Telecommunications Policy 34 (2010) 200–220

Contents lists available at ScienceDirect

Telecommunications Policy

URL: www.elsevierbusinessandmanagement.com/locate/telpol

Quantifying the costs of a nationwide public safety wireless network ☆

Ryan Hallahan [a,*], Jon M. Peha [a,b]

[a] Department of Engineering and Public Policy, Carnegie Mellon University, USA
[b] Department of Electrical and Computer Engineering, Carnegie Mellon University, USA

ARTICLE INFO

Keywords:
Public safety
First responder
Wireless
Spectrum
Cost estimate
Homeland security

ABSTRACT

The existing US public safety wireless infrastructure consists of thousands of disparate systems built by separate local agencies. Problems with interoperability, cost, spectral efficiency, and limited functionality plague these systems but could be significantly reduced through the deployment of a single nationwide network that serves all public safety personnel. Two major efforts towards such a nationwide network are the federal-government-only Integrated Wireless Network (IWN) and an FCC-led effort to create a public-private partnership in the 700 MHz band; the future of both projects is uncertain due in part to concerns surrounding cost. This paper presents a model to estimate cost for two fundamental approaches to a nationwide network: a *public-safety-only network* and a *public–private partnership* which serves both public safety and commercial subscribers. We apply this general model to four network scenarios which differ in the amount and band of spectrum allocated as well as the number and type of subscribers (public-safety-only versus commercial and public safety) under three traffic scenarios: voice-only, data-only, and voice and data. We demonstrate that the nation's many small systems could be replaced with a single nationwide network with a small fraction of the tower sites and spectrum. The cost of building this new infrastructure is comparable to what is likely to be spent in just a few years on upgrading and maintaining the existing infrastructure. In addition, we show that these cost estimates are highly dependent on some key system design parameters including the public safety capacity required and signal coverage reliability, which must therefore be well-defined in advance.

1. Introduction

Recent tragedies in the United States have demonstrated many of the deficiencies of the current public safety systems across the nation and the severe consequences that occur when these systems fail (National Commission on Terrorist Attacks Upon the United States, 2004; Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina, 2006). Among the problems, the existing infrastructure is expensive, spectrally inefficient, limited in functionality and lacks interoperability. The potential deployment of a nationwide public safety wireless system presents an opportunity to alleviate these problems (Peha, 2007), but there is considerable uncertainty surrounding the cost of the

☆ All research presented here was performed at Carnegie Mellon University. Opinions expressed belong to one or both authors, and do not represent any other individual or organization.

* Corresponding author.
E-mail addresses: hallahan@cmu.edu (R. Hallahan), peha@cmu.edu (J.M. Peha).
URLS: http://www.contrib.andrew.cmu.edu/~rhallaha/ (R. Hallahan), http://www.ece.cmu.edu/~peha (J.M. Peha).

0308-5961/$ - see front matter © 2010 Elsevier Ltd. All rights reserved.
doi:10.1016/j.telpol.2010.01.002

current proposals. In this paper, we provide an analysis of the costs of two fundamentally different approaches to a nationwide network while investigating the factors that have the greatest impact on cost.

In the wake of these tragedies, the lack of interoperability between systems (i.e. the ability to communicate across agencies) has been the focus of increased attention from both the academic community (Brito, 2007; Faulhaber, 2007; Mayer-Schoenberger, 2002; Weiser, 2007) and federal government (National Task Force on Interoperability [NTFI], 2003; SAFECOM, 2006a; US Department of Homeland Security [DHS], 2007). And while there are a variety of ways to improve interoperability by itself (Weiser & Hatfield, 2007), such as patching together the existing public safety systems[1] or deploying new networks based on newer narrowband technologies such as Project 25 (P25)[2], doing so is limited in its effectiveness, and would only address one of several problems plaguing the existing infrastructure.

Deploying a nationwide public safety wireless network can inherently solve technology-based interoperability by employing a coherent architecture and a single equipment standard in the design. By avoiding the shortcomings of the previous fragmented approach to public safety (Peha, 2007), a nationwide network can also address many problems which interoperability-specific solutions do little to alleviate, and often exacerbate (Peha, 2005). Instead of allocating spectrum individually[3] to more than 50 000 state and local public safety agencies across the country (Booz-Allen & Hamilton, 1999) who deploy networks independently and with limited coordination between neighboring agencies (Peha, 2005), there is a single nationwide network to be designed and deployed. A single network makes it possible to exploit significant economies (to reduce costs and increase spectral efficiency) and use broadband technologies to introduce new functionality (such as streaming video to users who previously had to rely on voice-only systems).

Currently, there are two fundamentally different approaches to the creation of a nationwide public safety wireless network: a system that would serve only public safety users and a public–private partnership that would serve both commercial and public safety users on the same network (Peha, 2007).

An example of a public-safety-only network is the Integrated Wireless Network (IWN). This is a program by the US Departments of Justice, Treasury, and Homeland Security to provide 80 000 federal public safety users across the nation with mission critical voice service (Office of the Inspector General, 2007). The current design for IWN (General Dynamics C4 Systems, 2009) is based on the Project 25 narrowband technology which will not support broadband data applications. Additionally, it is expected that the network will use spectrum from the federal allocations around 168 and/or 414 MHz as most of the agencies that would use this network have their existing land mobile radio (LMR) operations concentrated in these two bands (Hoffman, Matheson, Najmy, & Wilson, 2006). By extending this system to support broadband data applications and to serve local and state public safety users, there are potential cost savings and spectral efficiency gains as compared to independently building two nationwide networks to support these user groups separately, as discussed in (Peha, 2006).

In addition to a public-safety-only network like IWN, there have been proposals for a public–private partnership network that would serve both public safety and commercial users (Federal Communications Commission [FCC], 2007). Since public safety communication systems are designed for worst-case capacity demand scenarios and most of the time these large-scale emergencies are not taking place, there is usually unused capacity available on these networks (Bykowsky & Marcus, 2002; Marsh, 2004; Peha, 2007). This implies that if public safety were to share spectrum with a commercial partner, most of the time the commercial partner could use some public safety spectrum to serve commercial subscribers while allowing the public safety partner access to both the public safety spectrum and commercial spectrum in the rare emergencies when it is needed.

In August 2007, in the wake of an innovative proposal (Cyren Call Communications, 2006), the FCC (2007) licensed 10 MHz of 700 MHz spectrum nationwide to a single representative of public safety specifically for broadband use. Later, in February 2008, the FCC (2008a) auctioned a nationwide 10 MHz commercial license for the spectrum adjacent to the public safety allocation. The winner of this commercial license would have been obligated to build a nationwide public-safety-grade network in exchange for access to the 20 MHz of combined spectrum (Federal Communications Commission [FCC], 2007). This auction concluded without a winning bidder, which can be attributed, at least in part, to the considerable uncertainty about the requirements that would be placed on the network (Peha, 2008; Public Safety Spectrum Trust [PSST], 2007) and has led the FCC (2008b, 2008c) to consider changes to the rules that were attached to the commercial block of spectrum before it is re-auctioned.

The substantial uncertainty surrounding the cost of a nationwide public-safety-grade network is a significant impediment to its deployment. Thus, this work addresses the following two fundamental questions: (1) what will a nationwide wireless network for public safety cost with each of the two approaches under consideration, and (2) what impact do system characteristics and policy approaches have on this cost? By understanding these costs better and understanding what factors have the greatest impact on them, we can better enable policymakers to determine if any of

[1] Existing systems can be patched together either by using gateways to bridge disparate networks or by using multiband radios that can operate on a range of frequencies and standards (Weiser & Hatfield, 2007).

[2] Project 25 is a narrowband wireless technology designed for public safety systems. One of its stated goals is to improve interoperability. Phase I of the Project 25 standard operates on 12.5 kHz channels enabling voice or low speed data service of approximately 10 kbps (Association of Public-Safety Communications Officials [APCO]).

[3] The fragmented approach to spectrum allocation has led to public safety spectrum being spread across 10 bands ranging from 20 to 4900 MHz (Desourdis et al., 2002; Doumi, 2006; Public Safety Wireless Advisory Committee [PSWAC], 1996).