Public safety and emergency services in future wireless communication

Douglas C. Sicker
Interdisciplinary Telecommunications Department
Department of Computer Science
University of Colorado at Boulder
303-735-4949 (phone)
303-492-1112 (fax)
douglas.sicker@colorado.edu

As various forms of wireless communications become more pervasive, the expectation for this communication to support public safety and emergency functionality will arise. The public switched telephone network presently supports many such functions. The most familiar of these functions is that of Enhanced 911 (E911), for the provision of emergency response capability. A lesser known function is that of Telecommunication Service Priority (TSP), for the prioritization of service provisioning and restoration for national security or emergency preparedness missions. Other functions, such as Government Emergency Telecommunication Service (GETS) and Wireless Service Priority (WSP) provide what the Federal Communications Commission refers to as Priority Access Service (PAS). GETS provides a means of increasing call completion probabilities during times of heavy congestion, which may result from natural or man-made disasters or other emergencies. Likewise, WSP is now being deployed in the wireless space to provide increased probability of accessing resources during times of congestion. WSP will serve to complement GETS for end-to-end connections from wireline or wireless environments. Together these services (and a few not mentioned) form the primary basis for public safety communications.

Most of these public safety services rely on traditional telephony technology. For example, Signaling System 7 (SS7) and Intelligent Network (IN) allow priority services, specialized routing and network management capabilities for such services as GETS and WSP. However, this type of approach may not apply to emerging wireless systems, in that there is a fundamental shift away from centralized control environments, such as SS7 and IN. In such an environment, an authority (e.g., the service provider) controls the network by monitoring and assigning resources to the end users. This approach is rather antithetic to many of the emerging wireless architectures, where control and resource assignment is decentralized. A question this raises is what problems this shift creates and whether such services can still be provided in a reasonably reliable manner? Maybe a more fundamental question to consider is if these networks should support public safety and emergency services?

In this paper, we begin by considering a number of existing public safety and emergency services. Next, we consider the technical problems and requirements associated with providing these services. We next examine an existing wireless technology with respect to these requirements. To end, we consider the applicability of such services.

Keywords: public safety, emergency services, wireless, E911, priority, GETS, WSP

Introduction

As we have seen in the commercial wireless space, there is high expectation from the public, government agencies and public safety officials for communications networks to support emergency services. [1] This expectation has only increased with the recently heightened concerns regarding terrorism and the accompanying public safety readiness. The range of national security or emergency preparedness (NS/EP) events that might warrant the use of public safety and emergency services (hereafter referred to as public safety service) is broad.[1] It can include responses to requests made under heavy traffic loads (such as during a national disaster) to responses to requests made under normal traffic conditions (such as most E911 calls). However, we will not debate the virtues or the need for such services; nor we will define what warrants the invocation of such services. Rather, we consider the technical requirements for public safety and emergency services in light of changing network architectures and the implications this change has on the provision of such services.

In this paper, we examine public safety services with respect to future wireless networks. The intention is to outline the functions required to provide public safety services in future wireless networks. We begin with a brief discussion of how wireless network architectures are changing. Next, we provide a brief background on emergency services (E911) and more.

[1] While the term 'public safety' is often perceived as applying only to communication services among public safety officers, we use the term more loosely to include such things as priority access, priority provisioning,

existing telecommunications public safety services. From this we extract the basic functionality needed to provide these services. We then consider these basic functional requirements as they relate to existing wireless technology. This paper will not focus on the steps required to make existing wireless systems public safety capable. Rather, we will focus on describing the functions required of these networks. Finally, we will consider whether such public safety services are even applicable to these emerging wireless networks.

Architectural Change

We begin by briefly considering how networks are changing and what this change means to public safety services. We briefly examine a number of functional differences that exist between traditional and future networks, and what this might mean to providing such services. When we say future networks we mean packet based networks, namely Internet Protocol based networks.

Control: In the circuit switched world (including cellular), connections among end points are made by a provider controlled signaling system, namely SS7/IN. This function exists separate from the voice channel and provides a means of querying, setting up, altering, and tearing down connections. Packet networks, such as the Internet, do not make use of such centralized systems to control resources and connections. Rather, information such as routing data is contained within the packet as header information. Route updates and other such information are propagated as packet data along with other service data. This is not to suggest that signaling does not exist in the Internet, but rather that the design approach is not one of strict provider control.

As indicated, most public safety services rely on traditional telephony technology. For example, the SS7/IN allows priority services, specialized routing, and network management capabilities for such services as GETS and WSP.[2] It is the centralized coordination of this signaling system that allows for many of the public safety services discussed earlier. However, this approach does not apply to emerging wireless systems. For example, there is a fundamental shift away from control environments, where providers control the network by monitoring and assigning resources to the end users. This is antithetic to many of the emerging wireless architectures; where control is highly decentralized.

[2]Interestingly, most E911 systems still depend on antiquated technology and do not make use of SS7 and IN, which incidentally have been in existence and use for decades. However, rather than argue for the move toward another highly centralized control environment (such as SS7/IN), we must consider the public safety implications of moving toward distributed control environments.

Layered models: The layered model of Internet Protocol (IP) based networks separates the application from the transport, allowing for decentralized control. This decentralized control means that the end point may be responsible for providing the intelligence required to offer services. However, some public safety services cannot simply be pushed into the application layer and assumed to operate as required. For example, an E911 call requires that location information be passed to public safety officials. This location information will likely involve some radio signal information for position determination. The application layer will depend on this lower layer service to provide location capability.

Delay: Unlike a circuit switched network, most packet networks do not dedicate resources to the exclusion of other services. Various protocols exist to address the problem of resource reservation and prioritization for packet networks, but few of these are deployed. As such, packets may be delayed an unacceptable period of time, which may cause an E911 call to drop or be unintelligible. End-to-end delays of as little as 250ms can make conversation difficult and destroy video. Similar issues with packet networks include delay variation and packet drop.

A question that remains is how to allow highly distributed, highly decentralized networks to support services that have traditionally depended on highly centralized structures. Another question is how to deploy these services in emerging wireless networks in a reasonably reliable manner.

Existing Public Safety Services

In this section, we will examine a number of existing public safety and emergency services. While this will serve as a general template for future services requirements, it should be realized that the expectation of what defines a public safety service (and its requirements) will evolve just as networks evolve. To that end, we begin small with a core set of services.

The services we consider in this section include Government Emergency Telecommunications Service (GETS), Wireless Priority Service (WPS), Cellular Priority Services (CPS), Telecommunications Service Priority (TSP) and Emergency Services. While this is not exhaustive of all public safety services, it represents an important set of services.

GETS: GETS is the wireline Priority Access Service (PAS) service. It provides a means of increasing call completion probabilities during times of heavy congestion, which may result from natural or man-made disasters or other emergencies. It allows an authorized user to access services through the use of a universal access number and a PIN. GETS provides enhanced routing and various priority treatment of calls to improve completion rates. [2]

WPS: WPS provides a wireless counterpart to GETS by offering an enhanced probability of completing calls.

This technology has been provided through channel reservation or priority access queuing techniques. [3]

CPS: CPS, a generalized term for cellular wireless PAS, provides end-to-end cellular priority for NS/EP users and can make use of various technologies to provide this priority function. [4]

TSP: TSP provides for more timely installation and restoration of public safety services. This is a means of being placed on the top of the repair and install order process. [5]

Emergency Services: This provides a means of requesting emergency services. Enhanced 911 (E911) extends basic 911 by adding automatic number identification (ANI) and automatic location information (ALI) technology to emergency calls. The requirements involved in providing E911 services include; use of a universal emergency number ('911'), locating the user, determining the appropriate Public Safety Answering Point (PSAP), determining the number of the calling party and corresponding location and routing the call. [6]

From the above we will now extract a set of basic and specific functions.

Functionality

In this section, we examine a set of functional requirements necessary to support public safety services. To generalize, we might divide the above services into 1) prioritization of access and restoration and 2) emergency. Prioritization of access provides a means of increasing call completion probabilities during times of heavy congestion, which may result from natural or man-made disasters or other emergencies. Prioritization of restoration is simply the ability to offer a more timely installation and restoration for public safety users. Emergency services provides a means of requesting emergency response.

GETS, WPS, TSP and E911 represent a set of Public Switched Telephone Network (PSTN) oriented public safety services, and as such, depends on the architecture and functionality of the PSTN. However, this architecture will change substantially as we move more services toward packet based networks. Therefore, we need to generalize these requirements; uncouple them from the architecture in which they are provided.

In this following section, we consider the building blocks required of each service, with the goal being to create functions that are independent of the architecture.[3]

Addressing and numbering: The network must support the addressing/numbering required to route a universal number. A common example of this function is that of an emergency service number '911' or a directory service number '411'. This functionality will depend on the existence of an agreed upon session functionality to provide such an address.

Location: The network must support the ability to locate calling parties. Various methods may be used to locate a user including; base stations triangulation, Global Positioning Satellite (GPS), assisted GPS, manual registration and others. The accuracy of such systems depends on a host of technical and operational issues. The details of how this operates is outside the scope of the paper.

Querying: The network must support the ability to query the appropriate database in the appropriate manner. For example, a determination must be made to which public safety point a call should be routed. This process will depend heavily on directory services and access to these directories, as well as on the validity of these records. Many of the more difficult problems within this space may come back to policy and regulation, to resolve the who, what, where, when and how of accessing these directories. In that much of this functionality is at higher layers of the protocol stack, this requirement may be abstracted away from the underlying wireless networks.

Mapping: Arguably distinct from the location and querying system, public safety systems require geographic information systems. This provides the means of mapping and associating the various elements required in location dependent systems.

Quality of service: The network must provide the appropriate Quality of Services (QoS) required of the service. While there are many solutions for this QoS differentiation in packet networks, few are actually deployed. When we consider this issue in terms of a future wireless network, we must consider how best to integrate such capabilities with the public safety service. If a service requires support for voice or video, QoS may be an important issue. However, there are other services, such as messaging, that may not require special QoS treatment.

Prioritization of service: The notion of Prioritization of Service (PoS) relates to that of QoS. The idea is that not only does a service require special treatment (such as QoS for video), but that certain users of that service require additional specialized treatment (such as preemption). This issue arises when many players are trying to make use of a highly constrained resource, such as during times of disaster.[4] At such times, public safety officials may be required to preempt other players. These services may be origin dependent (based on the device) or user dependant (based on the user). A primary difference is the need to authenticate a user on any line, versus a line being specified for such services. [8] There

[3]For example, traditional PSTN public safety functions include things like trunk prioritization, emergency override and calling line restrictions override. While it may be that such services exist in future networks, these functions are closely tied to the PSTN.

[4]One provider, T-Mobile, a Global System for Mobile (GSM) provider, has taken advantage of a GSM feature referred to as enhanced Multi-Level Precedence and Preemption, which allows calls to queue while waiting for the next available radio channel. [7]

are a number of other PSTN specific functions used in PoS, such as priority routing, automatic repeat request and last trunk reservation. Some of these may apply to future services and some may not. Rather than focus on each of these functions, we merely describe the basic requirement.

Power: An easily overlooked issue is that of power. Any device that provides its own power has an additional availability constraint. Many rely on the availability of their wireline phone when their power is out. This sets an expectation for future networks. However, users of cell phones have come to realize the need to charge batteries on a regular basis and this same expectation will likely translate to other wireless devices. Nonetheless, this creates a possible availability issue for wireless devices with respect to NS/EP services.

Reliability: The network must provide the appropriate level of reliability. The ability for a packet network to provide the 99.999% reliability of the PSTN requires considerable effort. The public Internet provides around 99% reliability at a macro scale. While this falls short of the expectation of the PSTN, the Internet was not designed to provide similar reliability measures. Error detection and correction provides improved reliable delivery of data services but does not work well with real time services. Reliability raises a number of questions with respect to public safety services. What are the reliability and availability requirements expected of the system? Should these requirements differ among systems and how? How stable and usable is the design?

Security: The network must provide a broad level of security including the typical areas of confidentiality, integrity, availability and non-repudiation. Public safety services may require secure communications to avoid message interception. Certain communications might require strict authentication and authorization schemes to ensure that only appropriate users access the resources. This proposes an interesting problem in the wireless arena, where signals are broadcast into the ether for anyone to intercept. Wireless networks also raise interesting availability problems, such as jamming (a type of Denial of Service (DoS) attacks), where an attacker could block communications by transmitting a powerful and disruptive signal. Key management, the means of generating, distributing, storing, using, renewing and removing keys, is another area of concern for wireless public safety services. For example, over-the-air-rekeying, the means of renewing keys among wireless endpoints, requires additional security mechanisms unique to the wireless arena. Several of the above requirements may be fulfilled (or partially fulfilled) by the use of encryption technology. It is common to see Data Encryption Standard (DES) and triple DES employed in public safety services, and moving forward we can expect to see the use of Advanced Encryption Standard (AES). Much of the work is employing these schemes with the appropriate protocols.

One major concern that arises within the E911 space is the issue of false reports. The serious nature of this problem is easily realized by the consequence of a prank call tying up resources while a response to a real emergency is delayed. The methods of providing non-repudiation may be borrowed where applicable from existing security models. For example, a "handshake could occur where keys are exchanged in a manner that demonstrates the identity of the calling and called party (realize that the public safety answering point may also be spoofed). Presently in the PSTN, these false reporting events are addressed by law, in the form of felony crimes. A similar expectation is not unreasonable in future wireless space. The question that remains is whether the increase in the number of devices, the ease of spoofing, and other such differences, makes enforcement untenable.

Signaling: The network must provide a means of signaling session information. In the PSTN, this is provided by the SS7/IN and in the IP space this might be provided by Session Initiation Protocol (SIP).[5]

Order Processing: The network provider must support a means of prioritizing repairs and restorations. The complex Operational Support Systems (OSS) and Back-office Support Systems (BSS) that exist within the PSTN do not presently exist within most packet networks.

While not all of these functions are required to provide any one public safety service, together they represent a core set of requirements for the services we discussed in the previous section. With this said, it may turn out that only a subset of services (and therefore functions) will come to be expected of future networks. Further, new methods of performing these functions may evolve. Therefore the intent of the above list is to describe functionality regardless of how it is ultimately provided. Next, we will consider these functions with respect to a number of existing and emerging technologies.

Technologies

In this section, we will briefly examine an existing wireless set of standards, namely 802.11. This is not meant to be an exhaustive examination, it is only meant to be illustrative (and cursory at that).[6] We also briefly discuss the role of software defined radios and ultra wide band technologies with respect to public safety services.

---

[5] See [9]

[6] For example, we do not cover 802.16, Bluetooth, 3G/4G or Local Multipoint Distribution Service (LMDS) and Multichannel multipoint Distribution Service (MMDS) services. There are a number of other wireless options to consider for public safety services. This includes satellites, that while costly, can provide ubiquitous coverage and good diversity alternatives in disaster relief efforts.

802.11: 802.11 describes a family of wireless LAN standards.[7] These networks make use of unlicensed spectrum, which raises concerns of crowding and congestion. While these networks have been shown to be surprising resilient under heavy traffic loads [10], they do not support the QoS or PoS functionality described previously nor do they provide the level of reliability generally associated with public safety services. Furthermore, while 802.11 has been shown to support real-time services, [11] unlike 3G and 4G systems they were not designed for this purpose.[8] Another common complaint is the weak security protocols associated with 802.11 networks. These networks do not provide the security requirements discussed in the previous section. A final functionality to consider is that of location. The limited range over which 802.11 networks operate limits the geographic scope and subsequent location range of a user. However, there is no means of determining this location. Furthermore, even this limited range is too large to ensure a timely response to an emergency call. There are a number of possible solutions to the location problem.

Before leaving the topic, it might be interesting to consider a few experiments using 802.11 for public safety services. While 802.11 networks were designed for the portable environment, it turns out that they support high mobility as well. An experiment by the California Department of Transportation showed that an 802.11b network could support service to a vehicle moving at 70 mph. [13] This suggests a role for their use in highway patrol cruisers. Other experiments have shown 802.11b useful in supporting novel emergency services. For example, a new medical messaging service has been developed to receive data on FM sub-carrier (including RDS, DARC, or SuperDARC formats) and retransmit on 802.11b. In this service, the ambulance essentially becomes an 802.11 access point, allowing medical messages to be transmitted up to a mile. [14]

Two other technologies, Software Defined Radio (SDR) and Ultra Wideband (UWB), while not network protocols will likely have a profound impact on future wireless networks. Rather than consider the ability of this technology to support all of the afore mentioned functions, we describe a few specific applications that they may enhance.

Software Defined Radio: SDR provides a multiband, multimode radio technology. This allows users to change modulation type, operation mode, radiation power, and air interfaces. This brings such benefits as interoperability among dissimilar services and novel security services. SDR technology could support interoperability with existing wireless services and integration with new services. It could also provide the ability for public safety users to quickly negotiate into less congested spectrum during times of emergency. [15]

Ultra Wideband: UWB is defined as a wireless technology that makes use of more than 1.5 GHz of spectrum. The concept is to make use of broad ranges of spectrum often at low power. Such technology can co-exist on other service spectrum without inference and thereby make large amounts of spectrum and high rate services available. UWB brings the ability to reduce spectral congestion, minimize interference among devices, reduce power requirements, improve security and minimize interference from multipath interference. [16] The UWB signal provides a low probability of interception and detection, thereby increasing security and creating novel alternate path communications. This could be a useful security tool for public safety users. It is worth mentioning that a number of concerns do exist regarding the potential for interference of UWB with other services. The FCC recently addressed this problem in a Report and Order. [17]

Considerations

In this section, we examine the applicability of public safety services in future wireless networks. The question is whether these services are relevant and/or appropriate to future wireless networks. Rather than propose an answer to this question, we raise of number of important considerations. While we will consider several policy related issues, we will not examine policy specifically in this paper.[9]

Expectation: It is important to realize that future public safety services will likely be quite different from those provided in the PSTN space. For example, voice might be replaced with text messaging or it might be expanded to full voice, video and telemetry. While emerging wireless services will create new problems they will also offer new services (video), alternate devices, increased penetration, neutral platforms, flexibility and additional information. There may be a tradeoff among the inability to offer traditional services and the ability to offer new services (limited service support over broader coverage). The base expectations for what qualifies as a public safety service will likely change as new platforms and devices emerge.

Offering: One point worth considering is the distinction that could be made between a service that is held out as commercial "for fee (e.g., cellular service)

[7] While the standards include 802.11, 802.11a, 802.11b and 802.11d, we will look only at 802.11a and 802.11b.

[8] One advantage of 3G is that its PSTN-based architecture should rather readily support the network control traditionally applied to public safety services. 4G service is expected to provide much higher rates and support such services as voice and video. In that this is a very nascent technology there is good opportunity to integrate new public safety services into 4G. [12]

[9] Numerous federal actions have recently occurred regarding wireless public safety issues. Many of the actions focus on spectrum issues concerning public safety spectrum, while others have included such issues as priority access services waivers. While these issues are quite relevant to the topic of this paper, we do not have the space to address them.

and one that is not. The point being that a commercially offered service might have a higher expectation for providing public safety services. This notion of "holding out of a service may have some relevance in the legal and regulatory space, which is beyond the scope of this work.

Cost: To understand the appropriateness of public safety services requires some form of cost/benefit analysis. This cost analysis can be based on the direct, indirect or exogenous costs, with varying implications. Cost will be a major driver in the success or failure of such services. Note that the cost for such services may also be forced upon carriers by regulatory policy.

Diversity: The diversity of access options is a key reason to consider wireless support for public safety communications. Wireless networks would provide alternative communications channels in the event wireline networks were rendered inoperable. They also provide coverage in areas that might not otherwise be reached. In this sense, it would provide reliability and availability through diversity.

Accessibility: Should public safety functions allow a user to log into a network on which they do not have an account in order to allow that user to report an emergency event? Will network operators block interoperability with a possible negative impact on public safety services? In this way accessibility may be viewed as an access control problem.

Deployment: To avoid false starts, a number of initial requirements could be defined and considered for each service. Consideration must be made regarding the degree to which these requirements are implemented. Care should be taken not to spend too much time creating a complete implementation, without interim deployment cycles. For example, an interim IM based 911 service for 802.11 based devices could be implemented well in advance of a full-blown voice based E911 service. Coordination of local, state, federal and industry players will play an important role in the short and long term deployment and integration of public safety services.[10]

Interoperability: Interoperability with legacy public safety systems will be crucial. The PSTN can serve as a common platform on which other networks interconnect. However, the PSTN was created to support voice and thereby might be viewed as limiting emerging functionality such as video and high rate data. A question to consider is how will the new system integrate with existing systems and other new systems? Are there international interoperability issues? Technology will both provide solutions and additional problems for interoperability among so many disparate technologies and devices. Interoperability will have to include higher layer specifications, such as new extensible markup language (XML) formats and other application layer functionality, as well as the operational and back office support systems. Independence of the application from the transmission mode may be key to interoperability and backward compatibility with other public safety services, but this does not ensure that the application can necessarily interoperate or provide the functions needed for public safety functions.

Openness: The openness of these technologies may be relevant to their success in supporting public safety services. Openness is a broadly used term and may include aspects of design, agreement, process or more. Some questions to consider include: Will this system be based on "open, non-proprietary standards? Will the interfaces to the operating system be available for developers? Will the process require regulatory intervention? What, if any, security issues does open or closed design create?

As we have demonstrated, there are many factors to consider regarding the applicability of public safety services to future wireless networks and each of these factors has a set of questions to ponder. A difficulty arises in defining expectation and functionality of devices that do not yet exist. Another difficulty that exists is that of moving away from traditional expectations set by previous technology that might not be applicable in the future.

Conclusions

In this paper, we examined the functionality required of future wireless networks to support public safety services. We began by examining some of the architectural changes that are making this assessment necessary. We also examined existing technologies in order to determine the extent to which these technologies might support public safety services. We closed by discussing the applicability of public safety services in future wireless networks.

There are several issues that should be considered regarding public safety in the development of new wireless technologies. The first is that the architectural changes in emerging wireless networks will impact the manner in which public safety services are provided. The second issue to consider is that existing public safety services require a significant set of functions. The third issue to consider is that existing wireless networks may not provide the functionality associated with PSTN based public safety services. This brings us to consider the applicability of public safety services to future networks

[10] Within the public safety community various groups are looking at the role of wireless networks. One effort is the Public Safety Wireless Interoperability National Strategy (WINS). They are involved in promoting and interoperability efforts in wireless public safety networks. Project Mobility for Emergency and Safety Applications (MESA) [18] and Capital Wireless Integrated Network (CapWIN) provides a focus on the administrative, operational, and interoperability issues of existing wireless services. ITU E.106 represents new standards for emergency telecommunications services. [19] While this work is developing useful output, they are not presently focusing on the next generation wireless services issues.

and the notion that some NS/EP services may be provided in a different way on emerging networks and additional NS/EP services that are not currently provided on legacy networks may be provided by emerging networks. As we have attempted to demonstrate, it can be difficult to determine how applicable certain public safety services are for new technology, particularly since these technologies are so fundamentally different from existing technology.

While we do not recommend that government dictate public safety requirements for future wireless services, neither do we perceive this as an excuse to step away from supporting such services. By allowing new devices to support a general public safety functionality, we will increase public safety connectivity and availability. It might be prudent from the start to make a cursory analysis of what issues might arise for a particular technology implementation of public safety. This type of general analysis has precedence. Consider the 'security' section of an Internet Draft or efforts underway within the disabilities community to raise awareness of accessibility problems. The outcome of such an analysis could be as simple as 'it is not presently feasible or applicable'.

References

[1] *Revision of the Commission's Rules to Ensure Compatibility with Enhanced 911 Emergency Calling Systems*, CC Docket 94-102, RM-8143, Notice of Proposed Rulemaking, 9 FCC Rcd. 6170 (1994) (E911 NPRM).

[2] *GETS*, http://gets.ncs.gov

[3] *WPS,* http://www.ncs.gov/N2/wps

[4] *CPS*, http://www.ncs.gov/N2/Wps/cps1.html

[5] *TSP*, http://www.ncs.gov/tsp/briefing_hi_body1.html

[6] *A Report on Technical and Operational Issues Impacting The Provision of Wireless Enhanced 911 Services,*http://gullfoss2.fcc.gov/prod/ecfs/retrieve.cgi?native_or_pdf=pdf&id_document=6513296239

[7] *WPS*, http://63.121.95.245/wps/info_body.html and www.ncs.gov/N2/wps

[8] *Emergency PSTN Features*, http://www.ietf.org/internet-draft/draft-otty-ieprep-pstn-features-00.txt

[9] "Providing Emergency Services in Internet Telephony Schulzrinne H. and Knarig, A, www.computer.org/internet, June, 2002.

[10] *Testbed-based Performance Evaluation of VoIP over Wireless & Wired LANs*, http://www-sop.inria.fr/planete/qni/VoIP_wireless.pdf

[11] *Voice over 802.11,* http://www.80211-planet.com /news/article.php/1015241

[12] *4G Applications and Services*, http://www.pswn.gov/library/pdf/wireless_technologies_one.pdf

[13] *Towards Distributed Data Collection and Peer-to-Peer Data Sharing*, http://www.its.uci.edu/its/publications/papers/AS-WP-02-4.pdf

[14] *Roadside Telematics and Cue to Deliver Emergency Medical Messaging Over 802.11 and Bluetooth,* http://www.roadmedic.com/news/may0601.htm

[15] *Software-Enabled Wireless Interoperability Assessment Report,* http://www.pswn.gov/admin/librarydocs9/software_defined_radio_report_final.pdf

[16] *Ultra Wideband Communications,* http://www.pswn.gov/admin/librarydocs8/Emerging_Wireless_Technologies-Part4.pdf

[17] *Docket 8-153*, http://wireless.fcc.gov/publicsafety/2002docs.html and http://www.pswn.gov/admin/librarydocs10/uwb_gps_final.pdf

[18] http://www.projectmesa.org

[19] *E.106*, http://www.itu.int/ITU-T/studygroups/com16/ets/