need to re-define current systems for coexistence with communications networks. We need to carry out research for both radar and communications signals to ensure that spectrum coexistence is mutually beneficial, and determine the aggregate bandwidth and performance limitations of both.

8 Satellite Communications for Drop-in Back-haul

A major contributing factor to the long delay in providing relief to afflicted areas after disasters, both natural and man-made, is the nearly complete collapse of communications infrastructure. If the first responder teams could rely on having on-demand communications, carried in with them in a lightweight communications package which could easily be interfaced to their existing communications assets, the time without quality coordinated communications would shrink dramatically.

There are a confluence of factors now allowing us to mitigate this problem and for a small investment in a system to do the actual communications.

1. Increasing availability of commercial off the shelf software-defined radio gear available for construction of fully functional systems as prototypes for complete demonstration of the required cognitive radio systems. These include Ettus, Inc. Universal Software Radio Peripherals (USRP) to which we can easily add inexpensive communications board to provide the required RF paths [20]. A working cognitive radio networking testbed has been built using these devices at Virginia Tech in its CORNET [12, 13].

2. Intelsat, one of the worlds largest providers of geosynchronous communications satellites flies their large satellite buses with lots of excess power (as much as 1.5 kW) and will sell "RideShare" flights to geosynchronous orbit. These opportunities have been promoted by Department of Commerce's Office of Space Commercialization and called "Hosted Payloads"

[21] and in 1999, NRO and NASA Goddard Space Flight Center hosted a RideShare conference for which there are proceedings [22].

3. Delay tolerant and disruption tolerant networking [23, 24] has received major research support from DARPA in support of its WNAN radio development.

4. The Radio Amateur Satellite Corporation undertook a study and did a design of a rideshare payload for flight on an Intelsat bus. It would have supported approximately one hundred 64 kbps links with a small dish (60cm) and with a 2 meter dish high quality video links.

5. Dynamic spectrum access and cognitive Radio would be major enablers of such a system and Virginia Tech has been a major contributor to the research in this area.

NIST should allow a study to go forward on a design for such as system and how it could use White Space, Public Service spectrum, amateur radio (amateur satellite) spectrum to provide for a very inexpensive system on orbit with projected 15 year lifespan could have a major impact on the required communications early in disaster afflicted areas for minimal cost.

9 Hardening Wireless Infrastructure

Wireless systems are quickly replacing wired systems. This is clearly evident by the decline in land-line phones and the rise of cellular phones, with many having already given up land-line residential service. Data traffic for smart phones is well on track to surpass the amount of data being sent to residential and business DSL and cable modems. Although wireless systems enjoy mobility, there is, however, one key advantage of wire-line systems—reliability. Historically, wire-line systems are much better at withstanding natural disasters and their ability to handle high and unpredictable peaks in traffic demand is much better. Cell towers are vulnerable to many natural disasters. In addition, the power grid supplying cell sites can be disrupted and while these sites often having backup power capability, there is a limit to the longevity of this power supply. Furthermore, as the push for more inexpensive and smaller cell sites increases backup power capability is beginning to be sacrificed. Spectrum scarcity has become so pronounced that service providers operate at their capacity limit during the rush hour, leaving no room for traffic surges during crises. Furthermore, the back-haul is also an important reliability issue that depends on shared and concentrated (single point of failure) connectivity. These trends are especially disturbing when one considers that public safety is moving towards a cellular infrastructure (for example see Senate Bill S.911) with public safety relying on a combination of commercial cellular systems and publicly operated cellular systems (e.g, LTE 4G cellular in the 700 MHz re-farmed TV bands). The move for public safety towards LTE in the 700 MHz band is mandated by law.

To harden the infrastructure against unpredictable natural disasters requires innovative multi-disciplinary research, incorporating not just communications engineering, but social modeling (levered from epidemiology methodology), network engineering, policy, and cognition. The key challenge is integrating these disciplines in a coherent way to help solve the problems of affecting other disciplines. As an example, consider the occurrence of a natural disaster. Early indications of such a disaster can be revealed through sudden changes in cellular activity. For instance, the ability to

detect traffic accidents quickly has been shown through monitoring cellular traffic activity. The extent of cellular traffic congestion can also reveal the extent of the impact of the accident. Social models that incorporate cellular traffic data can help in detecting and classifying the extent of the incident with greater accuracy. Social models (such as social mobility models) can also be used to determine where congestion and reliability of communications network might be an issue with changing circumstances. These social models can include a number of factors such as the transportation infrastructure, characteristics of the environment (residential or business), population density, and many other factors. It's difficult to plan ahead for any disaster, since the number of possible situations can be overwhelming. Thus, one key aspect is to have an automated method for answering the numerous "what if" questions with wireless infrastructure faults and potential solutions. Could system performance be enhanced by changing antenna tilt; changing frequency allocation; turning on extra channels; adjusting a variety of radio resources, including speech QoS; adjusting data rates; and following certain policies? For example, say two cell sites are destroyed by a hurricane, how should the surrounding infrastructure be reconfigured to fill in the coverage and capacity gaps? Furthermore, one would expect that the traffic models (both cellular and transportation) could completely change due to destroyed infrastructure and the dynamic nature of human behavior when faced with disaster. How would people's communication demands change so that the network can be automatically tuned to accommodate their demands?

These numerous situations could be modeled by the network by probing the environment with scenarios of disaster. The cellular network could, for example, automatically examine mitigation strategies if infrastructure is reduced. This approach would require probing cell phones that would run late at night when the cellular traffic is low to report network performance (this could be implemented as an Android application). The probing process would be similar to war games for cellular networks, games constructed to learn vulnerabilities and mitigation strategies in dealing with loss of infrastructure. As an example, two cell sites could be turned off late at night, simulating the effect of the hurricane destroying those sites; the network can be optimized using the probing phones to feedback information about the network performance as the network tries different radio resource settings to fill in the lost coverage and capacity. Network resources might also be configured according to the nature of the type of disaster through implementation of a social policy. For instance, if the disaster represents a fire, highest priority access is given the fire department while terrorist activities might trigger a higher priority access for the FBI. Voice is usually given priority in any congestion situation, but there may be cases where a public safety organization might be given priority access for its data transmission. Policy has an important role and should impact the relative automatic allocation of radio resources and social scientists must work with engineers to create socially-optimized technical solutions. Social models can help in allocating the resources in area of unforeseen circumstances and help with the most unpredictable aspect, human behavior. For instance, transportation traffic may not flow away from the disaster, as one might intuitively expect, if individuals are seeking to find family members. Likewise, resources may need to be allocated for transportation traffic flowing into a disaster by the public safety organization after a rapid outflow of victims in the disaster area. Such traffic models (mobility and communications) must account for human behavior and public safety needs.

Today we do have rudimentary priority access for public safety in the cellular network. LTE standard promises much more refined prioritization for public safety to help deal with congested cellular traffic, but this feature has yet to be developed and tested. Policy for priority access is

yet to be addressed, e.g., who has higher priority the FBI or local police? There is talk within the cellular industry of self-optimizing network (SON) as a part of the LTE-Advanced standardization process, but the vision for this capability assumes relatively static resource allocation (such as channel allocation) among base stations and doesn't take into account the dynamic nature, priority access, and uncertainty that natural disasters can cause to a large scale cellular network. One thing is very clear, due to costs, equipment availability, and the need for nationwide interoperability, the cellular network will play a much more predominate role in public safety communications.

The key research challenge in building a robust and hardened network is the integration of various facets: social models, physical and network layer resources, and policy together to create tools for modeling, event detection, and real-time coordination of communication resources. Simulation environments can help in the development and evaluation of these tools, but automated techniques using real-life situations and infrastructure need to be developed for creating these models for specific situations and regions. Finally, it is necessary to develop methods for testing the tools on a large scale network. Even the assessment metrics represents a fundamental interdisciplinary research issue.

10 Femto Cells for Fast Network Recovery

While the demand for broadband wireless services is increasing, the ability to provide services is still lacking in many rural areas where cellular coverage is limited. This has been an ongoing problem for some time, and even though the technology is available, it has been a matter of delivering the services in a cost effective manner. However, there have recently been some technical advances that may overcome the cost barrier. There is a great opportunity to develop a product that can provide low cost broadband wireless services based on these new technologies, and increase the coverage of public safety networks in rural areas.

New enabling technologies can be used to develop such products include: femto cells and cognitive radios (Figure 2). The first key technology, femto cells, is low cost cellular base stations for home and office that will begin deployment in the US next year. These base stations are only a few hundred dollars and newer models are expected to handle up to 30 users. Standards bodies are developing approaches for making these base stations self deploying and self maintaining which will mean a substantial cost reduction in deployment and maintenance. Key cost savings comes from being able to use commercial handsets for the user equipment and thus take advantage of costs savings with mass production. The second technology is the cognitive radio; one that can automatically sense the propagation environment, understand the quality of service (QoS) needs, and make adjustments based on the situation. These radios provide the opportunity to exploit co-existence with television and bands which operate in the areas of spectrum which propagate well over long ranges and can penetrate into buildings. Cognitive radio is the mechanism for connecting the femto cells into the network (the back-haul technology) using opportunistic television and radar spectrum. The result is a system that can provide the following benefits:

1. thin clients requiring lower power (and longer battery life) are enabled.
2. since femto cells are lower power and have smaller radio footprints they allow for greater reuse

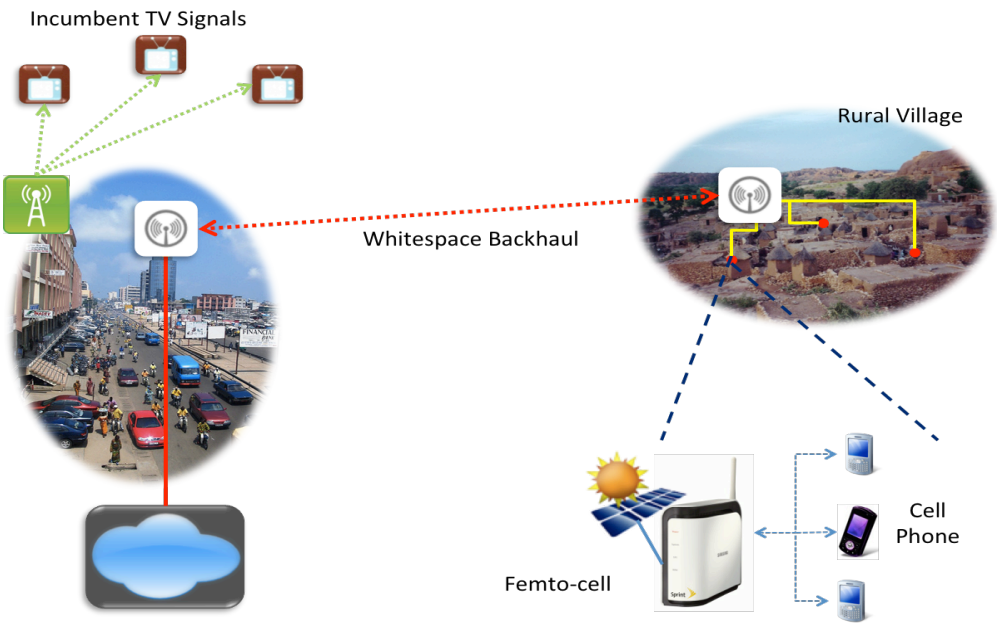

Figure 2: Technologies for rural broadband wireless services.

of spectrum.

3. the femto cells will have smaller radio footprints, reducing the number of types of signals the cell will be required to handle at any one instant in a cognitive radio networking scenario; this will therefore require less capable computational power to handle the simultaneous dynamic spectrum access.

However these systems still require a significant amount of research, particularly when deploying large networks of femto cells to increase capacity. Such networks must be self-organizing to reduce interference as well as intelligent to make good use of available spectrum, particular for backhaul. We will be experimenting with potential waveforms for cognitive radio networking, including TD-LTE which is likely to be considered for 5G cellular communications. The current testbed at Virginia Tech (CORNET) is equipped with very agile RF front ends, ideal for testing software-defined and cognitive radios for public safety. It is imperative that any proposed system for public safety and first responders be tested in a fully-equipped over-the-air testbed capable of handling real world scenarios in hostile wireless environments.

11 Open Standards, Software, and Hardware

Deploying open standards, software APIs, and hardware specifications has three major impacts on the success and wide-spread adoption of public safety radio hardware and protocols:

1. open standards insures interoperability between different systems, agencies, vendors and en-

hances inter-agency cooperating by eliminating jurisdictional boundaries to improve management of incidents and the effectiveness of first response teams;

2. the cost of research, development, and deployment of such devices will be significantly reduced as a result of allowing competitive commercial device-makers entry into the manufacturing process;

3. having an open standard improves the turn-around time for its own improvement by allowing first response teams in the field to give critical feedback to the standards bodies and protocol developers.

The use of LTE networks in the 700 MHz band for public safety is certainly a step in the right direction and provides operators the ability to send and receive large amounts of information; high bandwidth availability is critical for first response teams but is challenging when infrastructure has been compromised. As such it imperative build a non-proprietary network based on industry standards but without relying on commercial infrastructure.

As the dependency on reliable wireless communications infrastructure grows, so does the need for inexpensive devices. A report by the US Government Accountability Office in 2007 states that "until recently, the private-sector coordinating body responsible for developing Project 25 standards—a suite of national standards intended to enable interoperability among the communications products of different vendors—has made little progress [25]." Furthermore most P25 radios used by first responders cost about $2,500 [25, p. 38], about two to three times more than a conventional analog radio suitable for the task. In comparison, a fully functional TETRA radio (integrated GPS, color display, encryption, and authentication) runs less than $1,000. Additionally, the P25 base stations to enable such functionality typically cost in excess of $1M per site while the corresponding TETRA contracts are typically several times lower. TETRA, however, is unavailable in the United States as intellectual property rights owners have signed international agreements promising not to sell TETRA in the U.S. [26].

The disparate efforts concerning public safety technologies are apparent; the influence and the protection of intellectual property rights have hindered the development and production of affordable quality devices in public safety networks. Open standardization of common interfaces (APIs, hardware designs, etc.) helps not only gain wide-spread acceptance by the wireless engineering community but by public safety personnel as well. Opening the standardization of common interfaces, protocols, and application platforms promote competitive provisioning of both hardware and software development. Furthermore, open software and hardware architectures moves development away from privatized and proprietary systems which inhibit innovation and competition; this significantly reduces the cost of devices and decreases the time to market.

12 Conclusions

Until now, existing public safety standards have relied heavily on the security through obscurity model for reliable and protected communications links; however recent studies have exposed particular vulnerabilities in the infrastructure, waveforms, and security measures in currently deployed

systems. This document has presented the critical areas in which public safety should focus its research, including a wide-area network testbed, software-defined radio handsets, cognitive radio technologies for network resilience, enhanced security mechanisms (at the physical and network layers), and coexistence with radar signals for increased spectrum and network capacity. In particular we feel as though the development of a wide-area testbed is a critical step to the success of advancing the next generation of broadband public safety networks. Furthermore, moving quickly on coexistence with radar spectrum is crucial; public safety needs to be involved early to ensure priority access in these bands. Virginia Tech has a deep history of supporting public safety projects including an open-source P25 implementation (NIJ), cognitive radio spectrum bridging between public safety standards (NIJ), wide-band antennas for public safety (NIJ), assistance with the Virginia state police identify improvements in the public safety network, investigation of future network architectures for US customs, conduct a study for the use of Iridium for the FBI, and informal advice to Senate, House representatives, and the executive branch of the government on spectrum policies. We cordially invite NIST to visit our facilities in Blacksburg, VA and see a demonstration of some of these technologies.

13 Facilities and Equipment

Wireless@VT spans the technical spectrum in communications, including antennas and propagation, physical layer design, MAC layer design, networking, and VLSI design. Facilities include fully functional Radio Frequency (RF) and DSP laboratories for modem development, an RF anechoic chamber, instruments for antenna measurements, an antenna range, chip fabrication facilities, and workstation environment with design tools such as MATLAB, NS2, and Cadence. In addition, the center has custom hardware tools such as MIMO propagation measurement systems, Software Communications Architecture (SCA)-based radios, an 8-GHz UWB receiver, a cognitive radio test bed, and 1-GHz sliding correlator for propagation measurements. Many of the special hardware tools were built at Wireless@VT.

A cognitive network testbed has been built within Virginia Tech (CORNET) capable of running applications such as detecting unauthorized transmitters, position location of mobile nodes, cognitive MIMO algorithms, and distributed network algorithms. The Community Infrastructure is deployed in a new building on the Virginia Tech, Blacksburg campus called ICTAS-I. The university has allocated space and special equipment and accessories for the deployment of 48-node physical network [12, 13].

Wireless@Virginia Tech is composed of over 30 faculty members from several different labs spanning expertise in cognitive radio networks, dynamic spectrum access, antennas and propagation, secure communications, wireless and social networks, digital signal processing, and RF/VLSI circuit design.

References

[1] J. Warrick, "Crisis Communications Remain Flawed; Despite Promises to Fix Systems, First Responders Were Still Isolated After Katrina," *Washington Post*, p. A06, December 2005.

[2] D. Jackson, "LTE Rollouts to Begin This Year," *Urgent Communications*, January 2010.

[3] "LTE for Public Safety," *http://www.fiercewireless.com/nextgenspotlight/pr/lte-public-safety*, January 2011.

[4] "The OpenBTS Project," *http://openbts.sourceforge.net/*, October 2011.

[5] "Design Issues for P25 Digital," *http://www.nationalinterop.com/solutions_p25.html*, October 2011.

[6] "Open-Source SCA Implementation::Embedded (OSSIE) Development Site," *http://ossie.wireless.vt.edu/*, October 2011.

[7] "GNU Radio Website," *http://gnuradio.org/*, October 2011.

[8] Gio Cafaro and Tom Gradishar and Joe Heck and Steve Machan and Geetha Nagaraj and Scott Olson and Raul Salvi and Bob Stengel and Bill Ziemer, "A 100 MHz-2.5 GHz Direct Conversion CMOS Transceiver for SDR Applications," in *Proceedings of the SDR Forum Technical Conference*, Washington, DC, December 2009.

[9] Stephen Glass and Vallipuram Muthukkumarasamy and Marius Portmann and Matthew Robert, "Insecurity in Public-Safety Communications: APCO Project 25," *http://www.nicta.com.au/pub?doc=5076*, 2011.

[10] Sandy Clark and Travis Goodspeed and Perry Metzger and Zachary Wasserman and Kevin Xu and Matt Blaze, "Why (Special Agent) Johnny (Still) Cant Encrypt: A Security Analysis of the APCO Project 25 Two-Way Radio System," in *Proceedings of the 20th Usenix Security Symposium*, August 2011.

[11] Telecommunications Industry Association, "APCO Project 25—Over-the-Air-Rekeying(OTAR) Protocol," Technical Report TIA-102.AACA.

[12] T. R. Newman, S. M. S. Hasan, D. Depoy, T. Bose, and J. H. Reed, "Designing and Deploying a Building-wide Cognitive Radio Network Testbed," *IEEE Communications Magazine*, vol. 48, no. 9, p. 106—112, 2010.

[13] "CORNET website," *http://cornet.wireless.vt.edu/*, October 2011.

[14] Y.-S. Park, C.-S. Kim, and J.-C. Ryou, "The Vulnerability Analysis and Improvement of the TETRA Authentication Protocol," in *ICACT*, April 2010, p. 1469—1473.

[15] T. Clancy and B. Walker, "Predictive Dynamic Spectrum Access," in *Proceedings of the SDR Forum Technical Conference*, Washington, DC, November 2006.

[16] J. R. Guerci, M. C. Wicks, J. S. Bergin, P. M. Techau, and S. U. Pillai, "Theory and application of optimum and adaptive MIMO radar," in *Radar Conference, 2008. RADAR '08. IEEE*, May 2008, p. 1—6.

[17] D. Bliss and K. W. Forsythe, "Multiple-Input Multiple-Output (MIMO) Radar and Imaging: Degrees of Freedom and Resolution," in *Signals, Systems and Computers Conference Record of the Thirty-Seventh Asilomar Conference on*, vol. 1, 2003, p. 54—59.

[18] D. Bliss, K. W. Forsythe, S. K. Davis, G. S. Fawcett, D. J. Rabideau, L. L. Horowitz, and S. Kraut, "Gmti mimo radar," in *Waveform Diversity and Design Conference, 2009 International*, February 2009, p. 118—122.

[19] "TD-LTE White Space Project: Call for Participation," *http://www.wirelessinnovation.org/assets/documents/Project_TD-LTE%20White%20Space.pdf*, 2011.

[20] M. Ettus, "Ettus Research LLC," *http://www.ettus.com/*, October 2011.

[21] "Space commerce; hosted payloads," *http://www.space.commerce.gov/general/commercialpurchase/hostedpayloads.shtml*, 2011.

[22] "NRO/GSFC Rideshare Conference," *http://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20010084928_2001116065.pdf*, 1999.

[23] P. F. Marshall, "DARPA Progress Towards Affordable, Dense, and Content Focused Tactical Edge Networks," in *Military Communications Conference*, November 2008, p. 1—7.

[24] ——, "Extending the Reach of Cognitive Radio," *Proceedings of the IEEE*, vol. 97, no. 4, p. 612—625, April 2009.

[25] United States Government Accountability Office, "FIRST RESPONDERS; Much Work Remains to Improve Communications Interoperability," *http://www.gao.gov/new.items/d07301.pdf*, April 2007.

[26] D. Jackson, "P25-TETRA Comparison is A Non-Starter," *Urgent Communications*, February 2009.