Risk, Hazards & Crisis in Public Policy
www.psocommons.org/rhcpp/

On the Evolution of Wireless Communication Technologies and Spectrum Sharing for Public Safety: Policies and Practice

Naim Kapucu, Brittany Haupt, Murat Yuksel, Ismail Guvenc, and Walid Saad

The field of emergency and crisis management continuously strives to enhance collaboration, communication, and coordination among public safety organizations. Successful integration is challenging due to current policies and regulations. Moreover, policymakers must predict future needs. Regardless of the challenges, development and growth of a national public safety communication system is no longer a hopeless cause and is anticipated to mitigate challenges by enhancing security, dependability and fault tolerance, cost effectiveness, interoperability, spectral efficiency, and advanced capabilities. Although this national public safety communication system is in the process of being implemented by various local, state, and federal agencies, such adoption is voluntary and attributes to a disconnect between policies and stakeholders. This study reviews the evolution of public safety communication system and discusses benefits and challenges of a national system, the policies and regulations affecting wireless communication technologies and spectrum sharing, and the influence of evolving technologies.

KEY WORDS: wireless communication technology, spectrum sharing, public safety

Introduction

One key challenge for public safety systems revolves around wireless technology, spectrum sharing, and the disjointed infrastructure impeding the adoption of a national public safety communication system (Fantacci, Vanneschi, Bertolli, Mencagli, & Tarchi, 2009; Faulhaber, 2006; White House, 2013). Previous research and incidents have confirmed communication failures due to large- or small-scale disasters can lead to catastrophic consequences (Faulhaber, 2006; Kapucu, 2006; Manoj & Baker, 2007; Peha, 2006). This can, in turn, greatly influence the effective performance of a public safety communication system, which is already dependent upon national adoption along with timely, comprehensible, and adaptable communication for all stakeholders.

Published by Wiley Periodicals, Inc., 350 Main Street, Malden, MA 02148, USA, and 9600 Garsington Road, Oxford, OX4 2DQ.

Within the past decades, researchers and practitioners have continuously tackled the challenges of interworking local, state, and federal public safety systems to enhance security, dependability and fault tolerance, cost effectiveness, interoperability, spectral efficiency, and advanced capabilities (Peha, 2006). Although a national public safety communication system has been promoted, implementation is stunted due to voluntary participation and disconnects between policies and stakeholders (Habib & Mazzenga, 2008; Hallahan & Peha, 2008; Peha, 2006). This paper reviews the evolution of public safety communication and discusses benefits and challenges of a national system while addressing the following research questions: i) *What are the policies and regulations influencing wireless communication technologies and spectrum sharing?*; ii) *How do evolving technologies influence adoption of a national public safety communication system and affect wireless communication and spectrum sharing?*

Although earlier studies examined the benefits and potential challenges of implementing a nationally connected public safety system, such studies incorporated an idealistic overture and lacked detail regarding innovative technology and policy influences. Therefore, this article provides additional and up-to-date insight concerning implementation challenges of a national public safety communication system through a qualitative analysis of critical policies, wireless technologies, and spectrum sharing.

Evolution of Public Safety Communication

At its core, communication is the process of sending information over a medium (e.g., media, radio, and the internet), or channel, to a receiver for interpretation (Walker, 2012). As the communication process evolved from primitive smoke signals to innovative radio technologies utilizing the electromagnetic spectrum, societies attempted to capitalize on these innovations to inform and prompt specific responses. In terms of a particular policy framework, the Federal Emergency Management Agency (FEMA) worked with the Federal Communications Commission (FCC) to focus message distribution to those fitting within the following parameters:

1. Conditions of impending or actual nature that jeopardize public safety during times of civil emergencies.
2. Information relating to immediate safety of life issues or property protection, maintenance of law and order, or alleviation of human suffering and need along with combating of attacks.
3. Information essential to public activities for civil defense or additional government and relief agencies.
4. Information for Radio Amateur Civil Emergency Services training, drills, and testing.

Naturally, evolution in emergency preparedness activities influenced communication systems and processes. Catapulting policy adaptations, the terrorist attack of September 11, 2001 significantly increased priority of public safety and

wireless communication technologies. More specifically, the heightened use of the internet to disseminate disaster-related information led to critical research surrounding social media as a tool for public safety communication. The practicality of the internet and social media is continuously increasing due to its availability during all phases of a typical emergency management process. In fact, some researchers believe citizen involvement for spreading awareness is a necessity for today's society. However, the effectiveness of such involvement relies on high-speed wireless communication technologies (Black, Dietz, Stirratt, & Coster, 2014).

Additional influential policy adaptations at the beginning of the twenty-first century include Title XVIII of the *Homeland Security Act of 2002*, which renewed the vitality and focus of establishing the Department of Homeland Security's Office of Emergency Communications (OEC) to improve communication capabilities of first responders (Department of Homeland Security [DHS], 2014). The OEC developed the first version of the National Emergency Communications Plan (NECP). Since the first version, a standout development was the creation of the National Public Safety Broadband Network (NPSBN) and its development of wireless Internet Protocol-based technologies. Yet, these efforts are not sufficient to deploy a national public safety system overcoming interoperability and performance challenges.

The policy evolution continues with the *National Preparedness Goal* promoting shared responsibility across all sectors as well as a *Quadrennial Homeland Security Review* identifying threats with strong implications for national resilience and preparedness (DHS, 2014). An emphasis within the National Preparedness Goal is for the whole community to engage in prevention, mitigation, response, and recovery activities enhancing the capabilities of a secure and resilient nation (FEMA, 2016). One key initiative is the Operational Coordination translating into the establishment and maintenance of a unified coordination structure with policies to unite key stakeholders when executing core capabilities. Additionally, the National Response Plan (NRP) provides a national template for agencies to determine appropriate levels for federal involvement regarding domestic incidents (Kapucu & Garayev, 2012; Sylves, 2014). The layering of these plans and initiatives support harmonization and interagency management to handle incidents of significance. These incidents must meet criteria established within the Homeland Security Presidential Directive-5. In particular, the incident must include DHS and federal assistance along with multi-agency involvement and request to the President for incident management responsibilities (Kapucu & Garayev, 2012; Sylves, 2014).

In tandem with the NRP, the National Response Framework (NRF) begins with a core document providing a foundation composed of guiding doctrines for response, roles and responsibilities, and actions (Sylves, 2014). The next two layers of the framework include the grouping of resources and capabilities into Emergency Support Function annexes to support major functions during an incident (Kapucu & Garayev, 2012). The following layers detail support via administrative requirements along with procedures and responsibilities for

contingencies. Moreover, national planning scenarios provide strategic guidance and assist in operationalizing plans, defining national priorities and capabilities, and coordinating responses to high-consequence threat scenarios (Sylves, 2014).

Promotion of a National Communication Network for Public Safety

Regarding communication-specific roles and responsibilities, the FCC creates and administers policies regarding emergency communications along with its operability and interoperability of public safety communication systems and protection of existing infrastructure. The NECP incorporates five specific goals (DHS, 2014). The first relates to governance and leadership for the vision of enhancing coordination, planning, and decision making for public safety communications. The second relates to planning and procedures in terms of updating and improving communications and their readiness for dynamic environments. The third pertains to improving the abilities for responders to communicate and coordinate through exercise and training programs to understand available technologies and their gaps. Following this is to improve effectiveness of operations through coordination of communication resources, personnel, and capabilities across the entire community. The last is research and development focused on coordinating evaluation activities to support responders and unveil innovative capabilities.

The five goals of the NECP support three specific priorities for public safety communication. The first focuses on identifying and prioritizing areas for improvement in the emergency responders' Land Mobile systems. The second ensures emergency responders and government officials plan and prepare for the adoption, integration, and use of broadband technologies, including the planning and deployment of the NPSBN. The third focuses on enhancing coordination between stakeholders, processes, and planning activities across the emergency response community (DHS, 2014).

With thousands of independent wireless systems in current operation, a nationwide wireless broadband network may potentially address all of these shortcomings (Hallahan & Peha, 2011). In 2006, Peha reported the development of a nationwide wireless network under the supervision of the DHS to support law enforcement along with approximately 80,000 federal agents and officers. In addition, this Integrated Wireless Network projected more cost-efficiency and spectrum sharing. As of 2012, the Department of Justice ended the program due to evolving needs and the inability to address a broader scope along with budgetary issues. However, the U.S. Congress signed into law the Middle Class Tax Relief and Job Creation Act (Shapiro, Holtz-Eakin, & Bazelon, 2014). This act proposed the creation of a national First Responder Network (FirstNet) to generate and operate the first nationwide, high-speed wireless broadband network for public safety.

Slated to fulfill a recommendation from the September 11th commission, FirstNet is an independent authority within the U.S. Department of Commerce's National Telecommunications and Information Administration. The purpose of

this first-responder focused network is to provide broad wireless communications that cover all geographic areas, enable effective teamwork, enhance redundancy and resilience, and leverage needed access to spectrum (First Responder Network Authority, 2016).

To fund ventures of national communication systems, responsibility was transferred to the FCC to generate ways to reallocate spectrum and enable broadband systems to gain more access within the commercial market. This responsibility not only supports the generation of a national communication network, but it also allows the FCC to continue development of their main emergency communications components: (i) the 911 call processing and delivery system; (ii) the Emergency Alert System; and (iii) the radio/broadcast or television system (FCC, 2014). In addition, the FCC developed a National Broadband Plan (NBP) to strategize a 10-year implementation plan for a public safety broadband infrastructure (Manner, Newman, & Peha, 2010). The NBP was a proposed multi-faceted approach to understanding wireless infrastructure through several avenues. These include: (i) hardened Radio Access Network infrastructure that can enable a higher degree of coverage, resilience, and signal reliability; (ii) priority roaming on commercial networks for additional capacity and increased network resiliency; (iii) underground and in-building solutions for better coverage; and (iv) mobile technology for coverage during failures or remoteness (Manner et al., 2010). The collection of these services influences the broadband ecosystem in four ways:

1. Maximizing consumer welfare, investment, and innovation through policies designed for robust competition.
2. Encouraging competitive entry and network upgrades through government influences or controls to ensure management and efficient allocation.
3. Boosting the adoption and utilization as well as ensures affordability through reform relating to current deployment of universal service mechanisms.
4. Maximizing the benefits for various sectors through policy, standards, incentives, and law reform (FCC, 2010).

Although the FCC provides public safety agencies with flexibility in distinguishing spectrum usage, responsibility and control is primarily in the hands of local agencies (Liu, Guo, & Nault, 2014; Peha, 1998, 2006). A benefit of local control is the ability to match resources (e.g., tax dollars) to pressing needs; however, this comes at a cost as flexibility negatively affects spectral efficiency due to the independent transmitters and technology. Not only is flexibility an important aspect of spectral efficiency, but adaptability and interoperability of technology are as well (Jesuale, 2005).

A question raised is whether a centralized public safety system is the solution as opposed to a decentralized system. This is a challenging question to answer. A centralized system can be more efficient with regard to the integration and coordination of components along with increased interoperability (Dano, 2013; Liu et al., 2014). In addition, this type could outperform a decentralized system in terms of managing public safety networks. On the other hand, a decentralized

system is more flexible and adaptable to local needs and preferences achieving higher social welfare (Kapucu, 2006; Peha, 2006). Within a centralized approach to public safety systems, interoperability is typically promoted and projected to provide a higher quality-of-service (Miller, Granato, Feuerstein, & Ruffino, 2005); for example, interoperability challenges caused significant problems during the aftermath of Hurricane Katrina (Leavitt & Kiefer, 2006). However, such a system cannot completely address specific local needs and includes high costs to build a fully interoperable network (Liu et al., 2014; Peha, 1998, 2007; Rysavy, 2012; White House, 2013). In addition, there is an increased occurrence of spillover causing issues with interoperability equilibrium. Spillover occurs when one area receives more benefits from the system versus others within the network. With an estimated 40,000 to 45,000 cell sites, almost as much as Verizon or AT&T, the quality of interoperability will not only depend on effective use but management too (Manner et al., 2010). Nevertheless, political barriers should also be crossed to achieve interoperability for public safety communications (Mayer-Schönberger, 2005).

This centralized system could streamline public safety practices across the nation; however, its hierarchical component remains problematic. If one of the top nodes in the network fails, then the resulting isolation minimizes problem solving capabilities and resilience capacity (Kapucu, 2006). Although the hierarchical structure can establish control, allocate responsibilities, specify tasks, and gain efficiency and reliability, it does not adapt under dynamic conditions of large-scale disasters (Comfort & Kapucu, 2006). As it cannot be predicted how infrastructure failures will affect emergency management agencies, trust and reliance has been given to an Incident Command System (ICS), which is a centralized command and control structure incorporating five dimensions: command, operations, planning, logistics, and finance/administration (FEMA, 2015). ICS developed out of a cooperative program called Firescope, which addressed a need for fire suppression in California in the 1970s (Buck, Trainor, & Aguirre, 2006). This cooperative program became a critical disaster management tool leading to a series of rational bureaucratic principles to provide unified command and collaboration between local, state, and federal stakeholders (Buck et al., 2006; Hu, Knox, & Kapucu, 2014). However, the major challenges of ICS include the lack of flexibility and adaptive capability of the system in conjunction with the complex communication needs for all local, state, and federal actors (Hu et al., 2014; Liu et al., 2014).

In tandem with the ICS system, the Joint Planning and Execution Services, a component of the Department of Defense's IT system, provides an integral link between the overarching command system and the essential procedures, policies, and reporting structures needed to implement activities associated with emergency management (Defense Information Systems Agency, 2016). Through a secure framework, Joint Planning and Execution Services provides operators and logisticians a place to connect via real-time, network-centric, and web-based systems. The goal is to enhance execution capabilities and adaptive planning of human operators. Implementing this unique system hinges on

successful integration of varying communication technologies, networked infrastructure, security processes, and attention to the needs of diverse communities (Faulhaber, 2006; Habib & Mazzenga, 2008; Hu et al., 2014; Jaeger et al., 2007; Peha, 2006). In terms of dependability and fault tolerance, the key areas of concern include the ability for a national public safety communication system to cover all geographic areas, maximize capacity, and promote strategic infrastructure allocation while minimizing spectrum needs (Meissner, Luckenbach, Risse, Kirste, & Kirchner, 2002; Peha, 2006). In addition, communication infrastructure must be able to adapt to the needs of response agencies in regards to stationary (i.e., headquarters), semi-mobile (i.e., mobile command posts), and/or mobile actors (i.e., frontline personnel) (Meissner et al., 2002).

Evolving Technology and Spectrum Needs

To institute a national system and streamline current infrastructure, the start-up costs will be extremely high due to the small volume of currently fragmented public safety systems and a limited number of suppliers (Manner et al., 2010; Rysavy, 2012; Werbach & Mehta, 2014). For instance, as of April 2015, the Los Angeles City Council reported the suspension of the public-safety LTE network project due to issues with budget, negative perceptions from the community, and questions surrounding the benefits (Dano, 2015). This program was not to circumvent FirstNet, but their goals were similar. If anything, the program provided critical lessons learned for the FirstNet goals and objectives. A proposed and integral cost alleviating technique is through spectrum auctions to generate revenue or cancel out start up costs (FCC, 2010). One of the main areas of cost relates to spectrum sharing regulations and their impact on the effective and efficient utilization of wireless systems (Doyle & Forde, 2015; Government Accountability Office, 2012; Werbach & Mehta, 2014).

Historically, the government divided the radio spectrum into non-overlapping blocks which are then distributed via licenses (Peha, 1998). The current management system for spectrum sharing includes the Spectrum Access System (SAS) and the Emergency Response Interoperability Center. SAS is an avenue for spectrum allocation between commercial and federal entities while the Emergency Response Interoperability Center is a committee-based partnership to establish a common technical framework and process through issues of security and encryption, roaming and priority access, and more (Manner et al., 2010). More proactive and pervasive sharing of the spectrum are envisioned and regimes where sharing is the norm are being explored to increase the overall efficiency of spectrum usage as well as its availability for public safety communications (Yuksel, Guvenc, Saad, & Kapucu, 2016). Along with effectively managing spectrum, the FCC is responsible for regulatory decisions and these will affect the nation's economic infrastructure. For instance, technological needs will require wireless companies to raise prices as a way to manage demand and capacity needs (Shapiro et al., 2014). Moreover, the evolution of safety communication inadvertently led to spectrum congestion, especially within high traffic areas.

Modern communication technologies depend on taxpayers due to current regulations and policies (Hallahan & Peha, 2008; Liu et al., 2014). For alleviating costs, researchers developed general recommendations for policymakers, such as spectrum allocations, reassignments, and unlicensed usage. Other options touch upon sharing of wireless network infrastructure, cost changes of access structures, innovative spectrum-efficient technologies, and updating policies (Hu et al., 2014; Moore, 2010). Currently, the number of municipal governments within a county greatly affects the number of communications towers versus its size, population, and terrain (Peha, 2006).

Under this flexible yet competitive process, a key requirement for any sharing mechanism is the satisfaction of network performance under various operating conditions. Due to complex needs, Wang and Brown (2007) proposed a two-stage pricing combination. The first uses a sound static pricing policy to set specific levels of commercial traffic followed by an optimal dynamic policy for admission control. The benefits of such a combination includes efficient spectrum sharing without requiring additional availability, more stable revenue between commercial network and users, and an ability to adapt quickly if network conditions change (Wang & Brown, 2007). Although technology may be compatible with updated spectrum management policies, the constant evolution of the technology itself can cause a delay of integration (Peha, 2009). However, implementation of a nationwide system must overcome critiques of policymakers desiring to maintain the status quo alongside practitioners who are unable to streamline equipment with operational procedures and language (Peha, 2006).

In the current infrastructure, the United States is looking for ways to make spectrum more available for mobile use and other services involving wireless broadband technologies (Doyle & Forde, 2015; Fantacci et al., 2009). A common segment within the dialog focuses on secure connections within and between communication systems. In 2013, the White House released a memorandum regarding spectrum efficiency and operability to promote safeguarding between organizations for sensitive, classified, and proprietary data as well as assessment purposes. This is critical since implementation of a national system is a long-term commitment with varying costs, evolving needs, and influences from diverse jurisdictions ranging from personal, incident, jurisdiction, and extended area networks (Portmann & Pirzada, 2008). Moreover, effective collaboration and coordination hinges on public and commercial markets coming together for the common goal of enhancing public safety.

Despite many recent technological advances, a 2004 survey by the U.S. Conference of Mayors discovered more than 80 percent of participating cities could not communicate with FEMA and other public safety agencies due to interoperability issues. Moreover, 49 percent of cities reported connection issues with the state police and 44 percent issues with response and recovery (Brito, 2006). This lack of coordination is a major cause of the interoperability problem. There are over 50,000 public safety agencies in the United States from diverse jurisdictions, and obtaining voluntary participation from each agency is practically impossible. The connection issues between first responders and

emergency management practitioners often carry over, due to infrastructure and technological issues along with human error. First responders usually have several forms of communication devices to use, such as hand-held radios, mobile phones, laptops, and more. These devices not only allow for communication with diverse agencies on complex systems, but also increase the chance of errors in human command (Brito, 2006). Notable examples of technological issues related to interoperability consist of events such as September 11th, Hurricane Katrina, and the Oklahoma City Bombing. Inadequate radio equipment prevented verbal communication between federal, state, and local agencies and practitioners (Fu, 2011).

Another challenge of implementing a national public safety communication system is the ongoing evolution of technology. Adapting technology and creating flexible networks and applications require financial investment along with time to create, adopt, and implement. With the speed of technological advances surpassing policy and regulatory changes, there is a significant gap to address. Moreover, each disaster holds diverse characteristics influencing prediction, detection, and specific activities required for prevention, mitigation, response, and recovery. Therefore, supportive software for nationwide system must incorporate a dynamic process of information integration to navigate human and system interactions (Chiu et al., 2010). This complexity not only emphasizes the need for advanced capabilities of wireless technology, but also compounds the need for effective policies and timely dissemination of information before, during, and after emergencies (Manoj & Baker, 2007; Meissner et al., 2002).

To mitigate the scope, a network needs to anticipate the worst-case scenario and deploy response and recovery activities within and between a multi-layered public safety system (Abusch-Magder et al., 2007). Moreover, the network would require a fundamental shift in an organization's structural architecture from hierarchical and centralized approach to flat and distributed. For instance, the hierarchical structure became invalid once terrorists destroyed the communication center during the World Trade Center attacks. However, the inability to utilize the centralized system allowed smart phones to establish their significance. Individuals had to rely on their smartphone internet connections for mass communication due to the overloaded landline circuits in the New York City area (Fu, 2011). Some researchers investigated the diversity of research domains and technology solutions relating to public warnings believing a single technology for public awareness increases vulnerability as people need affirmation from several resources (Chiu et al., 2010).

Potential solutions for response networks ranged in debated directions in terms of radio technology (Lien, Jang, & Tsai, 2009; Mousa, 2012). The first approach is the utilization of third generation commercial mobile cellular wireless technologies, such as Evolution-Data Optimized (1x EV-DO) or Universal Mobile Telecommunication System (UMTS), as well as Wireless Fidelity (Wi-Fi) or Worldwide Interoperability for Microwave Access (WiMAX) technologies. With each solution, the benefits and limitations need to be addressed (FCC, 2016). For instance, WiMAX technologies allow for more extended coverage than existing

Wi-Fi systems along with dedicated spectrum for public safety. In addition, there would be fixed and mobile standards-based technologies that are compatible with commercial technology along with higher data support for diverse applications. Yet, WiMAX is not a feasible solution as it needs cutting-edge technology with consistent communication equipment that is compatible with commercial markets (FCC, 2016).

Another approach is to develop an air-interface technology specifically for emergency networks such as land mobile radio (LMR) or terrestrial trunked radio (TETRA). Engineers and academics propose using device-to-device (D2D) and peer-to-peer (P2P) communications to address concerns and increase the robustness of public safety systems and mobile services to breakdowns during disasters (Kumbhar, Koohifar, Guvenc, & Mueller, 2015; Lien et al., 2009; Mousa, 2012). D2D relies on close proximity to enhance quality of spectrum range and P2P utilizes WiFi-ready laptops and smart phones to sustain communication flow and coordination through supportive instant messaging, cellular social networking accounts, and voice-over-IP.

These advances also hinge on improving network connections for mobile interfaces. Through advances such as LTE, public safety agencies are able to tap into high performance radio technology with similar capabilities to utilizing a fixed network (Herndon Publishing, 2011). Although there is growing interest on regional levels, the goal is to have an integrated public and private network with commercial markets capable to connecting in to allow for more spectrum allocation and effective performance.

The deployment of these options hinges on the commercial technology's ability to increase its availability for public safety events while providing cost-efficient use of large-scale wireless networks, development of unique user-focused capabilities and services, and competitive interoperable solutions (Abusch-Magder et al., 2007). For instance, a proposal for development between the commercial market and public safety response agencies involves Cognitive Radio (CR), a spectrum management system with built-in intelligence that adapts to its environment (Di Benedetto, Cattoni, Fiorina, Bader, & De Nardis, 2015; Peha, 2009; Rysavy, 2012). Although idealistic in nature, CR would be able to make real-time, autonomous decisions increasing spectrum efficiency, and reducing burdens within a centralized management system (Di Benedetto et al., 2015; Somov, Rasheed, & Yedugundla, 2013). A critical benefit of CR would be its capability to find spectrum channels with minimal interference. The caveat is the inability to transition from unlicensed to licensed spectrum bands. In addition, identifying resources to balance the network may be dependent on game theory techniques to understand the players, actions, and utility functions within an existing public safety system operation (Somov et al., 2013).

The challenges of CR includes the inability to generate a flexible and adaptable system along with numerous, idealistic visions yet to come to fruition. Until a time during which technology allows for a network such as CR, researchers proposed a temporary solution of the 911-Now Network (see Figure 1) to assist in network development (Abusch-Magder et al., 2007). The process

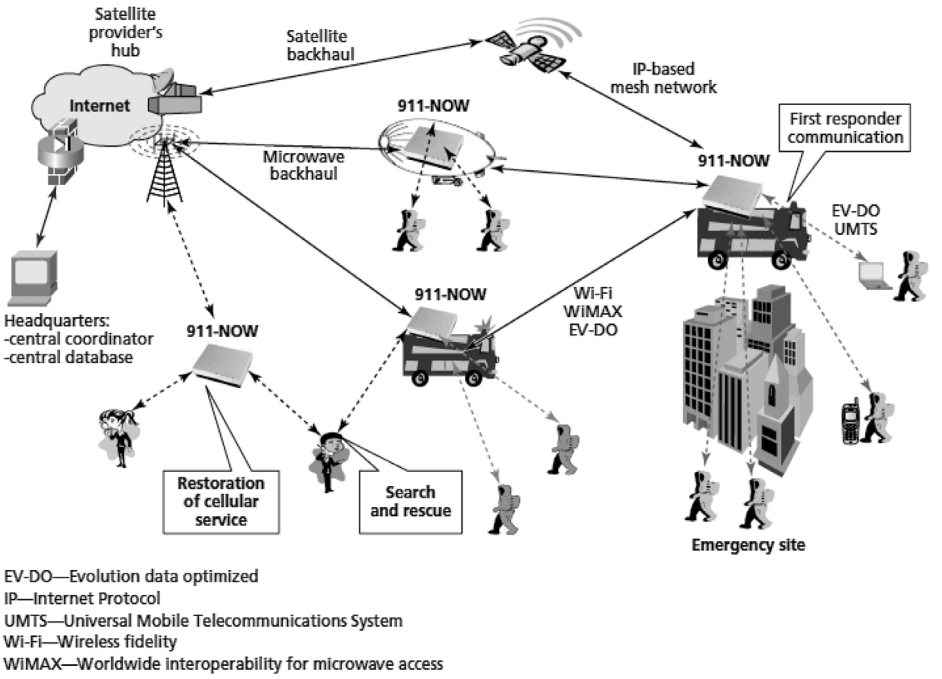

Figure 1. Adapted Visualization of the 911-Now Network (Abusch-Magder et al., 2007).

begins with an assurance of access and reliable communication anywhere and at any time followed by on-demand capacity and coverage for mobile incident area networks. This mobile network enhances local communication in the absence of any fixed network infrastructure and can integrate with previously deployed service architecture for a stand-alone network operation. The 911-Now Network would also provide cost-effective solutions, scalable and flexible to the emergency response, and the spatial and temporal network deployment scenario. Another benefit incorporates a wide area coverage through wireless mesh networking for deployment of jurisdictional area networks along with reliability and robustness through flexible multipath routing. The network also allows for wireless backhaul capabilities to a fixed private or public network and converges multimedia communication capabilities with voice, video, and high-speed data to enable increased situational awareness at the emergency site. Lastly, technological air interfaces are standards-compliant and support network interoperability through IP interfaces (Abusch-Magder et al., 2007).

As previously mentioned, integrating CR would allow for at least one reconfigurable radio component with parameters such as bandwidth. Although this is an idealistic venture, integration of a sensing engine would allow for the capability of accepting multiple inputs from radio components, such as networked nodes, data sources from the internet, and data-like geolocation. The system must also have a policy database to determine acceptable behavior within diverse circumstances. The complexity of this system lies in its dynamic

configurability and ability to learn, which allows for policy changes and inputs to determine appropriate configuration (Sherman, Mody, Martinez, Rodriguez, & Reddy, 2008). A specific example of CR integration is SmartRescue, which aims at using advanced sensors in smartphones to assist in acute crises. The data transmit through a mobile publish-subscribe (P/S) system enabling emergency management practitioners and the public to assess the hazard and understand location needs, as well as form a threat picture and user-centric evacuation plans (Radianti, Dugdale, Gonzalez, & Granmo, 2014). The challenge with this system is lack of available spectrum for urban areas, which is a significant obstacle for public safety, along with a compatible, flexible communication systems.

Similar to interoperability issues discovered during the terrorist attacks on September 11th and Hurricane Katrina, researchers noted drastic issues in utilizing similar technology and even being able to upgrade to needed devices. If some response agencies perform upgrades and others do not, then it interoperability increases interoperability making inter-agency communications virtually impossible (Manoj & Baker, 2007). In fact, researchers concluded that postponed or cancelled upgrades resulted in unplanned consequences during the September 11th attacks (Fu, 2011). Moreover, if some agencies implement new wireless communication systems and others do not, then, the issues will continue to occur. The plethora of issues to address, such as interoperability, security, lack of cognitive abilities, and connections, only amplify the demand for research from diverse knowledge domains. An additional aspect to explore consists of the rudimentary cognitive and connective capabilities within the current public safety system do exist and whether the existing standards lend themselves to cognitive abilities (Sherman et al., 2008). Lastly, the voluntary participation in the national communication system only aggravates the goal of unity. At some point, researchers, scientists, practitioners, and policymakers must come to a common space and bring their innovative resolutions to the table.

Conclusion

In the wake of every emergency, disruption between coordination of information, communication, and collaboration between response agencies leads to pressing issues. Since events like September 11, 2001, public safety planning has focused on enhancing collaboration, communication, and coordination among public safety organizations. Successful integration of plans such as the National Broadband Plan and the NECP is challenging and requires a great deal of time. Once strategic plans are in place, policymakers must predict future needs, like changes due to population and terrain, as well as gain access to spectrum and connecting infrastructure that will not inadvertently compromise public safety. Regardless of the challenges, development and growth of public safety communication systems is not a hopeless cause.

Within the development of a national system, there are a plethora of challenges related to the innovation and investment of wireless communication technology and spectrum sharing. However, the capability of wireless innovation

to succeed is dependent on the investment and cooperation among all sectors of the industry. Moreover, success hinges upon maintaining an interdisciplinary perspective and integrating this approach within policies and research. The ability to ensure effective spectrum sharing is a technical possibility for today's system; however, current inefficient use and operation increases risk of negative impacts. For instance, spectrum shortages lead to congestion periods causing first responders to delay communication or interrupt each other during response activities. Therefore, policymakers must ensure plans and regulations allow wireless technology innovations to thrive.

Naim Kapucu, Ph.D., is professor of public policy and director of the School of Public Administration at the University of Central Florida (UCF). His main research interests are network governance, emergency and crisis management, decision making in complex environments, and organizational learning and design. His work has been published in *Public Administration Review*, *Administration & Society*, *Journal of Public Administration Research and Theory*, *the American Review of Public Administration*, and *Disasters*, among many others. His recent book *Disaster Vulnerability, Hazards and Resilience,* was published in 2012 (with Rivera). He teaches network governance, public service leadership, emergency and crisis management, research methodology, and analytic techniques for public administration courses.

Brittany "Brie" Haupt, M.Ed., is a Graduate Research Associate at the UCF and studying for a Ph.D. in Public Affairs emphasis in Public Administration. Her research interests include the areas of cultural competency, emergency management communication, community resilience, and competency-based education. She has published in *Public Administration Review* and *Disaster Prevention and Management*, and presented at the American Society for Public Administration along with previous presentations centered on identity and development through her research efforts.

Murat Yuksel is an Associate Professor at the CSE Department of The University of Nevada—Reno (UNR), Reno, NV. He received M.S. and Ph.D. degrees in computer science of RPI in 1999 and 2002, respectively. He worked as a software engineer at Pepperdata, Sunnyvale, CA and a visiting researcher at AT&T Labs and Los Alamos National Lab. His research interests are in the area of networked, wireless, and computer systems with a recent focus on big-data networking, UAV networks, optical wireless, public safety communications, device-to-device protocols, economics of cyber-security and cyber-sharing, routing economics, network management, and network architectures. He has been on the editorial board of *Computer Networks*, and published more than 100 papers at peer-reviewed journals and conferences and is a co-recipient of the IEEE LANMAN 2008 Best Paper Award. He is a senior member of IEEE, senior and life member of ACM, and was a member of Sigma Xi and ASEE.

Ismail Guvenc (senior member, IEEE) received his Ph.D. degree in electrical engineering from University of South Florida, in 2006, with an outstanding dissertation award. He was with Mitsubishi Electric Research Labs during 2005, and with DOCOMO Innovations, Inc. between 2006 and 2012, working as a research engineer. Since August 2012, he has been an assistant professor with Florida International University. His recent research interests include heterogeneous wireless networks and 5G wireless systems. He has published more than 100 conference/journal papers and book chapters, and several standardization contributions. He co-authored/co-edited three books for Cambridge University Press, served as an editor for *IEEE Communications Letters* (2010–15) and *IEEE Wireless Communications Letters* (2011–present), and as a guest editor for several other journals. Dr. Guvenc is an inventor/coinventor in 23 U.S. patents, and has another four pending U.S. patent applications. He is a recipient of the 2014 Ralph E. Powe Junior Faculty Enhancement Award and 2015 NSF CAREER Award.

Walid Saad is an Assistant Professor at the Bradley Department of Electrical and Computer Engineering at Virginia Tech, where he leads the Network Science, Wireless, and Security (NetSciWiS) laboratory, within the Wireless@VT research group. His research interests include wireless and social networks, game theory, cybersecurity, and cyber-physical systems. Dr. Saad is the recipient of the NSF CAREER award in 2013, the AFOSR summer faculty fellowship in 2014, and the Young Investigator Award from the Office of Naval Research (ONR) in 2015. He was the author/co-author of three conference best paper awards at WiOpt in 2009, ICIMP in 2010, IEEE WCNC in 2012, and IEEE PIMRC in 2015. He is the recipient of the 2015 Fred W. Ellersick Prize from the IEEE Communications Society. Dr. Saad serves as an editor for the *IEEE Transactions on Wireless Communications*, *IEEE Transactions on Communications*, and *IEEE Transactions on Information Forensics and Security*.

Note

This material is based upon work supported by the National Science Foundation under NSF EARS grant numbers AST-1443946, AST-1443999, AST-1444077, AST-1506297 entitled Collaborative Research: Pervasive Spectrum Sharing for Public Safety.

References

Abusch-Magder, David, Peter Bosch, Thierry E. Klein, Paul A. Polakos, Louis G. Samuel, and Harish Viswanathan. 2007. "911-NOW: A Network on Wheels for Emergency Response and Disaster Recovery Operations." *Bell Labs Technical Journal* 11 (4): 113–33.

Black, David R., J. Eric Dietz, Amanda A. Stirratt, and Daniel C. Coster. 2014. "Do Social Media Have a Place in Public Health Emergency Response?" *Journal of Emergency Management* 13 (3): 217–26.

Brito, Jerry. 2006. "Public Safety Interoperability." *Regulation* 29 (3): 6.

Buck, Dick A., Joseph E. Trainor, and Benigno E. Aguirre. 2006. "A Critical Evaluation of the Incident Command System and NIMS." *Journal of Homeland Security and Emergency Management* 3 (3): 1–27.

Chiu, Dickson K. W., Drake T. T. Lin, Eleanna Kafeza, Minhong Wang, Haiyang Hu, Hua Hu, and Yi Zhuang. 2010. "Alert Based Disaster Notification and Resource Allocation." *Information Systems Frontiers* 12 (1): 29–47.

Comfort, Louise K., and Naim Kapucu. 2006. "Inter-Organizational Coordination in Extreme Events: The World Trade Center Attacks, September 11, 2001." *Natural Hazards* 39 (2): 309–27.

Dano, Mike. 2013. "The Looming Conflict Over Spectrum Sharing." *Fierce Wireless Tech* (June 21). Retrieved from http://www.fiercewireless.com/story/looming-conflict-over-spectrum-sharing/2013-06-21

———. 2015. "Updated: NTIA Suspends Funds for Los Angeles' Public-Safety LTE Network." *Fierce Wireless Tech*. Retrieved from http://www.fiercewireless.com/tech/story/losangelesofficialshaltpublicsafetyltenetworkcloudingfirstnetspro/20150402

Defense Information Systems Agency. 2016. *Joint Planning and Execution Services*. Retrieved from http://www.disa.mil/mission-support/command-and-control/JPES

Department of Homeland Security (DHS). 2014. *National Emergency Communications Plan*. Retrieved from http://www.dhs.gov/sites/default/files/publications/2014%20National%20Emergency%20Communications%20Plan_October%2029%202014.pdf.

Di Benedetto, Maria-Gabriella, Andrea Cattoni, Jocelyn Fiorina, Faouzi Bader, and Luca De Nardis. 2015. *Cognitive Radio and Networking for Heterogeneous Wireless Networks*. Switzerland: Springer International Publishing.

Doyle, Linda, and Tim Forde. 2015. "A Regulatory Perspective on Cognitive Radio and Spectrum Sharing." In *Cognitive Radio and Networking for Heterogeneous Wireless Networks*, ed. Maria-Gabriella Di Benedetto, Andrea Cattoni, Jocelyn Fiorina, Faouzi Bader, and Luca De Nardis. Switzerland: Springer International Publishing. 257–89.

Fantacci, Romano, Marco Vanneschi, Carlo Bertolli, Gabriele Mencagli, and Daniele Tarchi. 2009. "Next Generation Grids and Wireless Communication Networks: Towards a Novel Integrated Approach." *Wireless Communications and Mobile Computing* 9 (4): 445–67.

Faulhaber, Gerald R. 2006. "Solving the Interoperability Problem: Are We on the Same Channel—An Essay of the Problems and Prospects for Public Safety Radio." *Federal Communications Law Journal* 59: 493.

Federal Communications Commission (FCC). 2010. *National Broadband Plan*. Retrieved from https://www.fcc.gov/national-broadband-plan

———. 2014. *Emergency Communications Guide*. Retrieved from http://www.fcc.gov/public-safety

———. 2016. *Public Safety Tech Topics: WiMAX Applications for Public Safety*. Retrieved from https://www.fcc.gov/help/public-safety-tech-topic-11-wimax-applications-public-safety

Federal Emergency Management Agency (FEMA). 2015. *Disaster Emergency Communications Division*. Retrieved from http://www.fema.gov/disaster-emergency-communications-division

———. 2016. *National Preparedness Goal*. Retrieved from https://www.fema.gov/national-preparedness-goal

First Responder Network Authority. 2016. *Guiding Principles*. Retrieved from http://www.firstnet.gov/about/guiding-principles

Fu, Laura. 2011. "The Government Response to 9/11: Communications Technology and the Media." *Library & Archival Security* 24 (2): 103–18.

Government Accountability Office (GAO). 2012. *Spectrum Management: Incentives, Opportunities and Testing Needed to Enhance Spectrum Sharing (GAO 13-7)*. Retrieved from http://www.gao.gov/assets/660/650019.pdf

Habib, Ibrahim, and Franco Mazzenga. 2008. "Wireless Technologies Advances for Emergency and Rural Communications." *IEEE Wireless Communications Magazine* 15 (3): 6–7.

Hallahan, Ryan, and Jon M. Peha. 2008. "Quantifying the Costs of a Nationwide Broadband Public Safety Wireless Network." 36th Telecommunications Policy Research Conference. Retrieved from http://repository.cmu.edu/cgi/viewcontent.cgi?article=1039&context=epp

———. 2011. "The Business Case of a Network That Serves Both Public Safety and Commercial Subscribers." *Telecommunications Policy* 35 (3): 250–68.

Herndon Publishing. 2011. 4G is Here: LTE and WiMAX Take Public Safety Communications Into the Future. Retrieved from http://www.hendonpub.com/resources/article_archive/results/details?id=1457

Hu, Qian, Claire Connolly Knox, and Naim Kapucu. 2014. "What Have We Learned since September 11, 2001? A Network Study of the Boston Marathon Bombings Response." *Public Administration Review* 74 (6): 698–712.

Jaeger, Paul T., Ben Shneiderman, Kenneth R. Fleischmann, Jennifer Preece, Yan Qu, and Philip Fei Wu. 2007. "Community Response Grids: E-government, Social Networks, and Effective Emergency Management." *Telecommunications Policy* 31 (10): 592–604.

Jesuale, Nancy. 2005. "Overview of State and Local Government Interests in Spectrum Policy Issues." In *New Frontiers in Dynamic Spectrum Access Networks. First IEEE International Symposium*. 476–85.

Kapucu, Naim. 2006. "Interagency Communication Networks During Emergencies Boundary Spanners in Multiagency Coordination." *The American Review of Public Administration* 36 (2): 207–25.

Kapucu, Naim, and Vener Garayev. 2012. "Designing, Managing, and Sustaining Functionally Collaborative Emergency Management Networks." *The American Review of Public Administration* 1–19. DOI: 0275074012444719

Kumbhar, Abhaykumar, Farshad Koohifar, Ismail Guvenc, and Bruce Mueller. 2015. "A Survey on Legacy and Emerging Technologies for Public Safety Communications." *arXiv preprint arXiv:1509.08316*. 1–22.

Leavitt, William M., and John J. Kiefer. 2006. "Infrastructure Interdependency and the Creation of a Normal Disaster the Case of Hurricane Katrina and the City of New Orleans." *Public Works Management & Policy* 10 (4): 306–14.

Lien, Yao-Nan, Hung-Chin Jang, and Tzu-Chieh Tsai. 2009. "P2Pnet: A MANET Based Emergency Communication System for Catastrophic Natural Disasters." In *29th IEEE International Conference on Distributed Computing Systems Workshops*, Montreal.

Liu, Yipeng, Hong Guo, and Barrie R. Nault. 2014. "Centralized Versus Decentralized Provision of Public Safety Networks." *Technology* 1–27.

Manner, Jennifer A., Stagg Newman, and Jon M. Peha. 2010. "The FCC Plan for a Public Safety Broadband Wireless Network." *38th Telecommunications Policy Research Conference*. Retrieved from http://www.ece.cmu.edu/~peha/FCC_plan_for_public_safety.pdf

Manoj, Balakrishan S., and Alexandra Hubenko Baker. 2007. "Communication Challenges in Emergency Response." *Communications of the ACM* 50 (3): 51–3.

Mayer-Schönberger, Viktor. 2005. "The Politics of Public Safety Communication Interoperability Regulation." *Telecommunications Policy* 29 (11): 831–42.

Meissner, Andreas, Thomas Luckenbach, Thomas Risse, Thomas Kirste, and Holger Kirchner. 2002. "Design Challenges for an Integrated Disaster Management Communication and Information System." In *The First IEEE Workshop on Disaster Recovery Networks*, 24.

Miller, H. Gilbert, Richard P. Granato, John W. Feuerstein, and Louis Ruffino. 2005. "Toward Interoperable First Response." *IT Professional* 7 (1): 13–20.

Moore, Linda K. 2010. *Spectrum Policy in the Age of Broadband: Issues for Congress*. Collingdale, PA: DIANE Publishing.

Mousa, Anwar M. 2012. "Challenges of Future R&D in Mobile Communications." *International Journal of Advanced Computer Science and Applications* 3 (10): 1–10.

Peha, Jon M. 1998. "Spectrum Management Policy Options." *Communications Surveys, IEEE* 1 (1): 2–8.

———. 2006. From TV to Public Safety: The Need for Fundamental Reform in Public Safety Spectrum and Communications Policy. Retrieved from http://repository.cmu.edu/cgi/viewcontent.cgi?article=1022andcontext=epp

———. 2007. "How America's Fragmented Approach to Public Safety Wastes Money and Spectrum." *Telecommunications Policy* 31 (10): 605–18.

———. 2009. "Sharing Spectrum Through Spectrum Policy Reform and Cognitive Radio." *Proceedings of the IEEE* 97 (4): 708–19.

Portmann, Marius, and Asad Amir Pirzada. 2008. "Wireless Mesh Networks for Public Safety and Crisis Management Applications." *Internet Computing, IEEE* 12 (1): 18–25.

Radianti, Jaziar, Julie Dugdale, Jose J. Gonzalez, and Ole-Christoffer Granmo. 2014. "Smartphone Sensing Platform for Emergency Management." Proceedings of the 11th International ISCRAM Conference.

Rysavy, Peter. 2012. "Spectrum Sharing: The Promise and the Reality." *Wireless Spectrum Research and Development Workshop IV, MIT*, Cambridge, MA.

Shapiro, Robert J., Douglas Holtz-Eakin, and Coleman Bazelon. 2014. *The Economic Implications of Restricting Spectrum Purchases in the Incentive Auctions*. Retrieved from http://sonecon.com/docs/studies/EconImplicationsSpectrumAuctions.pdf

Sherman, Matthew, Apurva N. Mody, Ralph Martinez, Christian Rodriguez, and Ranga Reddy. 2008. "IEEE Standards Supporting Cognitive Radio and Networks, Dynamic Spectrum Access, and Coexistence." *Communications Magazine, IEEE* 46 (7): 72–9.

Somov, Audrey, Tinku Rasheed, and Venkata Kiran Yedugundla. 2013. "Power Control Game for Spectrum Sharing in Public Safety Communications." In *Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), IEEE 18th International Workshop*, 207–11.

Sylves, Richard. 2014. *Disaster Policy and Politics: Emergency Management and Homeland Security*. Thousand Oaks, CA: CQ Press.

Walker, Denise C. 2012. *Mass Notification and Crisis Communications: Planning, Preparedness, and Systems*. Danvers, MA: CRC Press.

Wang, Qi, and Timothy X. Brown. 2007. "Public Safety and Commercial Spectrum Sharing via Network Pricing and Admission Control." *Selected Areas in Communications, IEEE Journal* 25 (3): 622–32.

Werbach, Kevin, and Aalok Mehta. 2014. "The Spectrum Opportunity: Sharing as the Solution to the Wireless Crunch." *International Journal of Communication* 8: 22.

White House. 2013. *Expanding America's Leadership in Wireless Innovation*. Office of the Press Secretary. Retrieved from http://assets.fiercemarkets.net/public/newsletter/fiercewireless/whitehousememo.pdf

Yuksel, Murat, Ismail Guvenc, Walid Saad, and Naim Kapucu. 2016. "Pervasive Spectrum Sharing for Public Safety Communications." *IEEE Communications. Magazine* 54 (3): 22–9.