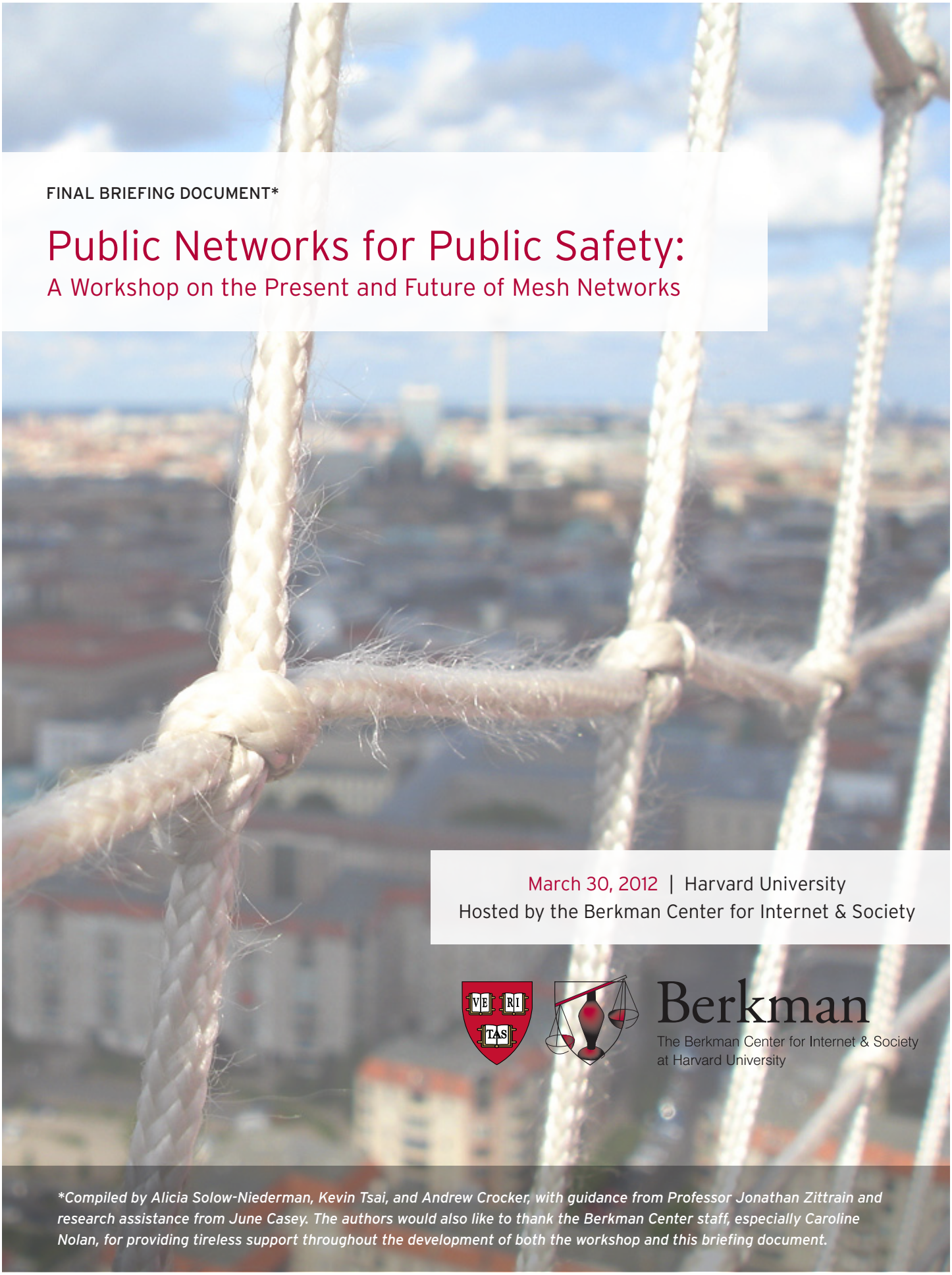

FINAL BRIEFING DOCUMENT*

Public Networks for Public Safety:

A Workshop on the Present and Future of Mesh Networks

March 30, 2012 | Harvard University
Hosted by the Berkman Center for Internet & Society

Berkman
The Berkman Center for Internet & Society
at Harvard University

Compiled by Alicia Solow-Niederman, Kevin Tsai, and Andrew Crocker, with guidance from Professor Jonathan Zittrain and research assistance from June Casey. The authors would also like to thank the Berkman Center staff, especially Caroline Nolan, for providing tireless support throughout the development of both the workshop and this briefing document.

Table of Contents

I. Document Background

This briefing document was developed in conjunction with "Public Networks for Public Safety: A Workshop on the Present and Future of Mesh Networking," which was held on March 30, 2012, at Harvard University. The workshop was intended as a starting point for conversation about whether mesh networks can and should be adopted within consumer technologies to enhance public safety communications and empower and connect the public as well as simultaneously improve public safety.

Attendees at the workshop included members of government agencies, academia, the telecommunications industry, and civil society organizations. The day began with a series of extended introductions and lightning talks, which laid out some of the key issues facing the use of mesh generally and its application to public safety communications in particular. Later sessions included an assessment of the current state of play for these applications, a presentation on social factors that affect community adoption of distributed networking technologies, and a taxonomy of the differences among a variety of decentralized networking technologies. After public safety officials reflected on the strengths and weaknesses of current public safety communication, the final session focused on translating insights presented at the workshop into a set of shared principles that could inform future efforts to advance the use of mesh—both as a networking technology and as a social construct—for public safety.

Building on the dialogue at this gathering, this briefing document seeks to:

- sketch a broad overview of mobile ad hoc networks (MANETs) and mesh technologies;
- identify critical technical issues and questions regarding the communications effectiveness of those technologies;
- explain how public safety communications relate to mesh and offer a synopsis of current regulations affecting those communications;
- describe a set of basic use cases that emerged from the conference
- map out stakeholders at the technical, regulatory, legal, and social levels, and associated interests, points of connection, and potential challenges;
- catalog select examples and, where possible, highlight potential next steps and areas for short term action; and,
- summarize key takeaways from the conference, with an emphasis on shared principles or best practices that might inform participants' diverse efforts to improve communications affordances for the public and the public safety community.

The latter portion of this paper aims to synthesize several strains of discussion that probed important framing considerations that could inform the present and future of mesh. Within the scope of this document, it is impractical to address all of the questions that emerged from our conversations. Therefore, we focus on two related but distinct models for mesh: mesh in a technical sense and mesh as a social layer construct, with an emphasis on the need for further conceptual development in regard to "social mesh." Section V of this paper addresses this framing issue in greater detail, aiming not only to continue the conversation about specific uses for and obstacles facing mesh (as either a technology or a social construct), but also to begin to assess conceptual challenges in this space. This analysis is continued in Section VI, Involved Parties and Potential Stakeholder Considerations, and Section VII, Mesh in the Intermediate Future. Finally, Section VIII offers key take-aways from the event. It highlights core principles and best practices that might both provide a theoretical underpinning for the future conceptual development of mesh networking technologies and social mesh models, respectively, and inform the real-world development of communications systems that involve either definition of mesh.

II. Overview

At present, the typical consumer receives wireless Internet service not from decentralized networks with distributed points of presence, but rather from wireless local area networks (WLANs) that rely on centralized distribution points controlled by commercial providers, such as an access point at a coffee shop or airport, or in one's own home. In this context, the consumer's device—whether it is a computer, a cellphone, or another device—is associated with a wireless access point that is connected to the Internet backbone through a wired connection controlled by an Internet Service Provider (ISP).[1] Under this model, consumer machines are end points, or terminal nodes in the network, that can only send and receive information via the ISP (see figure 1).[2]

Figure 1: An example of a traditional WLAN configuration.[3]

Mesh networks afford an alternative to this centralized "hub-and-spoke" WLAN model: rather than relying on the ISP for Internet connectivity, mesh technologies can produce ad hoc networks that allow distributed nodes to act as the senders, receivers, and conduits of information. In the mesh model of networking, " each user has the capability to receive and send information and to relay information on behalf of other connected computers."[4]

Mobile ad hoc networks represent a particular type of decentralized mesh network that contrasts with the WLAN model in several important ways. Unlike WLANs, MANETs "are mobile peer-to-peer networks that operate without the assistance of preexisting infrastructure."[5] MANETs can achieve intranet communication between connected devices without any reliance on the wired Internet backbone and allow any node in the network to access the Internet so long as a single node can achieve Internet connectivity. To provide such communications capabilities, instead of being connected by a single hop from the wireless router to the consumer's wireless device, user devices are connected to each other in a multihop environment in which a given device not only sends and receives information for its user, but also helps to route information between other devices and their users.

---

[1] Marius Portmann & Asad Amir Pirzada, *Wireless Mesh Networks for Public Safety and Crisis Management Applications,* IEEE Internet Computing, Jan. / Feb. 2008, at 19.

[2] Julian Dibbell, *The Shadow Web,* Sci. Am., Mar. 2012, at 63.

[3] Eusso, *54/108 Mbps Wireless Access Point,* http://www.eusso.com/Models/Wireless/GL2454-AP-QA/GL2454-AP.htm (last visited Mar. 8, 2012).

[4] Dibbell, *supra* note 2, at 63. For a visual representation that contrasts "traditional hub-and-spoke networks" created by connection through an ISP with the connectivity created in a decentralized mesh network, both during normal operations and in times of an ISP shutdown, see *id.* at 64.

[5] Jeffrey Andrews et al., *Rethinking Information Theory for Mobile Ad Hoc Networks,* IEEE Comm. Mag., Dec. 2008, at 94.

Wireless mesh networks (WMNs) are another type of wireless ad hoc network that utilize multihop connectivity to send and receive data. Wireless mesh networks are traditionally "built on a mix of fixed and mobile nodes interconnected via wireless links to form a multihop ad hoc network. ... [A] network of wireless routers forms a *wireless backbone*... which provides multihop connectivity between nomadic users and wired gateways."[6] So long as users are within range of the network, they can move around while their devices automatically reconfigure to find acceptable nodes to stay connected.[7]

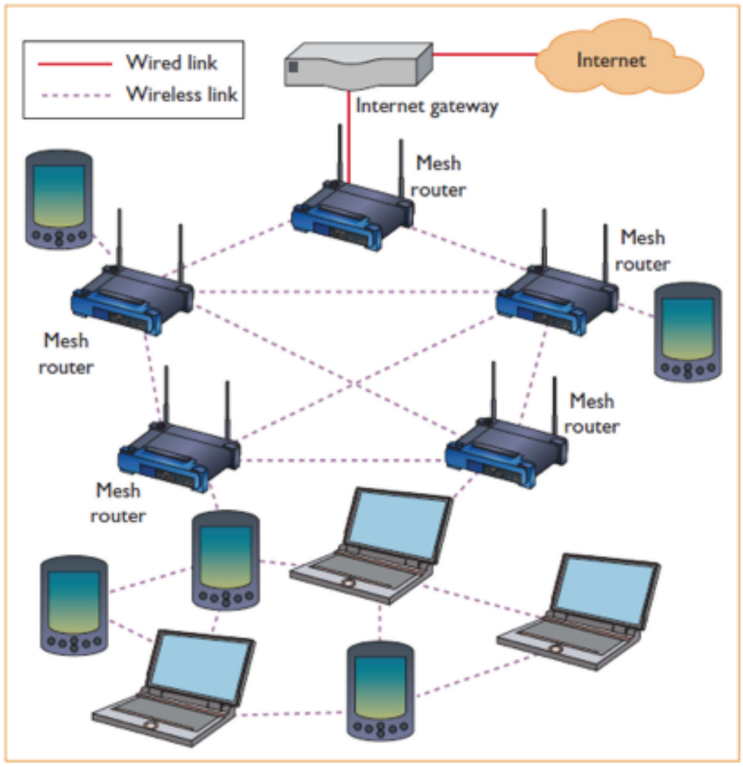

Figure 2: An example of a hybrid wireless mesh network (WMN).[8] The top half of the diagram depicts what is traditionally thought of as a mesh network created between wireless mesh routers. The bottom half of the diagram depicts mobile devices that are meshed together without any reliance on mesh routers to form a "client mesh." A network comprised of only the bottom half of the diagram would be a mobile ad hoc network (MANET).

WMNs offer a number of possible advantages over WLAN networks. Traditional WLANs require every wireless access point to be wired to the backbone, which both slows down hotspot[9] proliferation because no hotspot can exist until it is connected to the backbone infrastructure and is costly to build out because of the investments required to construct the necessary infrastructure.[10] WMNs mitigate this problem by reducing the number of access points that have to be physically cabled to the wired Internet backbone. Although the actual cost of WMN devices versus WLAN and cellular devices remains an open question, stakeholders motivated to cultivate a high-volume, low-cost ecosystem for WMN devices might deploy mesh technologies to drive down the costs of network deployment.

---

[6] Raffaele Bruno, Marco Conti & Entrico Gregori, *Mesh Networks: Commodity Multihop Ad Hoc Networks,* IEEE Comm. Mag., Mar. 2005, at 124, 125 [hereinafter Bruno, *Commodity Multihop*].

[7] *See* Jordan S. Hatcher, *Mesh Networks: A Look at the Legal Future,* 11.5 J. of Internet Law 12, 14 (Nov. 2007).

[8] Portmann, *supra* note 1, at 19.

[9] Bruno defines a hotspot as "an area that is served by a single WLAN or a network of WLANs, where wireless clients access the Internet through an 802.11-based access point." Please see Bruno, *Commodity Multihop, supra* note 6 for further discussion of hotspot installation and implementation.

[10] Bruno, *Commodity Multihop, supra* note 6, at 126.

Regulatory considerations also differentiate WLANs and WMNs. For instance, in cases that aim to achieve outdoor network coverage, laying cable to support a WLAN can require government involvement;[11] in contrast, communications via wireless ad hoc networks do not rely on such fixed backbone infrastructure and therefore are not subject to the same sort of regulatory oversight. It is important to note, however, that WMNs are not free from regulatory oversight. Depending on the purpose of the WMN and the frequency it employs, the network may be subject to licensing and frequency sharing requirements as part of larger regulatory control of a particular section of licensed spectrum.[12] Moreover, regulatory decisions may have an impact on wireless networks' overall range of propagation since policy choices can affect critical technical parameters such as power, frequency, allowable gain, and out of band emissions constraints.

In addition to such economic and regulatory considerations, WMNs offer several potential technical benefits. Compared to a WLAN's "hub-and-spoke" model of Internet access, in which each user's access point needs to reach a centralized ISP connection to access the Internet, WMNs can extend wireless Internet access because "multihop communications offer[] long distance communications via hopping through intermediate nodes."[13] Robustness is also an important potential benefit of WMNs. In a WLAN, communications effectiveness is dependent on fixed infrastructure; a device will lose connectivity if it cannot communicate with the wireless access point. A WMN, in contrast, is not as dependent on fixed infrastructure; the failure of an intermediate node can be overcome because devices can simply self-reconfigure by routing data through alternative nodes.[14] WMNs' ability to self-organize and self-heal makes them adaptable and resilient, rendering WMNs easier to deploy and maintain.[15]

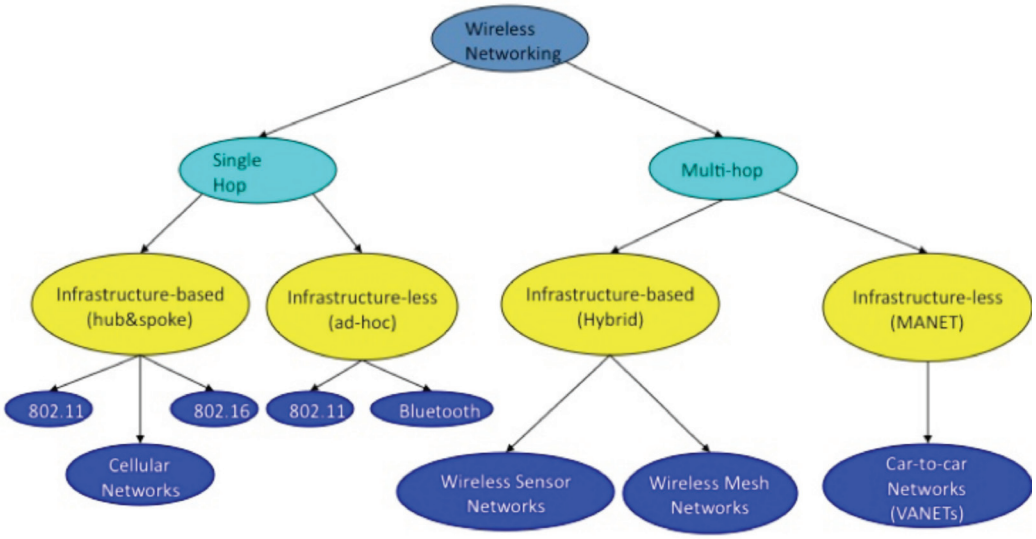

Figure 3: A taxonomy of mesh provided by conference participant Henning Schulzrinne of Columbia University and the FCC. This chart is adapted from the work of Mihail L. Sichitiu of North Carolina State University.[16]

---

[11] For instance, the Federal Communications Commission's (FCC) Wireline Competition Bureau regulates telephone pole attachment rules that affect the interactions between utility pole owners and telecommunications companies that want to attach broadband equipment to poles. See, e.g., Press Release, FCC, FCC Promotes Robust, Affordable Broadband by Reducing Costs & Delays in Access to Infrastructure (Apr. 7, 2011), *available at* http://hraunfoss.fcc.gov/edocs_public/attach-match/DOC-305620A1.pdf.

[12] *See 4.9 GHz Public Safety Spectrum,* Public Safety and Homeland Sec. Bureau, FCC, http://transition.fcc.gov/pshs/public-safety-spectrum/4-9GHz-Public-Safety-Band.html (last visited Apr. 7, 2012); *see also* 47 C.F.R. §§ 90.1201–1217 (2011).

[13] Bruno, *Commodity Multihop, supra* note 6, at 126.

[14] *Id.*

[15] Portmann, *supra* note 1, at 20 (noting, particularly, "easy and rapid deployment in an emergency").

[16] Professor Schulzrinne's presentation on the taxonomy of mesh networking can be downloaded at http://www.cs.columbia.edu/~hgs/papers/2012/2012-mesh.pptx. The original presentation by Professor Sichitiu from which Professor Schulzrinne's chart is adapted can be downloaded at http://www.ece.ncsu.edu/wireless/MadeInWALAN/wmnTutorial.ppt.

It is important to note that in real world deployments, WMNs also carry a number of technical issues. Such challenges, however, have not precluded various stakeholders from establishing WMNs. In the civil society sector, Aaron Kaplan's nonprofit community network FunkFeuer in Vienna, Austria, comprises over 200 user-owned, -installed, and -maintained nodes that provide high-speed Internet for its participants.[17] In Germany, the free mesh networking initiative Freifunk, co-founded by Juergen Neumann, provides service to a number of German municipalities, and its open source firmware has helped enable Internet service in Afghanistan, Ghana, and Vietnam.[18] Some of the largest community networks use a hybrid mesh and wired-backbone infrastructure and have exceeded node counts of 5,000 (the Athens Wireless Metropolitan Network in Greece) and 15,000 (Guifi.net in Barcelona).[19]

Although Europe has led the way in building out hybrid mesh networks at a large scale, there are many American projects that use mesh technology to provide wireless connectivity to communities. These include the Massachusetts Institute of Technology's Roofnet and Rice University's Transit Access Points (TAPs) projects, which have built WMNs covering limited areas for experimentation and the provision of consumer Internet service;[20] Purdue University's Mesh@Purdue project, which operates 32 nodes with the primary goal of providing Internet access;[21] and the Champaign-Urbana Community Wireless Network (CUWiN), which was founded in 2000 and provides free Wi-Fi to local residents.[22]

Beyond the use of WMNs for community wireless networks, WMNs have also been recognized for their potential for public safety applications because they are cheaper and easier to deploy than wired solutions.[23] Municipal government entities such as police departments and transportation agencies have installed WMNs to provide real-time video surveillance in cities including Cedar Rapids, Chicago, Dallas, Las Vegas, Los Angeles, and Phoenix.[24] A WMN in San Mateo and Milpitas, California, has helped police officers receive information from national databases in their vehicles so that they can stay in the field longer; an 8 square mile network in Ripon, California, is expected to save the police department at least $2,000 a month.[25] As WMNs mature, public safety data applications are likely to expand.[26]

Stakeholders are also investigating the potential use of mesh in the vehicular context. In its 2011 Report to the Secretary of Transportation, the U.S. Department of Transportation's Intelligent Transportation Systems Program Advisory Committee (ITS PAC) supported the development of safety applications for the deployment of vehicle-to-vehicle communications using consumer electronics.[27] Robin Chase, the founder of ZipCar and a veteran of the ITS PAC, believes that the "transportation sector is in a unique position to advance a common open platform for use, experimentation, and advancement of a mobile internet, as transforming and useful to

---

17 Dibbell, *supra* note 2, at 63.

18 *Freifunk wiki,* Freifunk.net, http://wiki.freifunk.net/Kategorie:English (last visited Mar. 17, 2012).

19 Dibbell, *supra* note 2, at 64.

20 Panayotis Antoniadis et al., *Community Building over Neighborhood Wireless Mesh Networks,* IEEE Tech. and Soc'y Mag., Spr. 2008, at 49. For more details on Roofnet, see Bruno, *Commodity Multihop, supra* note 6, at 127.

21 *Links to Other Mesh Networks,* UMIC-Mesh.net, http://www.umic-mesh.net/testbed/other_testbeds.html (last visited Mar. 17, 2012).

22 *Local Projects,* broadband.illinois.gov, http://www2.illinois.gov/broadband/Pages/Localprojects.aspx (last visited Mar. 17, 2012).

23 Brad Smith, *Mesh Helps Public Safety Keep an Eye Out,* Wireless Week, Feb. 1, 2008, at 20.

24 *Id.*

25 Naveen Lakshmipathy, *Wireless Public Safety Data Networks Operating on Unlicensed Airwaves: Overview and Profiles,* New Am. Found., Apr. 2007, at 4, 8. This article provides an excellent survey of several different wireless public safety data networks, with several mesh examples.

26 BelAir Networks, *Wireless Mesh Networks for Public Safety White Paper,* 2007, at 2 (identifying applications such as real-time broadcasting of critical alerts, mobile access to centralized databases like sex offender registries, mobile access to productivity applications, and mobile access to information while en route to an incident scene).

27 2011 Intelligent Transportation Systems Program Advisory Committee, *2011 Report to the U.S. Secretary of Transportation,* Nov. 28, 2011.

our economy as the internet itself."[28] Chase envisions buy-in from insurance companies (which could track, for instance, the location of stolen vehicles) and also suggests that ad hoc networks could enable the high-speed payment of tolls throughout the country.[29] Such applications could facilitate early adoption, even if the initial network were only able to handle small amounts of data with inconsistent connectivity.[30] Other researchers have also proposed innovations involving vehicular ad hoc networks and have suggested that WMNs could help reduce accidents and traffic jams by giving drivers important information while they are on the road.[31]

In addition, WMNs and MANETs have been recognized for their affordances in other unique contexts. For instance, the NGO *Télécoms san Frontières* has adopted mesh networks in emergency situations "to provide telecommunications infrastructure to disaster areas," establishing a connection to the wider Internet "through satellite or other means, and mesh[ing] together several nodes in order to extend the network coverage."[32] The Amateur Radio Service, which provides backup communications to public safety agencies and non-governmental relief agencies during times of emergency and or disaster, has been experimenting with mesh since 2003. Using amateur frequencies licensed from the FCC, Amateur Radio operators have created mesh routers with high-gain antennas, which can be deployed rapidly in an emergency.[33] Mesh has also been suggested in other use cases, including post-accident communication in mines;[34] in hospitals to track patient health;[35] and in environmental data monitoring to alert individuals and public safety officials when environmental readings exceed defined thresholds.[36] Without discounting these successes or the possibilities captured by nascent experimentation, it is still important to recognize that the WMNs that have been built out to date in both the community wireless and the public safety context have largely relied on a fixed infrastructure, frequently used proprietary nodes, and generally have not focused on mobile or ad hoc networking.

---

[28] Robin Chase, *Vision Statement for an Open Source Mobile Mesh Platform,* U.S. Dept. of Transp. Roundtable on the Possible Use of Mesh Networks, May 2008.

[29] *Id.*

[30] *Id.* (noting that while an initial open source mesh platform would be initially deployed with devices in cars, it could eventually be made useful with any mobile device).

[31] Antanas Vindasius & Sarunas Stanaitis, *Analysis of Emergency Message Transmission Delays in Vehicular Wireless Mesh Network,* 2010 Third Int'l Conf. on Advances in Mesh Networks, 2010, at 35 (noting, however, that researchers must consider effective broadcasting methodologies in designing vehicular mesh, since delays in transmission tend to grow in longer node chains).

[32] Hatcher, *supra* note 7, at 14. For research into enhancing satellite-public safety applications, see C. Bonnet et al., *A Mobile Ad-hoc Satellite and Wireless Mesh Networking Approach for Public Safety Communications,* 10th Int'l Workshop on Signal Processing for Space Comm., 2008.

[33] At the conference on March 30, 2012, Mike Corey of the American Radio Relay League (ARRL) provided an overview of Amateur Radio experimentation involving mesh technologies and provided a background document that is on file with the authors. As Corey explains, "Around 2003, Amateur Radio operators began experimenting with mesh networking. Through modifications made to commercially available 2.4 GHz wi-fi routers, Amateurs [sic] Radio operators were able to limit the frequencies the router uses to frequencies within the Amateur Radio spectrum. Once the modification was done, the routers could be configured into a mesh network. The range of the network is increased through use of high-gain antennas and careful positioning of the nodes in the network. The Amateur Radio version of mesh networking has unofficially been called high-speed multimedia mesh networking or HSMM mesh. Utilizing HSMM mesh, Amateurs can provide another level of communications support to served agencies."

[34] Souryal et al., *Simulation of a Medium Frequency Mesh Network for Communications in Underground Mines,* Industry Applications Soc'y Annual Meeting (IAS), 2010.

[35] Kevin Miller & Dr. Suresh Sankaranarayanan, *Monitoring Patient Health using Policy based Agents in Wireless Body Sensor Mesh Networks,* 2009 World Congress on Nature & Biologically Inspired Computing, 2009, at 503.

[36] Morreale et al., *Real-Time Environmental Monitoring and Notification for Public Safety,* IEEE Multimedia, Apr.–Jun. 2010, at 4.

III. Critical Challenges to the Communications Effectiveness of Mesh Networking Technologies

While mesh technologies appear promising, they remain subject to a number of technical issues that may impede their communications effectiveness. These issues cover a range of areas, but generally arise from the relative newness of wireless mesh technologies as compared to the legacy of wired Internet communications. A few of the major obstacles that face the present and possible future of mesh technologies are surveyed below; challenges include routing issues, resource management issues, quality of service (QoS) problems, security concerns, and battery life constraints.

Routing Issues

One of the key issues related to mesh networks is that routing protocols that were developed for the wired Internet are not suitable for ad hoc wireless technologies. Routing (identifying the sender-receiver path) and forwarding (delivering data packets along the sender-receiver path) are especially complicated in MANETs because such networks are by their very nature more dynamic and more complex to navigate than one-hop networks. Legacy routing methodologies that pre-compute minimum-cost paths by using predetermined paths—a relatively simple task in a wired system—can be particularly ineffective in the wireless environments that characterize MANETs because these ad hoc networks are inherently less static and less predictable.[37] This is an important issue because the routing protocol's effectiveness in choosing the right network paths under dynamic network conditions helps to determine the reliability and performance of wireless multihop communications,[38] and an inability to determine the best route impedes the communications effectiveness of the technology.

To surmount this routing problem, researchers have emphasized the need for approaches that are better suited to the broadcast nature of wireless.[39] However, despite significant research into routing protocols for MANETs, there is no consensus around a single routing standard. Multiple routing protocols, including the Optimized Link State Routing (OLSR) protocol,[40] the Better Approach to Mobile Ad-Hoc Networking, popularly known as the B.A.T.M.A.N. protocol,[41] and the LifeNet protocol,[42] are currently under development.[43] The lack of a single MANET-adapted routing standard effectively means that different mesh-enabled devices speak different languages and may not be able to communicate with each other.

Notably, organizations concerned with Internet standards have responded to this issue by attempting to develop a coordinated mesh routing protocol. Specifically, the Institute of Electrical and Electronics Engineers (IEEE) 802.11 Working Group, charged with developing WLAN standards, has been working to define a mesh routing protocol since 2003.[44] In July 2011, IEEE P802.11 Task Group S published an amendment for mesh

---

[37] Raffaele Bruno & Maddalena Nurchis, Survey on Diversity-Based Routing in Wire*less Mesh Networks: Challenges and Solutions,* 33 Computer Comm. 269, 270 (2010) [hereinafter Bruno, Diversity-Based Routing].

[38] *Id.* at 269.

[39] *Id.*

[40] *See olsrd — about,* OLSRD — an adhoc wireless mesh routing daemon, http://www.olsr.org/?q=about (last visited Mar. 24, 2012).

[41] *See Open-mesh WikiStart,* openmesh.org, http://www.open-mesh.org/projects/open-mesh/wiki (last updated Feb. 09, 2012).

[42] *See About LifeNet,* LifeNet, http://thelifenetwork.org/about.html (visited Mar. 24, 2011). LifeNet, which was co-created by workshop participant Dr. Santosh Vempala, is a flexible routing protocol specifically designed for mobile nodes. *See also* Hrushikesh Mehendale, Ashwin Paranjpe & Santosh Vempala, *LifeNet: A Flexible Ad hoc Networking Solution for Transient Environments,* SIGGCOMM'11, *available at* http://conferences.sigcomm.org/sigcomm/2011/papers/sigcomm/p446.pdf.

[43] *Homepage - Wireless Battle of the Mesh,* Wireless Battle Mesh, http://battlemesh.org/ (last updated Mar. 10, 2012); *see also* Marco Conti & Silvia Giordano, *Multihop Ad Hoc Networking: The Theory,* IEEE Comm. Mag., Apr. 2007, 78, 80.

[44] *IEEE 802.11s,* Wikipedia, http://en.wikipedia.org/wiki/IEEE_802.11s (last visited Mar. 24, 2012).

networking[45] that "describes a suite of protocols that allows IEEE 802.11s-capable devices to operate in a mesh, multi-hop network topology."[46] However, since this protocol has taken eight years to develop, a number of other routing protocols have proliferated in the interim; it remains to be seen how its publication may affect the broader mesh ecosystem.

The Internet Engineering Task Force (IETF) has also established a MANET working group to establish both a reactive and a proactive MANET protocol.[47] At present, no single routing protocol dominates the mesh landscape. Although companies do produce WMN products based on 802.11 hardware, many of these products use proprietary mesh protocols for routing and network configuration, which limits interoperability between different devices and systems.[48]

Resource Management

To enable decentralized communications, WMNs require a sophisticated coordinated multihop resource management algorithm. Although resource management algorithms are important for many reasons, fairness and network throughput present particularly challenging issues. Specifically, without a resource management algorithm that values fairness in provision of service, mesh nodes that are closer to a wireless gateway are likely to transmit more information than nodes that are farther away because more distant nodes have to go through a transmission and queuing delay at each intermediate node.[49] Moreover, network throughput suffers significantly if each node is given sufficient time to transmit notwithstanding distance.[50] These resource management challenges not only impede the actual communications effectiveness of multihop ad hoc networks, but also may have a negative effect on the adoption of such technologies. If users feel like they will not be getting a fair share of network resources and fear they cannot rely on the network when they are not sufficiently close to other nodes, then they may fail to adopt a decentralized network solution despite any benefits it might

For WMNs like those described in Section II, capacity can be calculated theoretically based on the geographical area covered, the number of Internet gateways, the number of nodes, and the kind of antennas used.[51] In real world deployments, however, speed and capacity can vary substantially. Community WMNs have begun to produce data on typical users' experiences, and open publication of more real-world data could be the first step in assessing and addressing resource management challenges.

---

[45] *IEEE P802.11s – Task Groups – Meetings Update: Status of Project IEEE 802.11,* IEEE, http://www.ieee802.org/11/Reports/tgs_update.htm (last visited Mar. 24, 2012).

[46] Press Release, IEEE, IEEE Publishes the IEEE 802.11s Amendment (Oct. 10, 2011), *available at* http://standards.ieee.org/news/2011/80211s.html; *see also Quick Guide to IEEE 802.11 WG & Activities,* IEEE 802 (Mar. 8, 2012), http://www.ieee802.org/11/QuickGuide_IEEE_802_WG_and_Activities.htm.

[47] *Mobile Ad-hoc Networks (manet) Description of Working Group,* Internet Engineering Task Force, http://datatracker.ietf.org/wg/manet/charter/ (last visited May 17, 2012).

[48] Portmann, *supra* note 1, at 20. Proxim's AP-4000M Wi-Fi Mesh is an example of a mesh product that pairs 802.11 with its own Orinoco Mesh Creation Protocol. *See* Ronen Isaac, *Wireless Mesh Hardware Comparison: Cisco, Motorola, Proxim, Strix Systems,* Continental Computers / wlanmall.com (Sept. 14, 2007), *available at* http://www.wlanmall.com/media/article/WLANmall-Mesh-Summary.pdf.

[49] Jason B. Ernst & Mieso K. Denko, *The Design and Evaluation of Fair Scheduling in Wireless Mesh Networks,* 77 J. of Computer and Sys. Sci. 652, 653 (2011).

[50] *Id.*

[51] Jangeun Jun and Mihail L. Sichitiu, *The Nominal Capacity of Wireless Mesh Networks,* IEEE Wireless Comms., Oct. 2003 at 8–14; Jun Zhang and Xiaohua Jia, *Capacity Analysis of Wireless Mesh Networks with Omni or Directional Antennas,* IEEE INFOCOM 2009, Apr. 2009, at 2881–2885.

Quality of Service (QoS)

QoS technologies aim to provide predictable and stable network performance, an important factor in assessing the current and future viability of the network. In the case of decentralized networks, routing and resource management issues can exacerbate inherent QoS problems for mesh technologies. For instance, to ensure consistently high QoS "when mobile clients move from the coverage of one mesh router to another, the client's communication sessions must be handed over from one mesh router to the next—that is, the packets the client sends and receives must be redirected via the new mesh router."[52] However, especially if the mobile client is moving at a high speed, these handoffs may not occur smoothly because there is "currently no standard way to transparently and seamlessly achieve this handover in a WMN."[53] This issue is amplified in the context of public safety communications, where strict QoS requirements make it all the more important that handoffs are handled efficiently, with no packet loss.[54] Traditional MANET routing protocols use a simple hop count mechanism, but this limitation can result in poor performance in the mobile ad hoc context.[55]

Additionally, current mesh networks do not efficiently utilize resources and depend on an over-provisioning of bandwidth and other resources. The lack of either comprehensive QoS support or efficient resource utilization constrains the willingness of network providers to build out large-scale WMNs.[56] Such issues are further complicated in an emergency situation that demands on-the-fly WMN deployments, a context in which the variability and unpredictability of wireless links can make adequate node placement challenging.[57]

Furthermore, potential interference when WMNs are operating on the popular unlicensed 2.4 and 5 GHz bands leads to additional frustrations with general QoS for mesh. QoS issues related to interference on unlicensed bands may prove especially problematic for public safety responders who rely on predictable and consistently high quality service in a variety of situations.[58] For public safety officials and private citizens alike, limitations on QoS also may prevent mesh from being able to offer advanced data, mobile, and video services.[59]

Security

Wireless networks as a whole are naturally more vulnerable to attack than wired networks because connectivity is accessible through the air.[60] This increased vulnerability both threatens communications effectiveness and undermines user trust in the technology. For example, although such attacks are not unique to mesh networks, one threat comes from man-in-the-middle attacks, in which a hostile adversary takes complete control of a communication link between legitimate parties and makes these parties believe they are communicating with one another when in fact the adversary controls the link, then proceeds to "inspect, inject, delay, delete, modify and re-order traffic to... bypass weak authentication protocols, hijack legitimate sessions, perform active traffic analysis and deny service."[61] Several different types of man-in-the middle attacks may occur as

---

[52] Portmann, *supra* note 1, at 22.

[53] *Id.*

[54] Ryan Wishart, Marius Portmann & Jadwiga Indulska, *Evaluation of Wireless Mesh Network Handoff Approaches for Public Safety and Disaster Recovery Networks,* Telecomm. Networks and Applications Conf., 2008, at 295.

[55] Portmann, *supra* note 1, at 23 (noting, however, that new routing mechanisms may help to solve this problem).

[56] George Vasilakis et al., *Business Opportunities and Considerations on Wireless Mesh Networks,* IEEE Int'l Symposium on Mobile and Multimedia Networks & Workshops, 2009, at 7.

[57] Portmann, *supra* note 1, at 24.

[58] *Id.*

[59] *See* BelAir Networks, *supra* note 26, at 8.

[60] Marius Portmann, *Wireless Mesh Networks for Public Safety and Disaster Recovery Applications,* in Wireless Mesh Networking: Architectures, Protocols and Standards (Yan Zhang ed., 2006), *available at* http://www.nicta.com.au/pub?doc=930.

[61] Stephen Glass, Vallipuram Muthukkumurasamy, & Marius Portmann, *Detecting Man-in-the-Middle and Wormhole Attacks in Wireless Mesh Networks,* Int'l Conf. on Advanced Info. Networking and Applications, 530, 530.

hostile agents target different networking layers.[62] Threats to a mesh network may also come from wormhole attacks, a type of man-in-the-middle attack in which two distant nodes in a network are connected to make stations at the ends of the wormhole appear to be neighbors, which in turn creates a false network topology that undermines network routing algorithms.[63] This tactic disrupts the flow of traffic, increases the probability that traffic will be routed through the attacker to nefarious ends, and makes it easier for the attacker to conduct further attacks undetected.[64] These kinds of security issues could be particularly problematic in a public safety context, where robust, reliable, and secure communications are essential. Solutions for securing the network layer of WMNs generally involve "cryptographically signed routing messages" in which secret keys are distributed using a variety of key management schemes.[65] However, effective, on-the-fly key management in ad hoc networks remains difficult, especially because it is highly dependent on network configuration.[66]

Battery Life

Battery life is a major concern for decentralized networks. MANETs are particularly power constrained compared to fixed networks,[67] a significant issue because power calibration is essential in allowing nodes to efficiently send and receive signals.[68] For any network model that involves commercial electronic devices, the limited battery life of these devices complicates transmission power calibration and also limits the amount of time a consumer device can serve as a node.

A 2009 mesh network testbed experiment provides sobering data on this issue: in the study, U.S. National Institute of Standards and Technology (NIST) researchers using a 3.7V 930mAh battery were only able to power an 802.11b/g Wi-Fi radio for one to two hours of active use.[69] While some more recently developed smartphones have a larger battery (the iPhone 4S, for example, has a 3.7V 1420mAh battery),[70] the testbed did not account for battery drain from consumers simultaneously using other applications on the same device. For infrastructure-based wireless networks, one extensively investigated energy management strategy has been to place user devices in a low power state, which means that they only intermittently send and receive messages in the network. However, this solution is not feasible in MANETs since the network relies on the devices themselves for connectivity; therefore, the fewer devices contributing actively to routing and forwarding, the more fragile the network.[71] At present, the high power cost to mobile devices serving as nodes may reduce the amount of time a network can remain connected.[72] This time constraint represents a major challenge to building out and maintaining networks that rely on ad hoc mobile nodes.

---

[62] See, e.g., Jaydip Sen., *Secure Routing in Wireless Mesh Networks, in* Wireless Mesh Networks (Nobuo Funabiki ed., 2011), *available at* http://arxiv.org/pdf/1102.1226.pdf, for a discussion of attacks on different layers of wireless mesh networks.

[63] *Id.*

[64] *Id.*

[65] Anne Marie Hegland et. al., *A Survey of Key Management in Ad Hoc Networks,* 8.3 IEEE Comms. Surveys & Tutorials 48 (Third Quarter 2006).

[66] *Id.* at 64.

[67] *See* Nagesh Nandiraju et al. *Wireless Mesh Networks, Current Challenges and Future Directions of Web-in-the-Sky,* IEEE Wireless Comm., Aug. 2007, 79, 80.

[68] *See, e.g.,* Peizhao Hu et al., *Evaluation of Commercial Wireless Mesh Technologies in a Public Safety Context: Methodology, Analysis and Experience,* IEEE 2010, 606.

[69] Michael R. Souryal, Andreas Wapf, & Nader Moayeri, *Rapidly-Deployable Network Testbed,* IEEE Global Telecomm. Conf., 2009, at 2.

[70] *iPhone 4 Teardown,* ifixit.com, http://www.ifixit.com/Teardown/iPhone-4-Teardown/3130/1 (last visited Mar. 14, 2012).

[71] Conti, *supra* note 43, at 81.

[72] *Id.*

Other Issues

In addition to these major challenges, researchers have looked into a number of other issues surrounding WMNs and MANETs, including:

- Interference measurement and modeling – understanding and accounting for broadcast interference;[73]
- Channel/radio assignment – assigning non-interfering channels to interfering links to increase spatial reuse;[74]
- Directional antenna limitations – directional antennas may increase range, but they reduce the number of nodes to which a given node can connect.[75]
- Omni-directional antenna limitations – broadcasting range for omni-directional antennas is limited and amplifiers may be of limited use in boosting range, as well as lead to other line of sight problems;[76]

During the conference, participants noted the possibility of using smart antennas and Multiple-Input Multiple-Output (MIMO) technology[77] to overcome some of the limitations detailed above regarding channel assignment and omnidirectional antennas. As wireless technology continues to proliferate and hardware becomes less expensive, it may be cost efficient to bundle multiple radios together to make mesh nodes more efficient. Participants also suggested that in an environment without MIMO technology, a smart antenna might not only reduce interference with another nearby node, but also reduce or even eliminate destructive multipath propagation, which is an important consideration for the communications effectiveness of ad hoc networks.

---

[73] Parth H. Pathak & Rudra Dutta, *A Survey of Network Design Problems and Joint Design Approaches in Wireless Mesh Networks,* 13.3 IEEE Comm. Surveys & Tutorials 396, 400 (Third Quarter 2011).

[74] *Id.* at 407.

[75] *Id.*

[76] Shaddi Hasan, *Why wireless mesh networks won't save us from censorship,* life and times of sha.hhid (Nov. 26, 2011, 8:02 PM), http://sha.ddih.org/2011/11/26/why-wireless-mesh-networks-wont-save-us-from-censorship/.

[77] *See* Jacob Sharony, IEEE LI, Introduction to Wireless MIMO – Theory and Applications 7–8, 13 (Nov. 15, 2006), *available at* http://www.ieee.li/pdf/viewgraphs/wireless_mimo.pdf.

IV. Public Safety Communications and Decentralized Networks

The early months of 2012 have witnessed dramatic changes in the public safety communications sector.[78] Confronted with limitations in traditional public safety communications such as those that hindered first responders on September 11, 2001, and in the aftermath of Hurricane Katrina, as well as potentially empowered by dramatic innovations in the commercial wireless industry,[79] a variety of actors across federal, state, and local legislative bodies and government agencies have been involved in discussions about the construction of a nationwide, interoperable wireless broadband network for public safety. Although the specifics of such a network are yet to be determined, it is clear that it will operate largely on specified public safety broadband spectrum using next-generation, Internet Protocol (IP) based systems.[80] Because the network's development and deployment will involve a considerable number of actors, questions regarding leadership, funding, technical standards, and coordination among stakeholders, in addition to specific questions about the shape and functionality of the network itself, remain open.

A. The Current State of Public Safety Communications

At present, public safety users rely on narrowband Land Mobile Radio (LMR) systems for their mission critical voice communications—such as the capability to dispatch first responders to emergency locations—which are essential to perform public safety's primary responsibilities.[81] LMR systems have evolved to meet the communications needs of several specific groups, the most significant of which are first responders (fire, police and emergency medical services), 9-1-1 call centers (known as Public Safety Answering Points or PSAPs), and other authorities in public safety agencies.[82] Specialized, redundant infrastructure has enabled LMR systems to be more resistant to natural and man-made disasters.[83] These systems take two forms: either "conventional," with dedicated, single-use channels for users or groups, or "trunked," with multiple channels devoted dynamically to groups of users.[84] In addition, they offer a number of features crucial for mission critical voice communications. These include:

- ***Direct Talk or Talk Around*** – when end users are out of range of the network, their devices can communicate peer-to-peer or peers-to-peers without infrastructure support;
- ***Push-to-Talk*** – instant or near-instant call setup at the push of a button with advanced features to avoid overlapping use;
- ***Group Talk*** – the ability to administer one-to-many communications, as with dispatcher support for field responders;
- ***Emergency Alerting/Priority Services*** – pre-established priority levels for hierarchical communications, with the ability to override priorities in an emergency;

---

[78] *See* Donny Jackson, *Obama makes it official, signs D Block legislation,* Urgent Comms., Feb. 23, 2011, http://urgentcomm.com/policy_and_law/news/obama-signs-dblock-law-20120223.

[79] *See* The White House, The Benefits of Transitioning to a Nationwide Wireless Broadband Network for Public Safety 1-3 (June 2011) (citing among innovations of consumer wireless competition in device market, innovative data and web offerings and explosion in number of subscribers), *available at* http://www.whitehouse.gov/sites/default/files/uploads/publicsafetyreport.pdf.

[80] *Implementing a Nationwide, Broadband, Interoperable Public Safety Network in the 700 MHz Band,* Third Report and Order and Fourth Further Notice of Proposed Rulemaking ¶18, 76 Fed. Reg. 10295 (proposed Jan. 25, 2011) (to be codified at 47 C.F.R. 90.18) [hereinafter FCC Order/FNPRM].

[81] Kenneth C. Budka, et. al, *Public Safety Mission Critical Voice Services Over LTE,* 16 Bell Labs Tech. J. 133 (2011).

[82] U.S. Gov't Accountability Off., First Responders: Much Work Remains to Improve Communications Interoperability 5, GAO-07-301 (Apr. 2, 2007), *available at* http://www.gao.gov/new.items/d07301.pdf [hereinafter GAO, First Responders].

[83] The White House, *supra* note 79, at 4.

[84] *See* GAO, First Responders, *supra* note 82, at 8.

- ***High-Fidelity Codecs*** – the ability to distinguish primary voice communications from ambient background noise; and
- ***Security*** – end-to-end encryption with the ability to distribute keys on the fly to a group.[85]

Although LMR systems are the backbone of mission critical voice communications for public safety, they have a number of drawbacks. They operate on fragmented frequencies licensed periodically by the FCC to various state, local, and regional agencies (a total of over 134,000 licenses)[86] that are independently responsible for maintaining the network and purchasing equipment out of their own budgets.[87] As a result, LMR systems and equipment from different agencies have long been limited in their ability to interconnect.

In an attempt to address such interoperability issues, some LMR systems and devices operate on a common set of standards called Project 25 (P25), which has been in development by a coalition of federal and public safety organizations since 1989. Its standards are intended to govern how LMR systems interconnect and provide services for roaming users,[88] as well as to ensure interoperability among devices produced by different manufacturers. However, P25 is voluntary for manufacturers and providers of LMR systems and equipment. Furthermore, in 2007, the Government Accountability Office determined that P25 adoption by state and local agencies had inadvertently led to concentration and higher prices in the equipment market without achieving satisfactory interoperability.[89]

Newer governmental initiatives such the Department of Homeland Security's SAFECOM project,[90] run by the Offices of Interoperability and Compatibility (OIC) and Emergency Communications (OEC), have been more successful at increasing interoperability among LMR systems, especially by creating shared definitions and standards used to determine funding.[91] Other important efforts to increase interoperability for LMR systems include the joint National Telecommunications and Information Administration (NTIA)-NIST Public Safety Communications Research (PSCR) program, which provides research, development, and testing of standards, and DHS's Emergency Communications Preparedness Center (ECPC), created by Congress in 2006 to improve interagency communications.[92]

In addition to interoperability issues, LMR systems are usually limited to mission critical voice communications; therefore, public safety agencies often supplement or "overlay" them with commercial or vendor-supplied broadband systems to implement other applications. At the level of the individual, although public safety officials use LMR systems for mission critical voice communications and very low speed data communications, most first responders also use a commercial cellular device for much of their day-to-day communications as well as a cellular data service such as a 3G modem with a laptop or "smart" handheld device for their data communications. However, unlike LMRs, these commercial systems used by agencies and individuals alike are generally not designed for use in emergency situations, and thus may be more vulnerable to bandwidth and resistance issues in disaster conditions.[93]

---

[85] *See* Budka et. al, *supra* note 81, at 134–35.

[86] U.S. Gov't Accountability Off., Emergency Communications: Various Challenges Likely to Slow Implementation of a Public Safety Broadband Network 7, GAO-12-343 (Feb. 22, 2012), *available at* http://gao.gov/assets/590/588795.pdf [hereinafter GAO, Emergency Communications].

[87] *Id.* at 7.

[88] Budka, et. al, *supra* note 81, at 137.

[89] GAO, First Responders, *supra* note 82, at 34.

[90] SAFECOM, http://www.safecomprogram.gov (last visited Mar. 6, 2012).

[91] *See generally* Off. of Interop. and Compat., U.S. Dep't of Homeland Security, Public Safety Statement of Requirements for Communications and Interoperability Vol. II. (Aug. 2008), *available at* http://www.safecomprogram.gov/library/Lists/Library/Attachments/302/Statement_of_Requirements_Volume_II%20-%20Version%201_2.pdf.

[92] Emergency Communications Act, Pub. L. No. 109-295, §671, 120 Stat. 1433, 1440 (2006).

[93] GAO, Emergency Communications, *supra* note 86, at 16.

B. Efforts to Build a Nationwide Public Safety Wireless Broadband Network

Against the backdrop of largely non-interoperable LMR systems operating in various sections of the wireless spectrum, efforts by the federal government to build a nationwide public safety broadband network have gained traction in the last five years. Initially, Congress approached the problems faced by the public safety communications sector by selectively reallocating choice spectrum in the 700 MHz band freed in the transition from analog to digital television to public safety; of note, the Balanced Budget Act of 1997 mandated allocation of 24 MHz in the 700 MHz band for public safety uses.[94] In 2007, the FCC's newly created Public Safety and Homeland Security Bureau (PSHSB) divided this spectrum into 12 MHz for narrowband uses (like LMR) and 10 MHz for broadband uses.[95] An adjacent 10 MHz block of spectrum known as the D Block[96] was designated for auction to private users, with the understanding that private licensees would share the spectrum with public users to create a nationwide broadband network for public safety. The 10 MHz dedicated solely to public broadband use was licensed to the Public Safety Spectrum Trust (PSST), a non-profit made up of public safety organizations that were to work in public/private partnership with the winner of the D Block auction to build the nationwide network.[97] This plan was accompanied by debates in Congress and among economists and network engineers regarding whether the proposed partnership would allow enough bandwidth for a robust public safety broadband network.[98] There was also disagreement about how much revenue such an auction would raise.[99] Ultimately, the D Block auction failed to meet revenue goals, and the project hung in limbo for several years.[100]

In the meantime, state and local public safety agencies began to petition the FCC for waivers of its rules to allow them to have early deployment of 700 MHz broadband public safety networks in their respective jurisdictions. Since 2010, the FCC has conditionally granted 22 such waivers. One stipulation for deployment of these networks has been the requirement that they be based on Long Term Evolution (LTE) standards.[101] As of March 2012, complete rules regarding the national broadband network have not been finalized.[102]

In the Middle Class Tax Relief and Job Creation Act of 2012 (Spectrum Act), signed into law by President Obama on February 22, 2012, the D Block spectrum was reallocated for dedicated public safety use, and the D Block as well as the existing public safety broadband spectrum will be licensed to a newly created entity, the First Responder Network Authority (FirstNet), to be housed within the NTIA. The Spectrum Act "establishes in the Treasury the Network Construction Fund for FirstNet to carry out its functions and the NTIA to make grants to states,"[103] thereby providing federal public safety agencies with at least $2 billion and up to $7 billion (contingent on revenues generated from spectrum auctions) to administer and oversee construction

---

[94] Pub. L. No. 105-33, §337 111 Stat. 253, 267 (1997) *available at* http://www.gpo.gov/fdsys/pkg/PLAW-105publ33/html/PLAW-105publ33.htm.

[95] FCC, *Implementing a Nationwide, Broadband, Interoperable Public Safety Network in the 700 MHz Band,* Second Report and Order 8, 22 FCC Rcd. 15289 (July 31, 2007), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-07-132A1.pdf.

[96] The D Block is actually two 5MHz blocks (uplink and downlink) adjacent to the previously dedicated public safety spectrum in the 700 MHz band. *See New Upper 700 MHz Band Plan,* Alliance for Innovation, http://transformgov.org/Images/full/Photo/Photo/100969 (last visited Mar. 15, 2012) (showing the 700 MHz allocation as envisioned by the FCC in 2007).

[97] GAO, Emergency Communications, *supra* note 86, at 8–9.

[98] *See* Donny Jackson, *Report: 10 MHz Not Enough for Public-Safety Broadband,* Urgent Comm., Oct. 11, 2011, at 6 (reporting on finding that 20MHz would be required to build broadband network).

[99] *See generally* George S. Ford & Lawrence J. Spiwak, *Public Safety or Commercial Use? A Cost/Benefit Framework for the D Block,* Phoenix Center Pol'y Bull. (Mar. 26, 2011), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1800065.

[100] FCC, *Order/NPRM, supra* note 80, at ¶13.

[101] *See* FCC, *Requests for Waiver of Various Petitioners to Allow the Establishment of 700 MHz Interoperable Public Safety Wireless Broadband Networks,* Order, 25 FCC Rcd. 5145 (Aug. 11, 2010).

[102] FCC, Order/NPRM, *supra* note 80, at ¶5; GAO, Emergency Communications, *supra* note 86, at 22.

[103] Cong. Res. Service Summary, Middle Class Tax Relief and Job Creation Act of 2012, H.R. 3630, 112th Cong., § 6202 (2012).

of the nationwide broadband network.[104] Under the terms of the Act, FirstNet is empowered to determine the architecture for this broadband network.

In another section of the 2012 Act, Congress allocated $115 million toward the implementation of so-called Next Generation 9-1-1 (NG9-1-1),[105] an ongoing effort to integrate "IP-enabled emergency services," including text and video, into 9-1-1 Public Safety Answering Points (PSAPs). The law reestablishes the 9-1-1 Implementation and Coordination Office (ICO), jointly run by the NTIA and the National Highway Traffic Safety Administration, to oversee the NG9-1-1 network.[106] NG9-1-1 was included as part of the FCC's 2010 National Broadband Plan, and the Commission opened a Notice of Proposed Rulemaking in September 2011 to accelerate its deployment.[107] In addition, as part of earlier NG9-1-1 efforts, the Department of Transportation built several proof of concept networks that incorporated IP-based services and envisioned an NG9-1-1 network that would incorporate legacy cellular and wireline phone and PSAPs as well as IP-based devices and systems.[108] Thus, under the 2012 legislation, the federal government is tasked with allocating funding for NG9-1-1 networks at the state and local level as well as determining the shape and capabilities of an NG9-1-1 network.

NG9-1-1 is motivated in part by the same factors spurring investment in the public safety broadband network: innovations in how consumers use telecommunications, which in turn require public safety organizations to adapt. The proportion of calls made to 9-1-1 from wireless devices has increased steadily as wireless subscribers increase,[109] and at present most 9-1-1 systems do not interact with common wireless applications, including text and video.[110] As with the public safety broadband network as a whole, NG9-1-1 involves an understanding of how new public safety technologies will impact and interact with other innovative technologies in the broader communications ecosystem.

C. The Future of Public Safety Communications

The recent Spectrum Act puts forth a trajectory that suggests the government will continue to focus on updating public safety communications, both for first responders and for civilian-facing 9-1-1 PSAPs (albeit with significantly more funding for the former group). With the resolution of the D Block reallocation and the establishment of FirstNet, several important steps have been taken toward the goal of achieving a nationwide interoperable public safety wireless broadband network. However, there are a number of challenges facing the full realization of this network as conceptualized by the law, including whether the initial $7 billion plus future revenues raised by spectrum auctions can provide sufficient funding to fully build the network, given that estimates of its total cost are on the order of $15 billion,[111] and whether the network will achieve nationwide interoperability given the legacy of current communications models.

---

[104] Pub. Law No. 112-96, §§6101-6303 and §§6206-6207 (2012), *available at* http://www.gpo.gov/fdsys/pkg/BILLS-112hr3630enr/pdf/BILLS-112hr3630enr.pdf

[105] Nat'l Emergency Number Ass'n, President Obama Signs Legislation Authorizing $115M for NG9-1-1 (Feb. 23, 2012), http://www.nena.org/news/84644/President-Obama-Signs-Legislation-Authorizing-115m-for-NG9-1-1.htm.

[106] Pub. Law No. 112-96, §6503 (2012).

[107] *See generally Framework for Next Generation 911 Deployment,* 76 Fed. Reg. 2297 (proposed Jan. 13, 2011) (to be codified at 47 C.F.R. 20).

[108] *See* Intelligent Transp. Sys., U.S. Dep't of Transp., *Next Generation 9-1-1 (NG9-1-1) System Initiative Final System Design Document* 1, 5 (Feb. 2009), http://www.its.dot.gov/ng911/pdf/USDOT_NG911_FINAL_System_Design.pdf.

[109] *See 9-1-1 Statistics,* Nat'l Emergency Number Ass'n, http://www.nena.org/?page=911Statistics (last updated 2012) (citing figure of up to one-half of 9-1-1 calls made wirelessly as of December 2008).

[110] *See* Julius Genachowski, Chairman, FCC, Remarks to APCO Annual Meeting (Aug. 10, 2011), *available at* http://transition.fcc.gov/Daily_Releases/Daily_Business/2011/db0810/DOC-309013A1.pdf *(citing challenges of updating 9-1-1 for smart phone applications). Conference participant Dr. Stagg Newman of Pisgah Comm Consulting has prepared a forthcoming report detailing the current state of NG9-1-1 and key policy issues facing its further implementation, which is on file with the authors.*

[111] GAO, Emergency Communications, *supra* note 86, at 29. For a comprehensive list of funding available for interoperable public safety networks, *see id.* at 44.

Finally, and perhaps most significantly, it is essential to consider how long it may take to build out a national public safety network that can provide the mission critical functions currently served by LMR systems and identify how best to meet those needs in the transition period. To take the specific case of LTE, which is one possible technological platform that FirstNet may select for the national broadband network, it may take 10 years or longer to achieve mission critical capabilities, and even then, certain functions—Direct Talk/Talk Around in particular—may not be well-suited to LTE at all.[112] Moreover, as one workshop participant noted, LTE network nodes may be lost in the face of natural or man-made disasters, and it is not yet clear what the geographic coverage of the network will be. As a result, public safety users might be forced to maintain two separate networks—one for voice and one for data—thereby continuing practices that have hindered interoperability in the past.[113] Since issues similar to those noted in the case of LTE may apply to other available platform options, it would be worthwhile to assess how decentralized wireless networks can mitigate these and any other limitations as FirstNet deploys the nationwide public safety broadband network. In particular, if the desire is to transition away from a communications model that relies on LMR systems, then one important open question is whether LMR spectrum might be repurposed to support mesh networks that supplement the developing public safety broadband network, although any such efforts might be limited by the T-band auction required by the Act.[114]

The ways in which these issues and other critical challenges are addressed will likely bear directly on the possible future of mesh in public safety communications. However, without many published resources on public safety and decentralized network technologies, it is difficult to specify how public safety communications might affect mesh and ad hoc mobile technologies beyond speculation about probable consequences, interactions, and affordances.

D. Public Safety Communications and Mesh

As suggested in the previous sections, the status quo for public safety communications is characterized by proprietary wireless spectrum, hardened fixed infrastructure, and costly, highly specialized user equipment. While public safety's mission critical functions may necessitate some of these characteristics, these attributes can also exacerbate the same interoperability issues that the nationwide broadband network seeks to alleviate.[115] Although legislative and regulatory interventions promise to do much to modernize public safety communications, involvement by other actors, especially industry, civil society, and academic stakeholders, might also help to overcome these hurdles. To the extent that decentralized networking solutions can expand the functionality of and enhance access to public safety communications during this moment of transition to next-generation technologies, WMNs and MANETs may be one aspect of a more diversified approach.

However, before discussing any possible affordances of these decentralized networks, it is essential to note how the recent move toward a nationwide broadband network also poses inherent difficulties for incorporating mesh technologies. Above all, concerns remain about the feasibility of mission critical and robust applications using mesh, and even mesh proponents acknowledge that MANET routing between end devices raise critical battery-life issues (see Section III for a more complete discussion of this and other engineering/technical hurdles to the communications effectiveness of mesh technologies generally and MANETs in particular).[116] In addition, the dedication of the 700 MHz spectrum to public safety use could limit the number of stakeholders who can participate in development of new technologies because of the closed nature of this new spectrum allocation. Significantly, such a model directly contrasts with more open models that have led

---

[112] GAO, Emergency Communications, *supra* note 86, at 22.

[113] *Id.* at 14; *see also* Budka et. al, *supra* note 81, at 140 (discussing theoretical dual-mode user device with LTE and LMR-style talk around services).

[114] See Pub. Law No. 112-96, §6103, *supra* note 104.

[115] See *supra* text accompanying note 89.

[116] Visiting Comm. on Advanced Tech., Nat. Inst. of Standards and Tech., U.S. Dep't of Commerce, Desirable Properties of a Nationwide Public Safety Communications System 11 (Jan. 24, 2012) *available at* http://www.nist.gov/director/vcat/upload/Desirable_Properties_of_a_National_PSN.pdf (hereinafter VCAT Report).

to widespread innovation (including mesh applications) in the unlicensed 2.4 and 5 GHz bands.[117] Moreover, different contexts may have different spectrum needs; in rural settings, lower frequency VHF may have the best long distance propagation characteristics.[118] The best way to coordinate these various bands, some unlicensed and some open only to public safety use, remains an open question in light of the push for a national broadband network in the 700 MHz band. How this coordination will affect current and potential use of mesh technologies is also unknown.

In short, there remain important challenges to address, not only at the technical and regulatory level, but also in terms of the best way to integrate mesh alongside existing tools and communications approaches. This challenge exists at the level of not only coordinating appropriate actors to deploy networks, but also ensuring that, over time, diverse stakeholders continue to use these networks in a way that recognizes their possible limitations and takes full advantage of their unique technical characteristics and communications affordances.

Significantly, mesh's emphasis on decentralized infrastructure and relatively inexpensive devices may offer alternative approaches without corresponding interoperability issues.[119] In particular, use of MANET devices could increase flexibility and resiliency, as described in Section II.[120] Mesh may be especially well suited for rapid deployment in emergency scenarios, subject to concerns about authentication and battery life, among others.[121] In addition, should officials decide to move towards the use of mesh in public safety networks, it might be possible to draw on expertise from the defense sector to develop innovative solutions, especially in light of the military's experience testing resilient mesh hardware in tactical communications scenarios, simulations involving similar stresses and conditions to those encountered in mission critical public safety communications.[122]

In the past six months, there have been some signals in the public sector that indicate an interest in building out mesh networks for public safety. Specifically, the National Institute of Standards and Technology's September 2011 comment "Soliciting Input on Research and Development Priorities for Desirable Features of a Nationwide Public Safety Broadband Network" explicitly sought input on, among other items, "Meshing (ad-hoc device-to-device communication): A type of networking where each node must not only capture and disseminate its own data, but also serve as a relay for other sensor nodes, that is, it must collaborate to propagate the data in the network" as a feature that might help "to ensure resiliency in an emergency."[123] Additionally, the January 2012 Report and Recommendations of the Visiting Committee on Advanced Technology of the National Institute of Standards and Technology (VCAT) entitled "Desirable Properties of a National Public Safety Network" included a section devoted to "Mesh or Mobile Ad Hoc Networking" in which it argued that "mesh networking could increase the flexibility of communication by allowing edge devices to serve as packet relays in a dynamic, mobile, mesh network design."[124]

As FirstNet—and other stakeholders at the Commerce Department, FCC, DHS, and other agencies—solicit input regarding the development of the 700 MHz public safety network, they are looking to industry, civil society, and academia for the expertise and proof of concept needed to determine the relative value of and place for mesh networks alongside the suite of tools utilized by the public safety community.

---

117 The spectrum licensing provisions of the 2012 Tax Relief Act emerged after strong debate about the role of unlicensed spectrum in previous competing spectrum reform bills. *See e.g.,* Paul Barbagello, *Rockefeller Says House Stopped Negotiating on Spectrum Bill but Differences Remain,* Telecomm. Monitor, Dec. 16, 2011.

118 GAO, Emergency Communications, *supra* note 86, at 15.

119 VCAT Report, *supra* note 116, at 11, 13–14.

120 *Id.* at 11.

121 *Id.* at 13.

122 *Id.*

123 Nat. Inst. of Standards and Tech., U.S. Dep't of Commerce, Soliciting Input on Research and Development for Desirable Features of a Nationwide Public Safety Broadband Network, 76 Fed. Reg. 56165, 56166 (Sep. 12, 2011).

124 VCAT Report, *supra* note 116, at 13.

V. Envisioned Mesh Use Cases

This section and Sections VI-VIII focus on participant viewpoints on mesh that were shared during the workshop. Section V highlights a few mesh use cases not already discussed in Section II and identifies future zones for mesh use and development. In describing several of these use cases, participants considered the value of mesh not only in terms of literal mesh networking in the technological sense, but also conceptually, in terms of the promise of ad hoc or decentralized networks to both improve public connectivity and enhance the safety of the public. Three broad areas for thinking of future uses of mesh are: 1) mesh as a supplement to (rather than a substitute for) mission critical public safety services; 2) mesh—both in the technical sense and as a social construct—as a way to connect communities and provide local services, with or without the use of actual mesh networking technologies; and 3) mesh as a technology that is under active experimentation as it operates in a unique economic environment.

A. Mesh as a Supplement to Mission Critical Public Safety Services

During the workshop, participants repeatedly emphasized that the reliability of communications services used by emergency responders was critical, and that emergency responders using those services should not have to worry about the stability of the technologies they use when they are in the field. Nevertheless, several public safety officials argued that mesh could be useful as an auxiliary to the current public safety infrastructure. Officials offered several stories where mesh or an ad hoc deployment was or could have been useful:

- A New England town lost all connectivity to the outside world after a hurricane. Although police and fire services had land-mobile radio, emergency responders also needed to access the Internet. Responders established an ad hoc network with the help of the local cellular provider.
- Bodies were found in a mountainous area where police were unable to access cellular services. Responders worked with a cellular provider to get additional cellular and data hot spots and enabled mesh services to units in the field.
- After a car struck a telephone pole, uprooting hundreds of feet of copper wiring, several thousand people were unable to call 9-1-1. Fortuitously, the local cellular provider had an unused cell tower in the area, and turned it on to restore service. Participants noted that a preexisting mesh network, even if it was not always switched on, could expedite the restoration of connectivity to emergency services and at least provide some supplemental service even if it was not completely reliable.

An official noted that while cellular companies are often able to help emergency responders access services in a disaster area, having the ability to set up a mesh quickly could substantially benefit command and control operations and help leaders understand the situation and determine how to distribute resources. This individual asserted that, in his experience, having specialized vehicles that can serve as mobile hotspots in disaster situations—enabling wider Internet connectivity to nearby laptops so long as the vehicle could access satellite or another available connection point—was invaluable in establishing a communications network where service was otherwise not possible.

Other participants raised several other current public safety-related mesh use cases:

- Dutch military personnel and firefighters use OLSR software developed by FunkFeuer that incorporates public safety features such as push-to-talk. Austria's Hamnet network also uses the FunkFeuer OSLR and serves as a de facto emergency broadband network that is slightly shifted from the normal WiFi spectrum.
- Carnegie Mellon University campus safety officials use mesh networks to improve emergency services. These mesh networks enable targeted emergency message delivery;[125] WiFi transmitters are set up both in fixed locations and in police trucks.
- Participants also emphasized that in a disaster situation such as Hurricane Katrina or in the aftermath of the 2011 Japanese Tohoku earthquake and tsunami, it can take a long time for major services to be restored, and that mesh would likely be most useful within that time period.

Participants also noted that citizens might use mesh capabilities to communicate with public safety officials in ways not afforded by existing communications channels. Locals, for example, might have the desire to reach out to public safety officials to provide verbal descriptions of a developing situation (such as a failing dam) or to share photographs and videos that might help officials understand how best to respond. To achieve such possibilities, it is important to think about the relationship between the public and public safety officials to ensure that connectivity empowers all involved parties.

The tenor of dialogue during the afternoon sessions revealed both tremendous potential benefits and risks associated with any use of mesh capabilities that might alter the status quo. One participant emphasized the need to consider how a particular affordance is actually implemented on the ground in different contexts, and to recognize how users may adapt it for their needs in unanticipated ways. A communications tool or technique that is well suited for one particular purpose may be ill-adapted in another instance, yet people on the ground may not recognize such constraints.

It is possible to imagine many hypothetical cases involving this phenomenon. To develop just one possible example, in the case of a failing dam, a crowd-sourced, interactive map that allowed individual users to upload their photographs onto a corresponding geographic location might provide public safety officials with important visual cues about the situation. However, while informative, it would be a mistake to rely on these visuals as a representative sample of the actual situation on the ground, because there might be some essential component of the dam's failure that was not visually captured by a user and uploaded to the map. It seems possible that indiscriminate use of such a communications technology without a simultaneous recognition of what such crowd-sourced data does and does not convey might ultimately prove counter-productive for the communications ecosystem. For instance, a public safety official could assume that he understands the entirety of a complex situation based solely on what he sees on a crowd-sourced data map; consequently, he could fail to use this available information as a complementary data source to enrich what he can learn from other sources. He might therefore act with incomplete information. Especially in a public safety context, this outcome could affect the reliability of the system and even harm actors operating within it. Individual civilian users might similarly count on the technology to do something it cannot. Therefore, in order to avoid unintended negative outcomes, it is essential to consider how people adopt and adapt a technology in practice and how any potential use within or between groups might affect overall faith in its affordances.

At the same time, mesh technologies have the potential to create new kinds of interactions and opportunities to share information and resources. On this note, workshop participants underscored the unique ways that mesh technologies might complement the existing communications environment for public safety officials

---

[125] Tim Means, *Ensuring Emergency Messages Get Delivered at Carnegie Mellon U.,* Campus Safety Mag. (Mar. 4, 2011), *available at* http://www.campussafetymagazine.com/Channel/Mass-Notification/Articles/2011/03/Ensuring-Emergency-Messages-Get-Delivered-at-Carnegie-Mellon-U.aspx.

and the public. One individual noted that giving consumers access to elements of a mesh network (such as mesh-enabled Wi-Fi repeaters on the side of a house) or placing these elements in public infrastructure (such as in streetlamps) could benefit emergency responders if the public were willing to switch devices over to agency use in the case of an emergency. It might even be possible to provide incentives for the public to switch over their devices in this way, perhaps by 'deputizing,' or giving official acknowledgement to private individuals for their contributions to the public safety community (e.g., a special title, a badge, or some other sort of public recognition). One participant suggested that mechanisms to reward participation could generate civic pride in supporting the network and possibly also shame individuals for a failure to do so, ultimately stimulating greater public participation. An additional or alternative incentive structure might take the form of a more traditional economic inducement, such as offering tax breaks for 9-1-1 fees if consumers permitted such switchovers. These sorts of social or economic incentives could motivate what would otherwise be purely voluntary actions and encourage the public to share resources in a way that supports public safety communications.

In addition, several participants agreed that communities comfortable with the use of mesh technologies could independently use a mesh network to connect their members and coordinate in an emergency situation. However, this outcome would require community buy-in, which reinforces the need to incorporate social and human dimensions alongside legal, regulatory, and technical considerations when discussing mesh deployment for public-safety applications. As suggested by several participants, such efforts might involve working directly with community members to reveal shared interests, expectations, and principles; one focus might be identifying good actors in the system and finding opportunities to educate and work with these community members to strengthen the system as a whole. Attempts to use mesh to supplement existing public safety capabilities should recognize how individuals interact with the technology in order to develop user education efforts regarding what mesh does and does not afford as well as how their actions may affect others within the decentralized communications network.

B. Mesh as a Way to Connect Communities and Provide Local Services

1. Past Experiences: Community Affordances of Mesh as a Technology

During the workshop, Greta Byrum, a policy analyst at the Open Technology Initiative at the New America Foundation, and Jonathan Baldwin, a graduate student at Parsons, the New School for Design, offered a presentation on the social dimension of mesh. Byrum and Baldwin worked with communities that used mesh networks in low-income communities in Detroit (Byrum) and the Red Hook Housing Development in Brooklyn (Baldwin). Both believe that mesh networks can only be effectively deployed and maintained in situations in which communities find that mesh networks respond to their needs.

Indeed, Byrum and Baldwin each emphasized the need to align mesh capabilities with the experiences of the communities where a mesh network is deployed, ensuring that actual needs are met and anticipated users are involved from the outset. A mesh is not built out from devices that relay information between passive agents; rather, people are effectively nodes in a mesh network. On this note, Baldwin discussed how the Red Hook community identified its major needs as activism regarding police stop-and-frisks and civic reporting of maintenance issues. To address these concerns, Baldwin worked with community members to create a Ushahidi-style[126] community map where people could point out where and what kind of problems were occurring in the neighborhood, which allowed them to better discuss the issues that challenged their community. If a mesh network can help satisfy such needs and empower community members, then users will recognize the relevance of mesh and become more willing to invest in the network. Both presenters stressed that such community buy-in is essential so that neighbors are willing to share their skills and knowledge with each other to support network infrastructure and repair the network if it fails.

---

[126] For more about Ushahidi, see *About Us,* USHAHIDI.COM, http://ushahidi.com/about-us (last visited Apr. 8, 2011).

Localized mesh applications like Baldwin's suggest that a mesh network can be valuable independent of its ability to access the Internet. For example, a community might find it beneficial to run a forum on the intranet level to discuss community issues without having to worry about observers from the wider Internet. Or a community might wish to post a neighborhood watch schedule or personal information about individual members that it might not be comfortable sharing on the wider web. Even if a community loses connectivity to the Internet during an emergency, a localized mesh intranet system could improve communication among members, facilitate information gathering, and enable effective responses to the situation. Identifying community needs and showing users how local uses for mesh could benefit communities might play a role in building stronger communities as well as expand public acceptance of mesh in general, especially because, as Byrum emphasized, trust is an essential factor in the way a network is built and used.

2. Future Consideration: Connectivity Affordances of the "Social Mesh"

The concept of mesh as a social, ad hoc or decentralized network rather than a technical tool may afford as yet under-realized possibilities. During the gathering, Byrum's emphasis on the social needs of community mesh and Baldwin's discussion of how he has met specific needs in Red Hook suggested a different use case for mesh, which participants called a "social mesh" or "crowdsourcing" approach. Baldwin's Ushahidi-style community map can stand as an example of such a social mesh because it does not necessarily depend on mesh as a communications technology to be effective. Rather, it exemplifies the use of peer-to-peer communications to share information that a community finds valuable for its specific needs.

This conceptualization of mesh offers considerable advantages for the connectivity and well-being of a specific community of users. Elaborating on this theme, one workshop participant cited Ushahidi[127] as a platform that provides a way for peers to engage with fellow community members by crowd-sourcing information-sharing and mapping data onto the community's geographical location. In emergencies, this capability can allow a community to better share knowledge and resources and collaborate when help is needed. Several other participants expressed support for a more crowd-sourced, social vision of mesh that foregrounds the value of decentralized connectivity rather than focusing on mesh as a networking technology. Filling in the possibilities of such a conceptual frame may be an important part of future conversations about mesh.

Several strains of conversation during the gathering suggest that it may be worth thinking more about how peer-to-peer or crowd-sourced communications in the model of a social mesh might be applied to public safety contexts to complement existing public safety communications. Perhaps, as a supplement to 9-1-1 emergency response efforts, a social mesh in which individuals can easily send and receive information could help assemble people to solve problems that are not so critical as to require professional intervention. As some participants suggested, one fruitful area might be building out a model in the vein of the 3-1-1 "non-emergency" systems[128] that currently operate in selected municipalities across the country. This model, dubbed "8-1-1" by one participant to denote that the call is made at a lower level of crisis than 9-1-1, would allow members of the public to reach out to others in the community for help with issues that do not represent true emergencies. In this way, a social mesh could allow individuals to share their needs and more effectively draw on the shared resources of the community, thereby freeing up vital public safety resources to deploy where they are more urgently required. One such example cited during the workshop was that of an individual whose car had become stuck in a snow bank and who might wish to call on neighbors for assistance; a social mesh could notify many people at once and be used to quickly determine which individuals were nearest and best equipped to help. A social mesh might also provide additional channels for communication during a state of emergency or sweeping disaster like Hurricane Katrina when public safety authorities are operating at or near capacity.

---

[127] *See generally* Ushahidi website at *supra* note 126.

[128] *See* Heather Hayes, *Dial 311: 311 service is e-government with a different name,* Fed. Computer Wk., Feb. 1, 2008, http://fcw.com/articles/2008/02/01/dial-311.aspx (noting experiences with 311 in a number of cities and explaining how one "311 center handled requests that otherwise would have flooded busy police and fire departments.").

While there remain a number of important questions regarding how and when it may be advisable to open up new methods for the public to communicate about public safety needs outside of official existing channels, this dialogue helped to draw important distinctions between the different conceptualizations of mesh and their applicability in different contexts. Stakeholders in this space might consider how to leverage peer-to-peer communications inspired by the social mesh model for public safety applications.

C. Mesh Experimentation and Adoption in the Current Economic Environment

As a developing technology, mesh networks are undergoing continued experimentation by researchers and private companies. As mentioned in previous sections, mesh has also been favored by members of civil society groups, many of which have focused on the development of mesh in Europe. One American hobbyist organization, the American Radio Relay League (ARRL),[129] has been experimenting with mesh for the last twelve years in multiple states. The ARRL has used mesh to link hospital services and provide connectivity for public safety NGOs in emergency management situations. While the ARRL is keen to experiment further with mesh, they are barred from deploying access except in emergency situations because the ARRL itself does not provide the Internet access. Making it easier for groups like the ARRL to experiment could spur further development of mesh technologies and result in the training of more operators who know how to handle a mesh network.

Mesh use in a public safety context is likely to largely remain within the realm of experimentation unless there are significant changes in the economic environment for public safety devices. Enabling community level mesh and more experimentation at a local level, however, is still valuable because state and federal officials may be more willing to accept mesh as a technology that can be trusted in a public safety context when they have more opportunities to encounter it in their lives. Multiple workshop participants noted that transitioning from an old, dependable technology to a new one is not just a matter of technical feasibility, but also a matter of whether public safety officials believe in a new technology enough to invest in it. State public safety officials are more likely to accept new technologies that are both dependable and economically attractive.

Leaving aside whether government purchasers could come to trust mesh technologies, the current economics for procuring public safety handset devices tend to make such new technologies unattractive. Currently, 60,000 public safety agencies make purchasing decisions for six million devices in a market fractured by varying public safety standards. This situation drives costs for a single device up to $11,000 and makes officials prone to invest in devices that they know have been tested for decades. Working to establish world public safety standards might help generate a larger market and drive costs down. One participant argued that placing mesh technologies in vehicles and allowing consumer opt-in would help fund more sophisticated mesh development to make the technology more dependable generally, which might eventually make public safety mesh devices more feasible. Others at the workshop more explicitly emphasized the importance of present-day economic considerations for the future viability of mesh at any meaningful volume and scale; one individual asserted that mesh technologies must improve very quickly to become economically competitive on a price/performance basis against embedded alternatives like WLANs.

Even if mesh technologies fail to achieve the necessary reliability and security standards for mission critical performance or to become economically sensible for device manufacturers, greater ubiquity of mesh could still benefit the public. As described above, localized mesh could benefit communities. In addition, making it socially popular to support a mesh network that could be turned over to public safety officials in an emergency could reinforce civic values and improve disaster response. With mesh networks commonly available in the field, local agencies could connect to a disaster area quickly through existing infrastructure rather than having to set up a mesh independently whenever an emergency arises. This capability would likely reduce the cost burden placed on local public safety agencies, making wider mesh adoption more attractive.

---

[129] *ARRL Homepage,* ARRL, http://www.arrl.org/ (last visited Apr. 8, 2011).

VI. Involved Parties And Potential Stakeholder Considerations

Bearing in mind the use cases discussed during the workshop, this section first lists four broad groups of stakeholders that have expressed interest in and have the ability to shape the future of mesh technologies, then puts forth some key considerations regarding the future of mesh and mobile ad hoc networks as they might be seen from the vantage points of different stakeholders, with a focus on decentralized innovation generally and public safety specific issues (PSSI) in particular. The parties and ideas listed below are not meant to be exclusive, and alternate ways of organizing both the categories and the ideas within each category may be possible.

Technical Experts include researchers and engineers who deeply understand how novel communications technologies like mesh work or could work, and who may approach the challenges faced by mesh technologies from an engineering perspective.

To the extent that they wish to advance mesh innovation, technical experts might:

- Make a clear evaluation of the communication need(s) that a particular decentralized solution is intended to serve, including a careful assessment of which technology is most appropriate for a specific context;
- Continue work to develop an efficient routing strategy for MANETs, distinct from legacy wired routing solutions;[130]
- Ensure that the provision of service is more fair across a MANET;[131]
- Strengthen WMN security by improving attacker detection techniques and designing an attack-resilient security architecture;[132]
- Continue to improve the energy efficiency of mobile devices to improve network sustainability;[133] and
- PSSI: find ways to reduce the performance gap between unplanned WMN deployment versus planned WMN deployment.[134]

Government Agencies and Public Safety Officials include federal, state, and local agency officials who are interested in the potential of mesh technologies and who can play a role in how such technologies develop at the regulatory or policy level.

Government officials might be particularly concerned with how a given technological innovation will affect the status quo communications ecosystem, and how the implementation of that technology could interact with existing regulations and policy objectives. To the extent that they determine mesh technologies are worth supporting, agencies and officials might:

---

[130] Conti, *supra* note 43, at 80; *see generally* Bruno, *Diversity-Based Routing, supra* note 37.

[131] Ernst, *supra* note 49, at 653.

[132] Glass, *supra* note 61, at 530-531; Jinyuan Sun et al., *SAT: A Security Architecture Achieving Anonymity and Traceability in Wireless Mesh Networks,* 8.2 IEEE Transactions on Dependable and Secure Computing 295 (Mar.–Apr. 2011); *see also* Mahira Atham Lebbe, Johnson I Agbinya & Zenon Chaczko, *Policy Based Danger Management in Artificial Immune System Inspired Secure Routing in Wireless Mesh Networks,* Proceedings of the Int'l MultiConference of Engineers and Computer Scientists, 2008, at 1.

[133] Conti, *supra* note 43, at 82.

[134] Hu, *supra* note 68, at 611 (noting test showing that throughput performance for unplanned network deployment was 44% - 67% lower than planned deployment).

- Avoid new regulations that make it difficult to deploy mesh/Wi-Fi networks;
- Avoid criminalizing the sharing of broadband connections through Wi-Fi (there has been speculation that federal and state theft-of-service statutes could apply to sharing; broadband service when terms of service agreements do not allow service sharing);[135]
- Continue to support open-source wireless mesh-networking projects;[136]
- PSSI: Implement social mesh or crowd-sourced information- and resource-sharing capabilities as complements to existing emergency response capabilities, both for day-to-day public safety operations and in times of disaster;
- PSSI: Determine whether a mesh solution is able to meet the rigorous performance standards for public safety and disaster recovery networks;[137]
- PSSI: Expand the amount of spectrum available for public safety broadband so that innovative services offered by mesh have sufficient spectrum space to work;[138] and
- PSSI: Integrate any decentralized network alongside the recently passed Middle Class Tax Relief and Job Creation Act of 2012 that licensed the D Block spectrum for dedicated public safety use and allocated $115 million to NG-9-1-1.[139]

Industry Members include private stakeholders who may be interested in the development of mesh technologies so they can more efficiently develop hardware and software that support mesh applications to offer value to consumers.

However, while some of the involved parties in this space are those who either have indicated an interest in mesh or who, at present, currently operate in the mesh router business or are currently involved in mesh technologies more generally, not all private stakeholders would necessarily look favorably upon the development and deployment of mesh technologies, for a variety of reasons.

Industry actors with an interest in advancing mesh networking might:

- Encourage working groups to rapidly define mesh networking standards so companies will not need to implement proprietary mesh protocols for routing and network configuration,[140] which would simplify the integration of mesh routers purchased from different vendors[141] and in turn make it easier for government agencies to invest in mesh;
- Request that the government reserve or leave open spectrum space for mesh applications, preferably in the highly prized white spaces frequencies,[142] to reduce interference and encourage experimentation;

---

[135] Hatcher, *supra* note 7, at 15 (noting that Time Warner cable has sent out cease-and-desist letters to customers with open Wi-Fi networks).

[136] Dibbell, *supra* note 2, at 63 (noting the U.S. State Department provided wireless mesh-networking project Commotion with a $2 million grant to develop decentralized Internet technology that could maintain connectivity when a repressive government shuts down ISPs).

[137] Wishart, *supra* note 54, at 295-6.

[138] *See* Jackson, *supra* note 98, at 8-9.

[139] *See supra* text accompanying notes 93-99.

[140] Portmann, *supra* note 1, at 20.

[141] *Id.*

[142] *See The Economics of White Spaces,* Bloomberg Businessweek, Feb. 27 – Mar. 4, 2012, at 36 (noting white spaces frequencies tend to have less interference than unlicensed bandwidths and are better able to carry long distances and through walls, as well as AT&T and Verizon's expressed determination to acquire a significant amount of available white spaces).

- Develop new and improve existing mesh products,[143] as well as showcase the capabilities of mesh[144] to enhance public and private awareness and adoption of mesh technologies;
- For industry members in the mobile development space, use open application programming interfaces or different device manufacturing methods to allow devices to more easily form WMNs (currently, mobile operating systems including Android and iOS prohibit mobile devices from entering ad hoc mode without circumventing vendor barriers by, for example, acquiring root access);[145]
- PSSI: In the vehicular mesh context, urge government support for an open source platform to spread mesh networks, thereby laying the foundation for future safety and convenience applications;[146] and
- PSSI: Continue to promote mesh for public safety applications[147] and develop commercial products that realize public safety needs.

Academics and Civil Society Stakeholders are a diverse group of individuals who envision a variety of uses for mesh networks, ranging from mesh as a means of building communities, to avoiding the centralization of Internet control, to providing cheaper or free Internet service. Such individuals may focus primarily on research, engage in activism on behalf of mesh networks and open technologies, or take part in some combination of research and advocacy.

Given the diversity of this group, academics and civil society stakeholders have varying perspectives on what should be done to advance mesh—or not. With this fact in mind, some constituents might:

- Build and reinforce real world communities that are connected via mesh,[148] which requires surmounting technical challenges and creating mechanisms to make participants comfortable sharing a mesh network with their neighbors;[149]
- Involve the public in the construction of peer-to-peer communications networks, regardless of whether these networks in fact make use of mesh network technologies;
- Continue to develop and simplify mesh network technologies[150] to reduce the technical expertise needed to deploy and maintain them;[151] and
- Demonstrate the technical feasibility of deploying unplanned wireless mesh networks at scale.[152]

---

143 *See Cisco Aironet 1550 Series Outdoor Access Point Data Sheet,* Cisco Systems, http://www.cisco.com/en/US/prod/collateral/wireless/ps5679/ps11451/data_sheet_c78-641373.html (last visited Mar. 22, 2012) (claiming mesh product is "industry's first enterprise and carrier-grade 802.11n access point to create a self-healing and self-optimizing wireless network that mitigates the impact of wireless interference").

144 *See Austin's Wireless Mesh Provides Free Access and Test Environment,* Cisco Systems (2006) http://www.cisco.com/en/US/prod/collateral/wireless/ps5679/ps6548/prod_case_study0900aecd80563c29.pdf.

145 Hanno Wirtz et. al., Establishing Mobile Ad-Hoc Networks in 802.11 Infrastructure Mode, CHANTS'11, 2011, at 49.

146 *See* Chase, *supra* note 28.

147 BelAir Networks, *supra* note 26, at 8.

148 Antoniadis, *supra* note 20, at 53.

149 *Id.* at 54-55.

150 *See* Jeffrey R. Young, *Fear of Repression Spurs Scholars and Activists to Build Alternate Internets,* The Chron. of Higher Educ., Sept. 18, 2011, *available at* http://chronicle.com/article/Fear-of-Repression-Spurs/129049/ (noting mesh-network efforts to create an "Internet in a suitcase" (Sascha Meinrath's Commotion project)); Dibbell, *supra* note 2, at 65 (noting Columbia Law Professor Eben Moglen's FreedomBox project).

151 Hasan, *supra* note 76 (claiming that setting up and troubleshooting a wireless mesh network is time consuming and difficult from a technical perspective).

152 Isaac Wilder, *Why Wireless Mesh Networks Will Save Us from Censorship,* The Free Network Found. (Jan. 9, 2012), http://freenetworkfoundation.org/?p=701.

VII. Mesh in the Intermediate Future

Workshop participants from the groups described in Section VII identified a number of potential steps for the future of mesh and public safety, particularly in the regulatory and government arenas. They also expressed concerns that echo the technical challenges described in Section III and anticipated future hurdles that could arise if the use cases in Section V go forward.

A. Changes to the landscape of wireless networking and public safety communications

- In the broad context of spectrum policy, the continuing "spectrum crunch" will necessitate less reliance on dedicated spectrum and more spectrum sharing through advanced technologies, of which mesh is likely a key component.
- As FirstNet becomes fully staffed and begins to take on the role of building out the nationwide broadband network, it will have the opportunity to update outdated systems.
    - Recent legislation and regulation reflects a widespread understanding that public safety communications has far to go to meet current public safety challenges, and that there is a significant opportunity to make use of next-generation consumer technologies in addressing these challenges.
    - These regulatory interventions and other related programs will offer a significant opportunity for public input. Academics and civil society stakeholders can provide a voice for implementing mesh technologies where they are appropriate.
- The military will continue to be a large user of mesh technologies, in part to facilitate infrastructureless communications and to lessen its reliance on dedicated spectrum.
- Especially as the field evolves in light of recent legislative changes and continuing technological advancements, a social mesh that leverages technology to allow neighbors to help neighbors and communities to share resources (e.g., "8-1-1") might complement public safety communications and responses.

B. Concerns for future mesh applications

- Mesh networking will continue to face general skepticism that it is not a viable technology, particularly for public safety applications and most crucially for mission critical applications.
    - Participants agreed that any use of mesh technologies in a public safety context would face a significant public relations hurdle, in that many public safety users have a strong perception that it is unreliable, even when faced with data to the contrary.
    - Convincing public safety users of the reliability of mesh may be difficult if the data comes solely from civil society and academic users, who may not be able to provide detailed usage statistics and analysis.
    - Although they are open to communications technologies that provide more connectivity to the general public and allow for two-way communication with first responders, public safety participants expressed concern that public safety users and first responders specifically may not be able to perform their primary tasks and handle this increased flow of information from the public.

- Participants highlighted the need to clarify how proponents of mesh conceptualize the use cases described in Section VI. Proponents must be able to articulate why mesh specifically, as opposed to another technological solution, is the right solution for the problem they are addressing.
    - In particular, participants expressed the need to justify the economic viability of a mesh solution over others.
    - More broadly, in considering possible mesh applications, it is essential to differentiate clearly between references to mesh as a networking technology and references to a social mesh for peer-to-peer communications and crowdsourcing of requests for assistance. Only in this way is it possible to develop appropriate approaches for each instance without muddling distinct concepts.
    - To ensure that mesh is used appropriately in a given context, it is essential not only to develop mesh as a networking technology and a social construct, but also to educate users about when they should and should not rely on mesh.
- The workshop also focused attention on general concerns of attempting to bridge the gap between bottom-up, decentralized technologies and the traditionally top-down public safety sector.
    - Participants expressed concerns about who will be the first mover. Public safety users need to be convinced of the reliability of mesh, yet the technologies must also be tested under realistic conditions, which academic and civil society participants may not be best positioned to do.
    - To the degree that mesh technologies have been developed in an open source organizational model and to the extent that such a model remains desirable, participants questioned how open source values and technologies can be realized if top-down policymaking is required before the successful deployment of a given technology for public safety purposes.
    - Academics and civil society may have difficulties in learning the concerns of public safety users and responding to them.

VIII. Key Take-Aways from Initial Working Meeting on Mesh Technologies

In keeping with the framing of the workshop as a starting point for conversation about whether mesh networks could be used to enhance public safety communications, participants agreed that a key output would be a set of core principles and best practices. These shared directives regarding goals, scope, and a roadmap for the future could guide consideration of technological developments, policy interventions, and communications with public and private parties about expectations for this space. In particular, there might be a feedback loop between principles and conceptual frameworks that could, in turn, support actual mesh development and deployment. Principles might also help to frame mesh as a social construct and inform the best realization of mesh networking technologies; simultaneously, these two conceptual models might suggest essential principles and best practices to take into account. This section presents a few of these principles in preliminary form, with the hope that they will seed additional dialogue and spur future research and development.

Stakeholders advocating the use of public networks for public safety should:

- Consider the best ways for mesh to act as a complement to, rather than a substitute for, traditional public safety communications, particularly mission critical applications.
    - Work with the public safety community to better understand what use cases would complement and fill in gaps left by existing technologies.
    - More fully describe the goal of connecting and empowering the public in public safety scenarios without interfering with primary public safety functions.
    - Evaluate the affordances of mesh technologies to create communications networks as well as the affordances of a social mesh to connect and empower the public in ways that might enhance public safety.
- Describe how the public will use these networks and consider what factors will spur adoption.
    - Consider the use of community incentives and mutual benefit in donating time, network resources and expertise.
    - Find ways to increase local buy-in as well as trust, including by appointing amateur experts or community managers of networks.
    - Clarify public needs and expectations in regard to both mesh networking and social mesh and consider how these factors might interact with public safety communications.
    - Continue to develop applications that would be useful in a localized network or intranet and that have natural relevance for public safety mesh networks.
- Develop metrics and use cases that will make the case for the reliability of these technologies in a public safety context.
    - Address security and resiliency concerns by providing actual use data, particularly from existing community wireless networks.
    - Develop shared goals for experimentation and testing by various stakeholders.
    - Act as a balanced, clear voice to ensure that ongoing regulatory processes continue in tandem with grassroots experimentation and provide breathing room for exploring mesh technologies and models as a component of next-generation public safety communications.

IX. Selected Resources

Informative Articles on Technical Issues Related to Mesh / MANETs

Raffaele Bruno & Maddalena Nurchis, *Survey on Diversity-Based Routing in Wireless Mesh Networks: Challenges and Solutions,* 33 Computer Comm. 269 (2010).

Raffaele Bruno, Marco Conti & Entrico Gregori, *Mesh Networks: Commodity Multihop Ad Hoc Networks,* IEEE Comm. Mag., Mar. 2005.

Marco Conti & Silvia Giordano, *Multihop Ad Hoc Networking: The Theory,* IEEE Comm. Mag., Apr. 2007.

Jason B. Ernst & Mieso K. Denko, *The Design and Evaluation of Fair Scheduling in Wireless Mesh Networks,* 77 J. of Computer and Sys. Sci. 652 (2011).

Stephen Glass, Vallipuram Muthukkumurasamy, & Marius Portmann, *Detecting Man-in-the-Middle and Wormhole Attacks in Wireless Mesh Networks,* Int'l Conf. on Advanced Info. Networking and Applications, 530 (2009).

Parth H. Pathak & Rudra Dutta, *A Survey of Network Design Problems and Joint Design Approaches in Wireless Mesh Networks,* 13.3 IEEE Comm. Surveys & Tutorials 396 (Third Quarter 2011).

Informative Articles on Mesh Related to Public Safety

Naveen Lakshmipathy, *Wireless Public Safety Data Networks Operating on Unlicensed Airwaves: Overview and Profiles,* New Am. Found., Apr. 2007.

Marius Portmann & Asad Amir Pirzada, *Wireless Mesh Networks for Public Safety and Crisis Management Applications,* IEEE Internet Computing, Jan. / Feb. 2008.

Brad Smith, *Mesh Helps Public Safety Keep an Eye Out,* Wireless Week, Feb. 1, 2008.

Ryan Wishart, Marius Portmann & Jadwiga Indulska, *Evaluation of Wireless Mesh Network Handoff Approaches for Public Safety and Disaster Recovery Networks,* ATNAC 2008.

Abdulrahman Yarali, Babak Ahsant & Saifur Rahman, *Wireless Mesh Networking: A Key Solution for Emergency & Rural Applications,* 2009 Second Int'l Conf. on Advances in Mesh Networks.

Informative Articles on Public Safety Broadband Networks and PSAPs

Kenneth C. Budka, et. al, *Public Safety Mission Critical Voice Services Over LTE,* 16 Bell Labs Tech. J. 133 (2011).

See Intelligent Transp. Sys., U.S. Dep't of Transp., Next Generation 9-1-1 (NG9-1-1) System Initiative Final System Design Document (Feb. 2009), http://www.its.dot.gov/ng911/pdf/USDOT_NG911_FINAL_System_Design.pdf.

Nat. Inst. of Standards and Tech., U.S. Dep't of Commerce, Desirable Properties of a Nationwide Public Safety Communications System (Jan. 24, 2012), *available at* http://www.nist.gov/director/vcat/upload/vcat-public-safety-subcommitte.pdf.

Off. of Interop. and Compat., U.S. Dep't of Homeland Security, Public Safety Statement of Requirements for Communications and Interoperability Vol. II. (Aug. 2008), *available at* http://www.safecomprogram.gov/library/Lists/Library/Attachments/302/Statement_of_Requirements_Volume_II%20-%20Version%201_2.pdf.

U.S. Dep't of Homeland Sec., Public Safety Communications Evolution (Nov. 2011), *available at* http://www.imsasafety.org/PDFs/Public%20Safety%20Communications%20Evolution%20Brochure.pdf.

U.S. Gov't Accountability Off., First Responders: Much Work Remains to Improve Communications Interoperability, GAO-07-301 (Apr. 2, 2007), *available at* http://www.gao.gov/new.items/d07301.pdf.

U.S. Gov't Accountability Off., Emergency Communications: Various Challenges Likely to Slow Implementation of a Public Safety Broadband Network, GAO-12-343 (Feb. 22, 2012), *available at* http://gao.gov/assets/590/588795.pdf.

The White House, The Benefits of Transitioning to a Nationwide Wireless Broadband Network for Public Safety (June 2011).

Informative Articles on Academic and Civil Society Perspectives on Mesh

Panayotis Antoniadis et al., *Community Building over Neighborhood Wireless Mesh Networks,* IEEE Tech. and Soc'y Mag., Spr. 2008.

Julian Dibbell, *The Shadow Web,* Sci. Am., Mar. 2012.

Jordan S. Hatcher, *Mesh Networks: A Look at the Legal Future,* 11.5 J. of Internet Law 12 (Nov. 2007).

Isaac Wilder, *Why Wireless Mesh Networks Will Save Us from Censorship,* The Free Network Foundation (Jan. 9, 2012), http://freenetworkfoundation.org/?p=701.

Jeffrey R. Young, *Fear of Repression Spurs Scholars and Activists to Build Alternate Internets,* The Chron. of Higher Educ., Sept. 18, 2011, *available at* http://chronicle.com/article/Fear-of-Repression-Spurs/129049/.