Public Safety Spectrum

July 2011

http://www.rysavy.com

About Rysavy Research

Rysavy Research LLC is a consulting firm that has specialized in wireless technology since 1993. Projects have included reports on the evolution of wireless technology, test reports, spectrum analysis for broadband services, evaluation of wireless technology capabilities, strategic consultations, system design, articles, courses and webcasts, and network performance measurement.

Peter Rysavy, president of Rysavy Research, specializes in the capabilities and evolution of wireless technology. He has written more than a hundred and twenty articles, reports and white papers, and has taught forty public wireless courses and webcasts. He has also performed technical evaluations of many wireless technologies including municipal/mesh Wi-Fi networks, Wi-Fi hotspot networks, mobile browser technologies, cellular-data networks, and wireless e-mail systems.

From 1988 to 1993, Peter Rysavy was vice-president of engineering and technology at LapLink where projects included LapLink, LapLink Wireless, and connectivity solutions for a wide variety of mobile platforms. Prior to that, he spent seven years at Fluke Corporation where he worked on touch screen and data acquisition products.

Peter Rysavy is also the executive director of the Portable Computer and Communications Association (PCCA, http://www.pcca.org), a group that evaluates wireless technologies, investigates mobile communications architectures and promotes wireless-data interoperability. Peter Rysavy graduated with BSEE and MSEE degrees from Stanford University in 1979. More information is available at http://www.rysavy.com.

Notice

Rysavy Research provides this document and the information contained herein to you for informational purposes only. Rysavy Research provides this information solely on the basis that you will take responsibility for making your own assessments of the information.

Although Rysavy Research has exercised reasonable care in providing this information to you, Rysavy Research does not warrant that the information is error-free. Rysavy Research disclaims and, in no event, shall be liable for any losses or damages of any kind, whether direct, indirect, incidental, consequential, or punitive arising out of or in any way related to the use of the information.

Table of Contents

Introduction

Through advances in technology, mass adoption, and global innovation, today's wireless networks offer tremendous voice and data capabilities. Voice coverage is reliable and ubiquitous, while data services, now commonly called mobile broadband, provide throughput rates to users of millions of bits per seconds, orders of magnitude higher than just a decade ago. New generations of wireless technology, such as Long Term Evolution (LTE), have just started to be deployed, and will deliver even greater data capabilities. LTE is the perfect choice for public safety applications. This paper will explain why 20 MHz of contiguous spectrum is essential for this technology.

This paper also discusses the emergence of LTE as a global standard, the bandwidth requirements of different applications, the relationship between spectrum and capacity, the crucial need for at least 20 MHz for public safety, and the challenges of alternate approaches that seek to share spectrum between Public Safety and commercial operators.

LTE as a Global Standard

LTE is the technology likely to see the broadest deployment of any new wireless technology over the next decade. Nearly all major cellular operators have committed to adopting LTE. The result will be huge economies of scale leading to cost-efficient services and devices. LTE not only provides high data throughput, but packets traverse the network with low delay, and traffic flow can be controlled to provide high levels of quality-of-service for applications such as video and voice over Internet Protocols (VoIP). First Responders have wisely endorsed LTE for their 700 MHz broadband networks.

Spectrum and Capacity

The amount of capacity in wireless networks depends on a variety of factors, but in general, mobile-broadband networks have significantly lower capacity than fixed-broadband networks. Capacity can be calculated by assessing the spectral efficiency of different wireless technologies, a value that is represented in bits per second per Hertz of spectrum (bps/Hz). While new technologies such as LTE are spectrally more efficient than prior technologies, all wireless technologies are reaching what is called the Shannon bound, a law that dictates the maximum spectral efficiency that a technology can achieve relative to noise.

By knowing the radio channel size and the spectral efficiency of the wireless technology, one can estimate the aggregate capacity of a cell site. LTE in its initial deployments has a spectral efficiency value for the downlink of about 1.5 bps/Hz per sector. For the uplink, it is .65 bps/Hz.[1] Thus, LTE will have the capacity values as shown in Table 1.

Table 1: LTE Capacity Values

Amount of Spectrum	Downlink Capacity	Uplink Capacity.
10 MHz (5 MHz down, 5 MHz up)	7.5 Mbps	3.25 Mbps
20 MHz (10 MHz down, 10 MHz up)	15 Mbps	6.5 Mbps

Given the application requirements discussed in the next section, these capacity values, even for 20 MHz are quite finite. The capacity in 10 MHz, as is made clear below, is simply too limiting to provide a broadband network that can accommodate the needs of first responders.

Application Bandwidth Requirements

There are multiple factors that are fueling growth in data usage including:

- **Faster networks.** The faster that data can be exchanged, the more likely it is that applications will take advantage of the speeds, especially since faster speeds can mean less waiting time for workers.
- **More network-enabled devices.** New device categories such as tablets and netbooks are expanding overall data consumption, especially because of the delivery of high-quality video. Just as consumers and enterprises are adopting these new device categories, so will first responders.
- **Increasing computing speeds.** The faster the platform can compute, the more data an application can process in real time.
- **Higher screen resolution.** Greater screen resolution corresponds to higher resolution video options for users.

[1] For a detailed discussion of spectral efficiency values, refer to my report, "Transition to 4G," September, 2010. http://www.rysavy.com/Articles/2010_09_HSPA_LTE_Advanced.pdf

- **Embedded modems.** An increasing number of laptops and tablets come with embedded 4G modems, facilitating the use of mobile broadband service.

The question is how much bandwidth do applications actually need. Some typical values are shown in Table 2:

Table 2: Application Bandwidth Requirements

Application	Bandwidth Requirements
Voice over IP	10 thousand bits per second (kbps) to 20 kbps (both downlink and uplink directions.)
General-purpose audio to record all sounds	About 100 kbps.
Video	Ranges from 200 kbps on a small-screen device like a phone, to 1 million bits per second (Mbps) for medium resolution on a laptop, to 5 Mbps for high definition.
Web browsing	Usually requires about 1 Mbps or higher to provide good response time.

By comparing these throughput requirements against the capacities listed in the previous section, one can see that just a handful of first responders could easily consume the capacity of a 10 MHz LTE network. LTE in 10 MHz has a downlink capacity of 7.5 Mbps. Thus, 8 downlink streams at 1 Mbps each would consume the capacity of the cell sector. On the uplink capacity is even more constrained at 3.25 Mbps where just 4 uplink streams would consume capacity. For example, these streams could be video from patrol cars at a crime scene.

Public-safety applications will increasingly demand higher bandwidth. The same innovation shown in commercial broadband will extend to public-safety broadband. In the February 2011 report "Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2010-2015," Cisco predicts a 92% compound annual growth rate in mobile traffic. There is no reason that such trends do not also apply to Public Safety. Examples of public-safety applications include:

- Wireless video surveillance.
- Aerial video from a helicopter over a scene fed to personnel below.
- Video-based training to remote emergency workers.
- Real-time license plate recognition.
- Testimony based on video transmitted from an emergency-services vehicle or command post.
- Sending and receiving high-resolution pictures.
- In-field biometrics (such as iris and fingerprint identification).
- Automated vehicle location and navigation.
- Medical applications such as telemedicine, patient records, and high-resolution video to enable medical services performed at a scene of an accident.

It is important to note that another aspect of some public-safety applications is that they demand bandwidth continuously. For example, a patrol car in an emergency situation may need to transmit a constant video stream.

The Need for 20 MHz

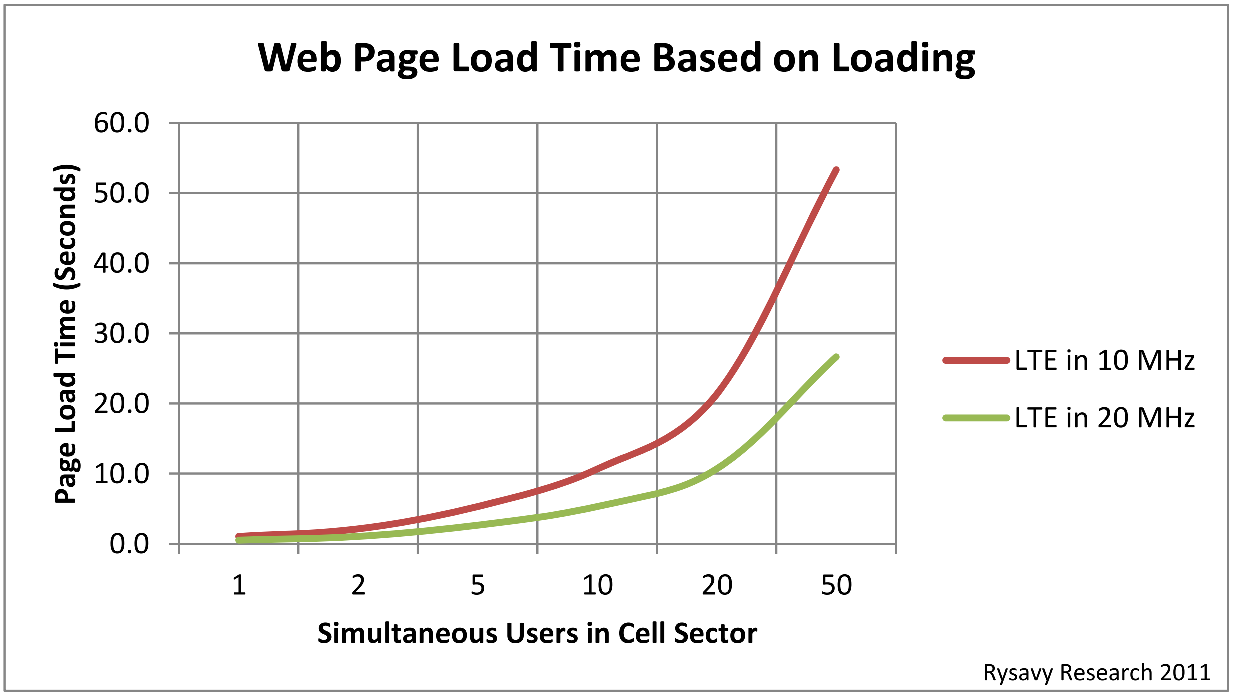
In light of the finite capacities of LTE as discussed above and growing bandwidth demands of public-safety applications, my view is that 20 MHz of spectrum for LTE is the absolute minimum to satisfy the needs of law enforcement. The available throughput per user goes down as the number of users increases. Given that many broadband applications need 1 Mbps or higher throughput, sector capacity can be exhausted quickly.

While commercial operators can design their networks for typical densities of mobile users, emergency situations can result in needing to support extremely high densities of public-safety workers. For this reason alone, the public-safety network has to have as high a capacity as possible. The network must have at least 20 MHz of spectrum. Anything less could lead to catastrophic consequences due to applications performing unreliably or failing completely.

The consequence of insufficient spectrum is restricted capacity, which combined with high demand, causes network congestion. For applications, this means sluggish behavior or outright failures.

Figure 1 shows an example of how an application begins to respond extremely slowly as the number of simultaneous users increases. Assuming a Web page of 1 MByte size, a page load time of 10 seconds (considered very slow) occurs with 10 users in a 10 MHz deployment scenario but not until 20 users in a 20 MHz deployment scenario.

Figure 1: Web Page Load Times Based on Simultaneous Users



Beyond sluggish performance in congestion situations, there is also the high likelihood that networks simply have to drop packets of data. Packets arrive at a base station over a high-speed connection such as fiber but then the base station forwards the packets using the slower radio connection. If there are too many incoming packets the inevitable result is that the base station, or infrastructure nodes prior to the base station, will drop or significantly delay packets.

Consequences of such congestion are not just slower performance but also application failures. Most communications protocols implement timeouts on their operations, including Transmission Control Protocol (TCP) itself, the packet-transport protocol used in the Internet to provide reliable end-to-end delivery. With large delays or dropped packets, communications protocols attempt to deliver data reliably, but at some level of congestion, they can no longer cope properly, and applications will either indicate a failure, or worse yet, require an application or full-system restart.

Beyond needing 20 MHz just to satisfy bandwidth requirements, there are compelling reasons for providing Public Safety 20 MHz of contiguous spectrum.

- LTE is spectrally more efficient operating in 20 MHz channels than 10 MHz channels. In other words, the network can deliver more bits per second using a 10 MHz radio channel (10 MHz down, 10 MHz up) than in two 5 MHz radio channels.
- Using non-contiguous radio channels will significantly increase the cost of the radio-access network due to the need for additional radios and antennas.
- Adding spectrum later in a non-contiguous manner will result in devices in the field likely not being able to take advantage of the new spectrum.

Challenges in Sharing Spectrum

There are arguments for alternative approaches to dedicating spectrum for Public Safety, such as sharing commercially-allocated spectrum between first responders and commercial operators, with the commercial operator serving as the primary user or licensee. This is a bad idea for a multitude of reasons.

The first reason is that the needs of commercial customers and Public Safety are inherently different. Commercial networks are developed in a highly competitive environment where operators invest in a way to provide services at the lowest possible cost to customers. These low costs are a major factor in what is driving the broadband market. First responders, however, need hardened networks that are extremely reliable. This hardening includes items such as long-term backup power, redundant backhaul, diversified routing, and explosion-proof sheltering, thus significantly increasing the cost of the network, and likely not making it viable from a competitive aspect for the private sector.

Sharing of spectrum also assumes that public-safety applications will obtain the bandwidth they need when they need it from the commercial entity. This assumption, however, is fraught with risk for the following reasons:

- **Policies implemented by commercial operators may not sufficiently address public-safety needs.** Policies, such as reserving certain amounts of bandwidth for commercial customers, may result in insufficient capacity for public-safety applications in emergency situations.
- **Prioritization schemes may not work correctly.** In an emergency situation where there is massive demand on the network from both constituencies, it is possible that prioritization schemes will not work as planned simply because they may never have been tested under such extreme conditions.

- **Users may defeat prioritization schemes.** It is already common for users to hack their devices, especially smartphones, to access services not in their current service plans. These modifications could defeat the prioritization schemes at exactly the time they are most needed.

Nevertheless, if Public Safety has control of the spectrum and they wish to lease part of their network capacity to other entities, this can be feasible and even desirable for defraying costs, so long as Public Safety can specify the terms of such arrangements, can implement the appropriate preemption capabilities, and so long as the underlying network is built to address the specific requirements of Public Safety.

Conclusion

I strongly believe that Congress should reallocate the 10 MHz D Block (758-763 MHz and 788-793 MHz) directly to Public Safety. This will enable a national broadband network for emergency services that will address the critical needs of this country. There are many reasons to have 20 MHz of contiguous spectrum available for Public Safety, including sufficient capacity, lowest-cost network deployment, and dependable network operation in emergency situations. Not doing so places this country in unnecessary jeopardy. This is a historic, and potentially last chance to allocate 20 MHz of contiguous spectrum to Public Safety. We should not squander this opportunity.