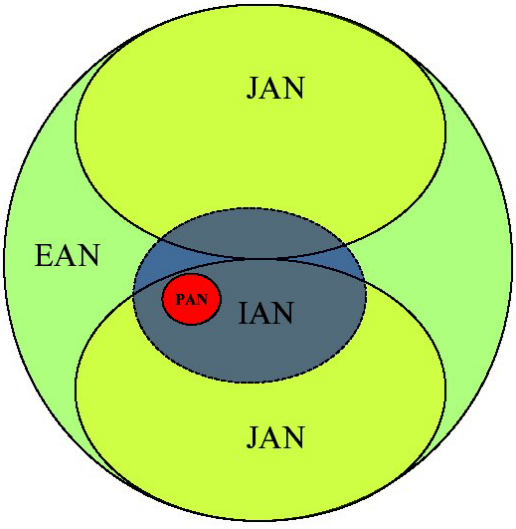
Wireless Technologies and the SAFECOM SoR for Public Safety Communications

Leonard E. Miller
Wireless Communication Technologies Group
Advanced Network Technologies Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, Maryland

2005



Cover photo: Santa Clara County antenna farm, from http://www.sccfd.org/frequencies.html

Wireless Technologies and the SAFECOM SoR for Public Safety Communications

Preface

The Problem: Lack of Capacity, Interoperability, and Functionality

National assessments of public safety communications (PSC) that were made in the 1990s found that the nation's public safety agencies faced several important problems in their use of radio communications[1]:

- *First*, the radio frequencies allocated for Public Safety use have become highly congested in many, especially urban, areas….
- *Second*, the ability of officials from different Public Safety agencies to communicate with each other is limited…. Interoperability is hampered by the use of multiple frequency bands, incompatible radio equipment, and a lack of standardization in repeater spacing and transmission formats.
- *Finally*, Public Safety agencies have not been able to implement advanced features to aid in their mission. A wide variety of technologies—both existing and under development —hold substantial promise to reduce danger to Public Safety personnel and to achieve greater efficiencies in the performance of their duties. Broadband data systems, for example, offer greater access to databases and information that can save lives and contribute to keeping criminals "off the street." Video systems promise better surveillance capabilities, increased use of robotics in toxic and hazardous environments, and better monitoring and tracking of both personnel and equipment.

The national assessments of PSC have had significant impact on legislation, regulation, and funding.

Since these assessments, significant reallocations of spectrum for PSC have been made through regulation. Also, through "refarming" (revising spectrum channel plans to implement narrower channels) and the standardization of trunking technologies, the efficiency of spectrum use by PSC is being addressed. Standards for PSC equipment have been written that improve the interoperability of radio systems from different vendors, and the need for interoperability in all its aspects is being dealt with systematically. Increased funding has enabled the upgrading of many local and regional PSC systems.

In this report, the potential use of new wireless technologies "to implement advanced features to aid in their mission" is reviewed in the light of national efforts to define user requirements for next-generation PSC systems.

User-Defined Requirements for Next-Generation Systems

The SAFECOM Statement of Requirements (SoR), released in April 2004, envisions PSC operations as taking place in a networking environment that is capable of operating as a "system of systems" in order to satisfy the requirements of public safety agencies for communication

[1] Final Report of the Public Safety Wireless Advisory Committee to the Federal Communications Commission and the National Telecommunications And Information Administration, 11 September 1996.

systems that provide increased functionality and efficiency, in addition to built-in interoperability. That is, wireless devices, local networks, regional networks, and wider area networks are envisioned as being able to "work together to pass information back and forth seamlessly."[2] The SoR lists the following system elements:

- PSC devices (PSCDs), which are handheld or wearable radios.
- Personal Area Networks (PANs), which permit wireless data sharing among PSCDs and sensors attached to an individual first responder, including data on the location, environment, and physical condition of that individual.
- Jurisdictional Area Networks (JANs), which are the permanent network infrastructure in particular cities or areas that are dedicated to PSC, capable of connecting to larger area networks.
- PSC user groups, which are sets of devices and/or personnel that are recognized by the system as authorized (either permanently or temporarily) to share communication and information, and that access portions of the existing network infrastructure as necessary, or forming an ad hoc network among themselves in the absence of an infrastructure.
- Incident Area Networks (IANs), which are temporary network infrastructures brought to the scene of an incident or otherwise configured for an incident.
- Extended Area Network (EAN), which consists of regional, state, and national network resources, particularly those dedicated to public safety communications.

The SoR is concerned not only with interoperability, but also with enhanced functionality and performance of PSC systems, described qualitatively in terms of several representative usage scenarios. Later versions of the SoR will translate the functional requirements into quantitative requirements.

Enabling Wireless Technologies

In this report, we describe the current and emerging wireless communication technologies that are likely to provide the functionality and performance that are needed for user-defined PSC applications and scenarios. The components of the "system of systems" that are considered in this report, and the wireless technologies that are likely to implement them, are the following:

- PANs: Bluetooth and other wireless PAN technologies.
- JANs: IEEE 802.16e mobile broadband wireless networking and mesh networking technologies.
- IANs: IEEE 802.11 wireless local area networks and wireless ad hoc networking technologies.

The descriptions of these technologies are tutorial and are intended for people at all levels of the effort to improve PSC. In an appendix to this report, background details are provided for selected aspects of the technologies.

[2] "Statement of Requirements for Public Safety Wireless Communications and Interoperability," SAFECOM, Version 1.0, 10 March 2004.

Table of Contents

Preface iii
Table of Contents v
List of Figures vii
List of Tables viii
1. Introduction 1
1.1 Interoperability Continuum for Public Safety Communications 1
1.1.1 Elements of Interoperability 1
1.1.2 The Role of Technology in Achieving Interoperability 1
1.2 Ongoing Interoperability Standards Efforts 1
1.2.1 Project 25 3
1.2.2 Project MESA 4
1.3 The SAFECOM SoR 5
1.3.1 Network Architecture 6
1.3.2 Scenarios 7
1.3.3 Qualitative Description of Communication Requirements 9
1.4 Wireless Technologies Covered in This Report 11
2. Personal Area Network Technologies 12
2.1 What Is a Wireless PAN? 12
2.1.1 WPAN as Distinguished From WLAN 12
2.1.2 IEEE 802.15 Series of WPAN Standards 13
2.2 802.15.1 (Bluetooth) Description 14
2.2.1 Bluetooth Network Topology 14
2.2.2 Service Discovery Protocol and Profiles 15
2.3 802.15.3 Description 16
2.3.1 Original IEEE 802.15.3 High-Rate WPAN (Wi-Media) 16
2.3.2 Alternate PHYs for 802.15.3 19
2.4 802.15.4 Description 21
2.4.1 IEEE 802.15.4 Applications 21
2.4.2 IEEE 802.15.4 Technical Features 22
3. Incident Area Network Technologies 25
3.1 The IEEE 802.11 Wireless Standards 25
3.2 Basics of WLAN Networking 26
3.2.1 WLAN Networking Modes 26
3.2.2 Data Handling for Wireless Transmission 27
3.2.3 Channel Access Techniques 28
3.2.4 Bridging and Wireless Distribution System 29
3.3 Ad Hoc Networking 30
3.3.1 The Potential of Ad Hoc Networks 31
3.3.2 MANET Routing Protocols 32
4. Jurisdiction Area Network Technologies 36
4.1 Prospects for Broadband PSC 36
4.1.1 Opportunities at 700 MHz 36
4.1.1.1 The Greenhouse Project 38

4.1.1.2 Progress Toward PSC in the 700 MHz Band 39
4.1.2 PSC Opportunities at 4.9 GHz 39
4.2 Enabling Technologies for Broadband PSC JANs 41
4.2.1 WiMAX (IEEE 802.16) 41
4.2.2 Mesh Networking 44
5. Appendix: Tutorials on Wireless Technology 48
5.1 Tutorial on Packet Radio 48
5.1.1 Channel Access Protocols 48
5.1.2 Multihop Packet Routing Protocols 51
5.2 Tutorial on Digital Voice 54
5.3 Tutorial on VoIP 56
5.3.1 VoIP Basics 57
5.3.2 Wired and Wireless IP-PBX 58
5.3.3 Voice Over WLAN 59
6. References and bibliography 61
6.1 Cited References 61
6.2 Additional Bibliography 65

List of Figures

Figure 1.1.1 Interoperability Continuum (from [1]). 2
Figure 1.2.1 Interoperability of Project 25 radios (from [3]). 3
Figure 1.2.2 Grouping of Project 25 standards documents (IS = Interim Standard) (from [4]). ... 4
Figure 1.3.1 Conceptual relationships among PAN, IAN, JAN, and EAN (from [8]). 7
Figure 1.3.2 Format for information in the SoR (from [11]). 9
Figure 1.3.3 View of PS technology migration (from [8]). 10
Figure 2.2.1 Bluetooth basic network topology (based on [13]). 14
Figure 2.2.2 Alternating master-slave packet transmissions (from [12]). 15
Figure 2.3.1 Multimedia cable replacement with high-rate wireless networking (from [18]). ... 17
Figure 2.3.2 Elements of an IEEE 802.15.3 piconet (based on [17]). 18
Figure 2.3.3 802.15.3 superframe structure (from [16]). 18
Figure 2.3.4 Example of a dependent piconet. 19
Figure 2.3.5 FCC emissions mask for average radiation by UWB devices (from [19]). 20
Figure 2.4.1 Example variety of objects networked using IEEE802.15.4 (from [22]). 21
Figure 2.4.2 Channels available to 802.15.4 low-rate WPAN (from [22]). 22
Figure 2.4.3 Optional IEEE 802.15.4 frame structure (from [22]). 23
Figure 2.4.4 Types of Zigbee links based on nodes with different capabilities (from [24]). 24
Figure 3.2.1 Infrastructure and ad hoc modes of WLAN operation (from [26]). 27
Figure 3.2.2 Contention Access in IEEE 802.11 28
Figure 3.2.3 Hidden terminals and exposed terminals. 29
Figure 3.2.4 Carrier-sense Multiple Access (CSMA) with Collision Avoidance (CA) 29
Figure 3.2.5 Multihop WDS (from [27]). 30
Figure 3.3.1 Mobile ad hoc network scenario (from [30]). 31
Figure 3.3.2 Increased wireless system performance using ad hoc networking (from [31]). 32
Figure 3.3.3 Proactive MANET routing protocol comparisons (from [30]). 33
Figure 3.3.4 On-demand MANET routing protocol properties (from [30]). 34
Figure 3.3.5 A possible classification of ad hoc routing protocols (from [33]). 34
Figure 4.1.1 Selectable per-carrier modulations in the SAM system (from [38]). 37
Figure 4.1.2 Comparison: FCC mask for 4.9 GHz with 802.11, DSRC masks (from [45]). 41
Figure 4.2.1 Adaptation of 802.16 data modulation to link conditions (from [48]). 42
Figure 4.2.2 Comparison of single-carrier and OFDM modulations (from [50]). 43
Figure 4.2.3 Mesh network for residential broadband access system (from 55]). 45
Figure 4.2.4 Mesh network providing broadband access to a city (from [56]). 45
Figure 4.2.5 Mesh connectivity around obstacles to propagation (from [55]). 46
Figure 4.2.6 Use of mesh technology to extend the range of a WLAN (from [57]). 46
Figure 4.2.7 Mesh networking control of ad hoc connectivity (from [58]). 47
Figure 5.1.1 ALOHA packet radio network (based on [61]). 49
Figure 5.1.2 Theoretical performance of ALOHA and Slotted ALOHA. 50
Figure 5.1.3 Throughput performance of CSMA for ideal condition of zero propagation delay. 51
Figure 5.1.4 100-node mobile network topology having full connectivity (from [68]). 52
Figure 5.1.5 Multihop communication 52
Figure 5.1.6 Effect of radio transmitter range on throughput and delay (from [30]). 53
Figure 5.1.7 Hierarchical labels of repeaters and stations (from [69]). 54

Figure 5.2.1 Quality of digital speech in terms of MOS (“mean opinion score”) vs. bit rate for different types of voice coding (from [71]). 55
Figure 5.2.2 MOS ranking of different vocoders for Project 25 selection (from [73]). 56

List of Tables

Table 4.1.1 Band plan for 700 MHz public safety spectrum (from [36]). 37
Table 4.1.2 Total data rates for SAM for different available bandwidths (based on [38]). 37
Table 4.1.3 State and Local Public Safety Frequency Allocations Above the 800 MHz Band... 40
Table 5.2.1 MOS ranking and quality scale (from [72]). 55

1. Introduction

In this introductory section, we briefly consider what is involved in achieving interoperability in public safety communications (PSC), including the role of technology, and as background we summarize ongoing PSC standardization programs.

1.1 Interoperability Continuum for Public Safety Communications

It is well known that interoperability among different local public safety organizations, such as fire departments, depends a great deal on the willingness of the participants to work together—as much as, if not more than, how their radios work together. However, it is not always appreciated that interoperability has to take place at many different levels in order to be effective.

1.1.1 Elements of Interoperability

The SAFECOM program of the Department of Homeland Security (DHS) has developed the concept of an "interoperability continuum" to "help the public safety community and local, tribal, state, and federal policy makers address critical elements for success as they plan and implement interoperability solutions" [1]. As illustrated by the graphic in Figure 1.1.1, these elements include governance, standard operating procedures (SOPs), technology, training and exercises, and usage of interoperable communications.

For example, in the element of governance, the minimal level of interoperability occurs when individual agencies work independently, while the optimal level occurs when individual agencies participate in regional and statewide interoperability committees.

1.1.2 The Role of Technology in Achieving Interoperability

While technology is only one element of interoperability, it is very important. As Figure 1.1.1 suggests, a minimal type of interoperability between local agencies can be achieved by having them "swap" each other's radios, in effect creating an overlap in their PSC implementations. A more sophisticated solution is to provide gateway equipment that will allow messages to be patched from one radio system to another. Better interoperability is of course achieved if the local agencies shared spectrum channels (simplifying the requirements for patching) and the best solution is for no patching to be required at because the agencies use compatible equipment—either from the same vendor or based on a common standard.

In what follows, as background we describe ongoing interoperability standardization efforts.

1.2 Ongoing Interoperability Standards Efforts

Ongoing PSC radio interoperability standards efforts are taking place under the Project 25 (P25) program and, internationally, under Project MESA. Much has been accomplished, but much remains to be done.

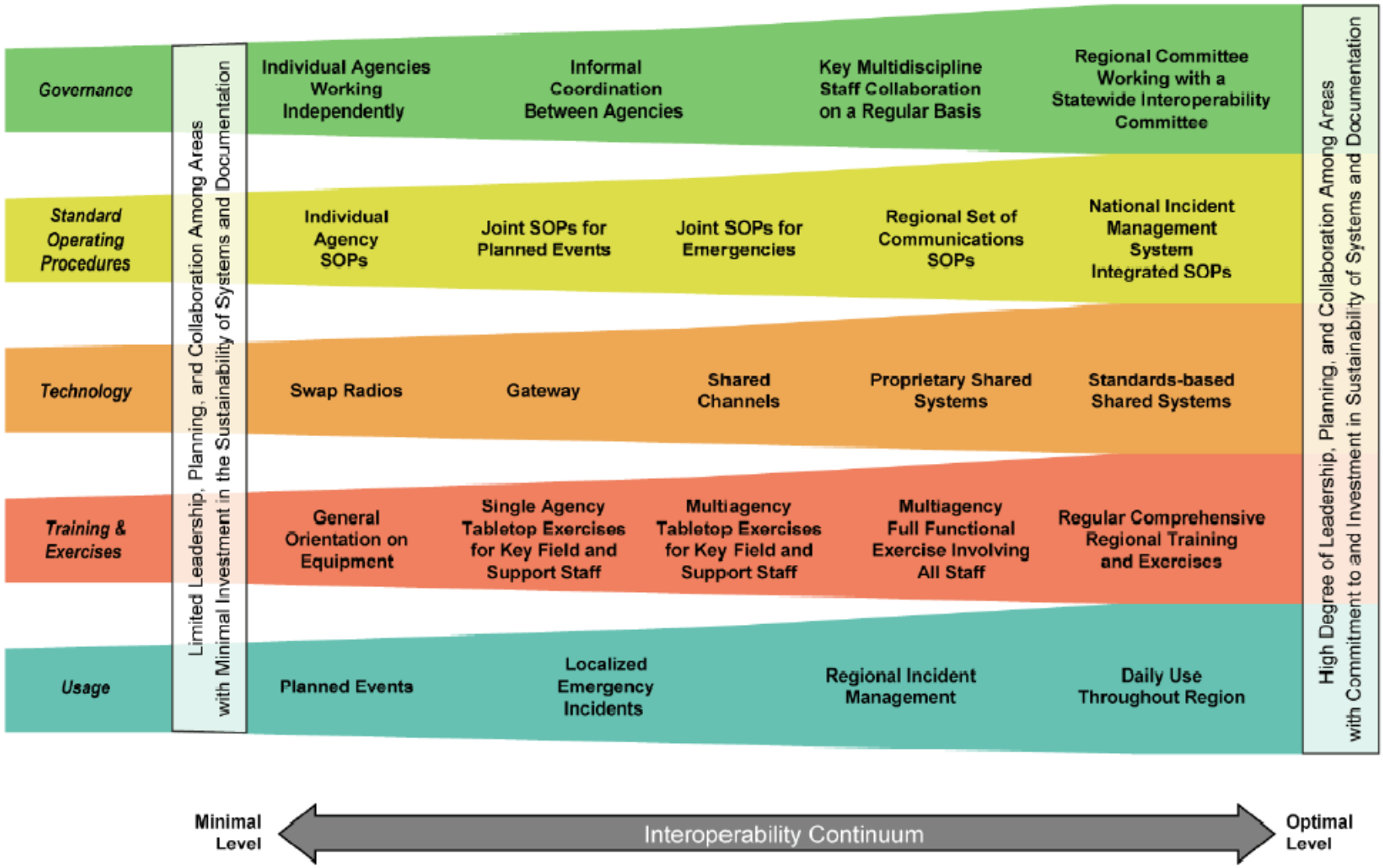


Figure 1.1.1 Interoperability Continuum (from [1]).

1.2.1 Project 25

Representatives from the Association of Public Safety Communications Officials International (APCO), the National Association of State Telecommunications Directors (NASTD), selected Federal agencies, and the National Communications System (NCS) established Project 25 (P25), a steering committee for selecting voluntary common system standards for digital public safety radio communications. The Telecommunications Industry Association (TIA) committee, TR-8, facilitates such work through its role as the ANSI-accredited Standards Development Organization (SDO), and has developed in TR-8 the 102-series of technical documents. [2]

Phase I P25-compliant radios can communicate in analog mode with legacy radios, and in either digital or analog mode with other P25 radios, as illustrated in Figure 1.2.1. The P25 suite of standards involves digital Land Mobile Radio (LMR) services for local, state and national (federal) public safety organizations and agencies.

The scope of the Project 25 effort is indicated by the documents grouping envisioned in Figure 1.2.2. An overall standards document, TSB102 (denoted Interim Standard (IS) 102 in the figure), provides definitions and a systematic structure for the collection of standards. Standards titled TSB102A__ deal with protocols to support various services, such as control and encryption. Standards titled TSB 102B__ deal with radio and networking system interface issues, including the specification of radio waveforms, data formats, and a common vocoder operation. Standards titled TSB 102C__ deal with equipment issues, such as test and measurement.

P25 Phase II implementations will involve time and frequency modulation schemes (e.g., TDMA and FDMA), with the goal of improved spectrum utilization. Significant attention is also paid to interoperability with legacy equipment, interfacing between repeaters and other subsystems, roaming capacity and spectral efficiency/channel reuse. In addition, Phase II work involves console interfacing between repeaters and other subsystems, and man-machine interfaces for console operators that would facilitate centralized training, equipment transitions and personnel movement.

Figure 1.2.1 Interoperability of Project 25 radios (from [3]).

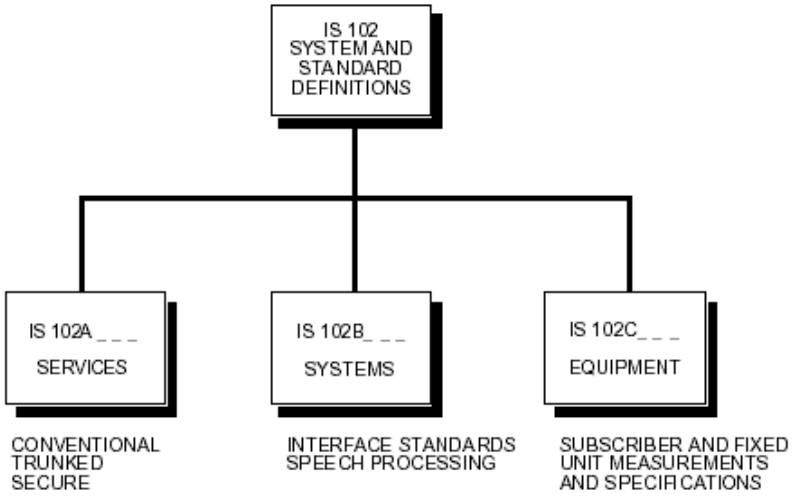


Figure 1.2.2 Grouping of Project 25 standards documents (IS = Interim Standard) (from [4]).

1.2.2 Project MESA

P25 Phase III planning activities are addressing the operation and functionality of a new aeronautical and terrestrial wireless digital wideband/broadband public safety radio standard that could be used to transmit and receive voice, video and high-speed data in a ubiquitous, wide-area, multiple-agency network. The European Telecommunications Standards Institute (ETSI) and TIA agreed to collaborate on next-generation mobile broadband specifications for public safety users. The initial partnership agreement was ratified by TIA and ETSI in 2000 and in 2001 it was Project: Project MESA (Mobility for Emergency and Safety Applications). Other regional standards groups (*e.g.*, Asia and Canada) and international organizations (*e.g.*, UN/NATO) are also becoming engaged in Project MESA activities.

Project MESA exists to facilitate dependable, advanced, efficient, effective and inter-operable equipment, specifications and applications that are involved with public safety-oriented broadband communication needs. Additionally, MESA will attempt to harmonize existing specifications and scenarios as part of its mandate. The end result will be a suite of standards and specifications harmonized for broadband terrestrial mobility operations, including con-nectivity to broadband satellite communications services, driven by common scenarios and spectrum allocations. Benefits to the Public Safety community and to the citizens they serve, will be realized in two distinct but highly related areas [5]:

- System end-users:
    - In-building, portable voice and data coverage.
    - Real-time support for wireless portable computer applications.
    - Rapid messaging, including email, free-form text, and file transfers.
    - Constantly updated personnel and equipment location data.
    - Aerial video for major events, or disaster response coordination.
    - Transmission and reception of high-resolution digital images.
    - Satellite connectivity of disaster “hot-spots.”

  - Real-time incident video and Internet protocol (IP) voice communications overlay.
  - Full robotics remote control, including audio/video monitoring and transmission.
  - Remote sensing and aeronautical connectivity (Air-Ground-Air).
  - Economies of scale for Public Safety equipment acquisition; also allowing for increased Public Safety Department access to technology and information.
- System owner/operators:
  - Local, national, regional and international interoperability.
  - Frequency neutral technology.
  - Accommodation of multiple agency networks.
  - Network authentication and encryption.
  - Competition in system life cycle procurement.

1.3 The SAFECOM SoR

The SAFECOM document, "Statement of Requirements for Public Safety Wireless Communications and Interoperability" [6], is dated 10 March 2004 and was made available publicly from the SAFECOM website in April 2004. The document has the following major sections:

- Section 1, "Public Safety Requirements and Roles," defines public safety communication needs and public safety roles and functions.
- Section 2, "Communications Services Definition," defines communications services—interactive and non-interactive voice communications, and interactive and non-interactive data communications.
- Section 3, "Public Safety Wireless Communications Scenarios," outlines several public safety scenarios based on typical operations to provide a view of desired future public safety communications capabilities and modes of operation.
- Section 4, "Operational Requirements of Public Safety for Wireless Communications and Information," identifies the wireless communications operational needs of public safety.
- Section 5, "Wireless Communications Functional Requirements," defines the wireless communications functional requirements corresponding the scenarios and operational requirements.
- A complete glossary of the terminology and acronyms used in the document.
- An appendix containing a list of desired system capabilities that was developed at the SAFECOM-AGILE-NIST Summit on Interoperable Communications for Public Safety [7].
- An appendix containing a number of additional operational scenarios.

1.3.1 Network Architecture

The SAFECOM Statement of Requirements (SoR), released in April 2004, envisions PSC operations as taking place in a networking environment that is capable of operating as a "system of systems" in order to satisfy the requirements of public safety agencies for communication systems that provide increased functionality and efficiency, in addition to built-in interoperability. That is, wireless devices, local networks, regional networks, and wider area networks[3] are envisioned as being able to "work together to pass information back and forth seamlessly" [6]. The SoR lists the following system elements:

- PSC devices (PSCDs), which are handheld or wearable radios.
- Personal Area Networks (PANs), which permit wireless data sharing among PSCDs and sensors attached to an individual first responder, including data on the location, environment, and physical condition of that individual.[4]
- Jurisdictional Area Networks (JANs), which are the permanent network infrastructure in particular cities or areas that are dedicated to PSC, capable of connecting to larger area networks.
- PSC user groups, which are sets of devices and/or personnel that are recognized by the system as authorized (either permanently or temporarily) to share communication and information, and that access portions of the existing network infrastructure as necessary, or forming an ad hoc network among themselves in the absence of an infrastructure.
- Incident Area Networks (IANs), which are temporary network infrastructures brought to the scene of an incident or otherwise configured for an incident.
- Extended Area Network (EAN), which consists of regional, state, and national network resources, particularly those dedicated to public safety communications.

The relationship among these network concepts is illustrated by the diagram in Figure 1.3.1. The diagram is intended to highlight the fact that JANs are subsets of EANs, both in terms of facilities and in terms of network access/connectivity. Since an IAN is defined as a temporary network infrastructure, its facilities are presumably not part of its corresponding JAN or of the EAN; the diagram in Figure 1.3.1 therefore represents the connectivity—generally cross-jurisdictional, requiring interoperability—that an IAN would be set up to use. The figure implies that a PAN is a subset of an IAN, which is true when there is an incident and the data from a PAN is accessible to the IAN and vice versa. A clearer sense of the SoR's meaning regarding these concepts is gained from seeing the hypothetical interactions between the different networks that are described in the example scenarios included in the SoR.

[3] The accepted terminology in referring to the scope of particular networks and technologies includes the terms local area network (LAN), metropolitan area network (MAN), and wide area network (WAN). The SoR avoids identifying the elements of its PSC system architecture closely with any of these networks by using new terminology that is specifically oriented to public safety users.

[4] The term PAN is generic, while "wireless PAN" (WPAN) is a trademark of the IEEE 802.15 working group.

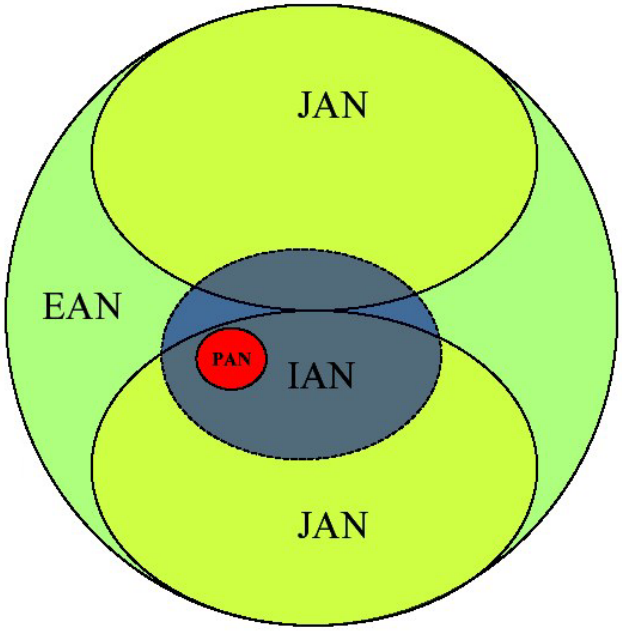


Figure 1.3.1 Conceptual relationships among PAN, IAN, JAN, and EAN (from [8]).

1.3.2 Scenarios

The SAFECOM SoR describes a vision for desired advancements in public safety wireless communications capabilities by means of illustrative, hypothetical scenarios involving emergency medical services, fire and rescue services, law enforcement, and combinations of these public safety services. The level of detail in the scenarios varies, and is intended to highlight particular desired aspects of future public safety communications in the 2004-2019 timeframe.

The scenarios provide descriptions of the voice and data communications used under various circumstances, and are summarized in the SoR as follows:

- Routine, day-to-day operations[5]
  - EMS: heart attack. Throughout the scenario, the ambulance, the paramedic team, and the patient are tracked by the network providing geolocation information in real time. All patient information and vitals are recorded through wireless monitors and voice recognition systems with no reliance on paper reports and notes. All EMS hospital staff orders as well as paramedic treatments are recorded by the hospital and ambulance databases. All monitors and devices used with the patient are wireless to allow easy patient transport and mobility. All conversations between dispatcher and paramedics and between paramedics and hospital staff are conference call, simultaneous (multiuser full duplex) discussions.
  - Fire: residential fire. Throughout the scenario, the fire personnel and equipment, EMS support personnel, and the fire victims are tracked by the network providing

[5] An often-quoted principle of public safety communications technology is that equipment that is not used on a daily basis will not be relied upon in an emergency.

geolocation information in real time, providing the Incident Commander (IC) with current accountability of public safety personnel and of the fire's victims. All victim information and vitals are recorded through wireless monitors and voice recognition systems with no reliance on paper reports and notes. All fire personnel and equipment have monitors to measure vital conditions and status that are reported by the wireless PAN and IAN systems to the IC's GIS. The GIS also has access to city building department databases, which are searched and queried for building information and plans, fire hydrant locations, etc.

  - Law Enforcement: traffic stop. Throughout the scenario, the law enforcement personnel and equipment as well as the arrested suspect are tracked by the network providing geolocation information in real time to provide the field supervisor as well as dispatch with current accountability of all personnel. All suspect information and evidence are recorded through wireless monitors and voice recognition systems with no reliance on paper reports and notes. All information is tagged with the original officer's identity code. All evidence is tracked with RFID tags to provide an audit trail. All law enforcement personnel and equipment have monitors to measure vital conditions and status that are reported by the wireless PAN and IAN systems to the IC's GIS. National and state criminal-justice records and state civilian records are searched and queried for information relating to the traffic stop, etc.

- Multi-discipline, multi-jurisdiction
  - An explosion at a chemical plant. The abstracted view of Incident Command is very different than that of a first responder reacting to a situation in the field. As such, their communications needs and capabilities are tailored to meet those differences. While the communications and actions depicted in the scenario are oversimplified versions of what would actually have occurred in real life, what has been captured is the general nature of the communications, the command and control functionality, and examples of access to a wide variety of information on an on-demand basis. The command and control of Incident Command on-scene and the Emergency Manager provides for the safety and accountability of all the assets at the incident and provides information on additional resources that could be brought to the incident. The networks for communications and information exchange are created on an ad hoc and/or temporary basis at the scenes. They overlay on one another to provide interoperability and integrate with the larger jurisdiction area networks to form a system of systems for command and control.

These scenarios emphasize the many different kinds of wireless connections that are involved, as well as extensive use of GIS capabilities. In an appendix of the SoR, the following additional scenarios are presented, with an emphasis on the interoperation of the different entities' networks:

- Multi-discipline, within a local area
  - A pre-planned event (college football game)
  - A terrorist car bomb

- Multi-discipline, large-scale regional events
    - A hurricane
    - An earthquake

Project MESA has generated a similar statement of requirements document [9] for a future public safety communications "system of systems" that contains operational requirements described using scenarios. There is a greater variety of scenarios in the MESA SoR, but the SAFECOM SoR scenarios are more advanced in terms of details.

1.3.3 Qualitative Description of Communication Requirements

The SAFECOM SoR is a statement of *operational* and *functional* requirements and does not quantify the *technical* requirements of communication technologies that are needed to produce a system of systems that operates as described in the SoR's scenarios. However, the careful evaluation it contains of the needs of PSC practitioners is extremely valuable and is a necessary first step in the specification of next-generation PSC systems. For example, for each discipline (fire, police, emergency services), the SoR contains the information on operational and functional requirements that are shown in Figure 1.3.2.

To develop technical requirements for PSC system, the process will be to carefully analyze each scenario and to develop detailed estimates of communication system parameters such as required throughput, capacity, etc. that will specify the equipment and facilities that the system must possess. An effort to follow up the SoR with such specifications is being made in parallel with a similar effort under Project MESA [10].

It has been noted [8] that the realization of highly interoperable public safety communication systems faces several challenges, including the facts that

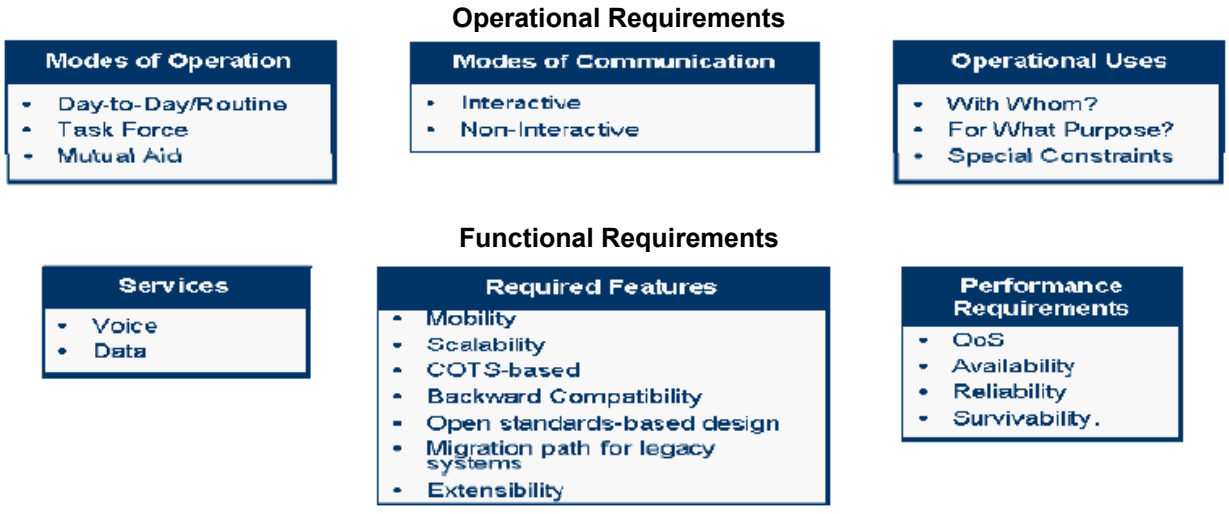


Figure 1.3.2 Format for information in the SoR (from [11]).

- Public safety communications infrastructure and equipment is often in use well past its useful life:
    - Outdated analog infrastructure exists in many jurisdictions
    - Many communications systems are up to 30 years old, rendering interoperability difficult
- Outdated equipment is unable to accommodate advanced features needed to support operations
- Agencies using equipment operating in disparate frequency bands cannot communicate with one another
- The use of proprietary technologies hinders the ability to interoperate with other agencies.

The development of more effective and interoperable public safety communication systems nationwide therefore involves multiple aspects of technology evolution and migration, as suggested in Figure 1.3.3 [8]:

- *Radio technology* continuing to migrate from conventional analog systems to conventional/analog trunked systems and in the future, to conventional/trunked digital systems.
- *Communication content* continuing to migrate from voice only to both voice and data and in the future, combined voice, data, images, and video.
- *System architecture* continuing to migrate from propriety architectures to open standards.
- *Interoperation* continuing to migrate from isolated communities to shared systems and, in the future, fully interoperable systems.

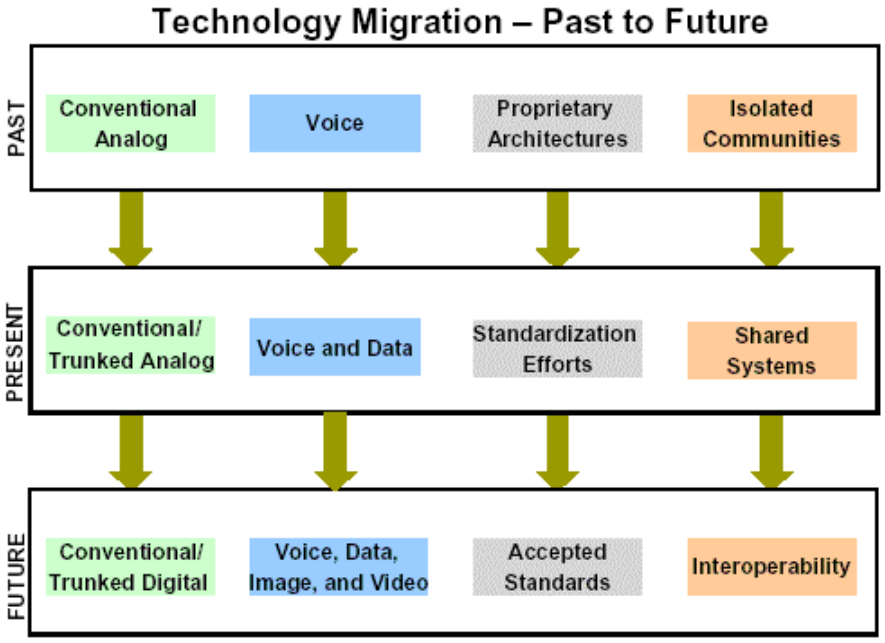


Figure 1.3.3 View of PS technology migration (from [8]).

1.4 Wireless Technologies Covered in This Report

There are of course many wireless technologies competing in today's marketplace for consumer, telecommunications, and other non-PSC applications. The application of any of them directly to the implementation of elements of the SAFECOM SoR's "system of systems" is not a certainty, even though it is very desirable to use commercial off-the-shelf (COTS) technologies to reduce costs. However, in a general way we can we speak of wireless technologies that are "relevant" to the different system elements, in that they are potentially applicable to PANs, IANs, and JANs. We do not consider EANs because for the foreseeable future this role is played by either the Internet or by a public safety version of the Internet, with "edge" or access by various gateway techniques.

In this sense, we can tentatively identify the following current wireless technologies with the system elements in the SAFECOM SoR [11]:

- Personal Area Network: One or more IEEE 802.15 wireless PAN protocols. These are discussed in Section 2.
- Incident Area Network: One or more IEEE 802.11 wireless LAN protocols. These are discussed in Section 3.
- Jurisdiction Area Network: In place of, or in conjunction with, current land mobile radio (LMR) systems, a mobile wireless broadband protocol such as IEEE 802.16e. These are discussed in Section 4.

2. Personal Area Network Technologies

In this section, we describe the several wireless personal area network (WPAN) technologies that exist today or are in the planning stage in the IEEE 802.15 Working Group. The potential application of each type of WPAN for public safety communications (PSC) depends on the capabilities of the particular WPAN technology, primarily in terms of data rates.

2.1 What Is a Wireless PAN?

The fastest growing wireless communication technology today is the wireless local area network (WLAN) technology based on the IEEE 802.11 series of standards. Because most people are familiar with how WLAN devices are used to provide network services to laptops and other non-fixed users, it is convenient to describe WPANs in terms of their differences with WLANs. Following that description,

2.1.1 WPAN as Distinguished From WLAN

The majority of WLAN applications (at least initially) involved providing users wireless access to fixed networks for email, Internet access, and other network services, for distances of tens of meters. On the other hand, WPAN applications were originally conceived as low power, short-range (under 10 meters) wireless communications among ad hoc groups of devices to eliminate cables. The concept of a "personal area network" is articulated as follows in the IEEE 802.15.1 (Bluetooth) WPAN standard [12]:

> Interconnecting personal devices is different from connecting computing devices. Typical connectivity solutions for computing devices (e.g., a WLAN connectivity solution for a notebook computer) associate the user of the device with data services available on, for instance, a corporate Ethernet-based intranet. This situation contrasts with the intimate, personal nature of a wireless connectivity solution for the personal devices associated with a particular user. The user is concerned with electronic devices in his or her possession, or in his or her vicinity, rather than to any particular geographic or network location. The term *personal area network* (PAN) was coined to describe this different kind of network connection. The untethered version of this concept is a WPAN. A WPAN can be viewed as a personal communications bubble around a person. Within this bubble, which moves as a person moves around, personal devices can connect with one another. These devices may be under the control of a single individual or several people's devices may interact with each other.

WPANs are further distinguished from WLANs in terms of operations [12]:

- WPANs are engineered to save power in order to guarantee device mobility, thereby involving shorter radio ranges compared to WLANs, which are generally engineered for coverage in order to guarantee access to a fixed network.
- In IEEE 802.15.1 WPANs, contention-free access[6] is maintained at all times by imposing master-slave relationships between the devices and operating on a single, time multi-

[6] In each type of wireless networking system, "medium access" (use of the frequency channel) is controlled in a particular way. If everyone's transmissions are timed so that no two devices transmit at the same time, the access method is described as "contention-free." Otherwise, the system uses "contention access" and is designed to handle occasional "collisions" that happen when two or more devices transmit at the same time.

plexed, slotted system with minimal interference from adjacent WPAN networks, unlike WLANs, which even in a contention-free period are subject to interference from adjacent access points.

- The IEEE 802.15.1 WPAN "master" device polls its collection of "slaves" (*i.e.*, they transmit when told to do so by the master). In this manner, the master regulates the bandwidth assigned to the different slave devices based on quality-of-service requirements that it enforces. WLANs typically are meant to give equal access to all users.
- WLANs do not have an inherent or implied lifespan; they exist independent of their constituent devices. However, in a WPAN, if the master does not participate, the network no longer exists; in a WPAN, a device creates a connection that lasts only for as long as needed and has a finite lifespan.

2.1.2 IEEE 802.15 Series of WPAN Standards

The technical activities of the IEEE 802.15 WPAN Working Group (WG) are conducted by Task Groups (TGs) or Study Groups, which remain active while a new standard is being developed by them. To date the 802.15 WG has had eleven TGs:

- 802.15.1 (inactive) Formalized the commercial Bluetooth WPAN specification as an IEEE standard.
- 802.15.1a (inactive) Updated the 802.15.1 standard.
- 802.15.2 (inactive) Generated policies for improving the coexistence of 802.15.1 devices and WLAN devices.
- 802.15.3 (inactive) Generated a standard for high-speed WPANs (known commercially as Wi-Media).
- 802.15.3a In the process of choosing an alternative high-speed WPAN signaling method.
- 802.15.3b In the process of improving the 802.15.3 standard.
- 802.15.3c In the process of choosing a high-speed WPAN implementation at millimeter wave frequencies.
- 802.15.4 (inactive) Generated a standard for low-speed WPANs (known commercially as Zigbee).
- 802.15.4a In the process of choosing an alternative low-speed WPAN signaling method that will enable geolocation.
- 802.15.4b In the process of improving the 802.15.4 standard.
- 802.15.5 In the process of developing mesh networking protocols for WPANs.

Of these WPAN standards, in what follows we describe in some detail the operations of 802.15.1 (Bluetooth), 802.15.3 (Wi-Media), and 802.15.4 (Zigbee).

2.2 802.15.1 (Bluetooth) Description

The original WPAN system is Bluetooth[7], which is specified by IEEE standard 802.15.1. The standard was developed primarily for commercial products featuring data and voice transfer between communication and/or computing devices utilizing frequency-hopping radio transmissions in the unlicensed 2.4 GHz band, and supporting wireless device connections up to 10m (up to 100m if the transmitter's power is increased). For data traffic, a unidirectional (i.e., asymmetric) maximum of 723.2 kb/s is possible between two devices. A bidirectional 64 kb/s channel supports voice traffic between two devices. This capability combined with ad hoc device connection and automatic service discovery make it an attractive solution for mobile devices such as a hands-free headsets in addition to cable replacement applications.

2.2.1 Bluetooth Network Topology

Bluetooth devices are generally organized into "piconets," each of which consists of a single "master" device and up to eight active "slave" devices. A device may belong to more than one piconet, either as a slave in both or as a master of one piconet and a slave in another. Interconnected piconets are known as "scatternets." Figure 2.2.1 illustrates the concepts of piconet and scatternet. Piconets may be static or may be formed dynamically as devices move in and out of range of each other. A device leaves standby (the low power, default state) by initiating or receiving an inquiry or a paging command. An inquiry may be used if the address of a targeted device is unknown; it must be followed by a page command. A page command containing a specific Device Access Code is used to connect to a remote device. Once the remote device responds, both devices enter the connected state, with the initiating device becoming the master and the responding device acting as a slave. Once in the connected state,

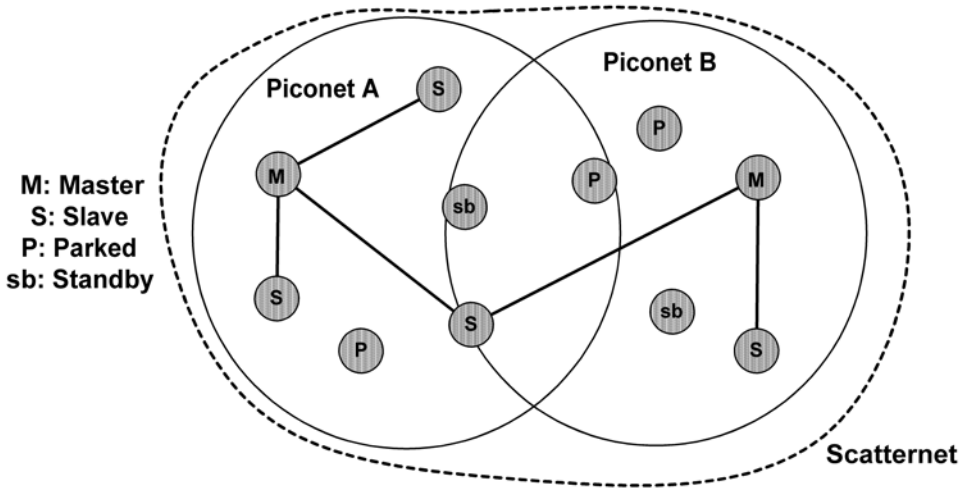


Figure 2.2.1 Bluetooth basic network topology (based on [13]).

[7] The name "Bluetooth" was inspired by the Danish King Harald Bluetooth, known for unifying Denmark and Norway in the 10th century [14].

the slave device will synchronize to the master's clock and to the correct frequency-hopping pattern. The master makes regular transmissions in order to keep the piconet synchronized. Slaves listen on every master-transmit time slot in order to maintain synchronization with the master and to receive data addressed to them.

Each piconet is distinguished by its being synchronized to a specific frequency-hopping pattern at a hop rate of 1,600 hops per second using the 79 frequencies spaced 1 MHz apart from 2.402 GHz to 2.480 GHz; the modulation on each hop is Gaussian (shaped) minimum frequency-shift keying (GMSK) at the pulse rate of 1 MHz. Each hop is a time slot during which data packets are transferred, alternately the master and the slave, as illustrated in Figure 2.2.2.

2.2.2 Service Discovery Protocol and Profiles

According to [15], the Bluetooth service discovery protocol (SDP) determines what services are available on a particular device. A Bluetooth device may act as an SDP client that submits queries for services, an SDP server providing services, or both. SDP provides access only to information about services; utilization of those services must be provided via another Bluetooth or third-party protocol. In SDP, a service may provide information, perform an action, or control a resource. SDP servers maintain service records to catalog all available services provided by the device.

The purpose of SDP is to discover, not access, services. Two processes are supported: searching and browsing. Searching is useful if the client is looking for specific capabilities, but for a client to identify all services offered by a remote device, the SDP "browsing" mechanism must be used. Browsing is accomplished via the search capability by using a special service attribute supported by all service classes.

Profiles, defined by the Bluetooth Special Interest Group (SIG), are intended to ensure interoperability between Bluetooth applications and devices from different manufacturers. These profiles define the roles and capabilities for specific types of applications. Different profiles may encompass different layers and protocols and to different degrees. In addition to requirements for interoperability, protocols may define required services to other applications or to end users. All Bluetooth devices must support the Generic Access Profile at a minimum. This profile defines device discovery, connection procedures, and procedures for various security levels.

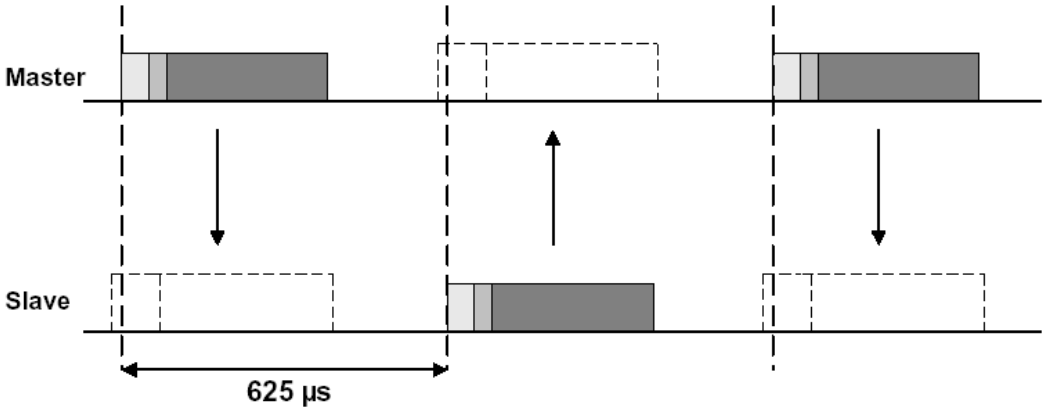


Figure 2.2.2 Alternating master-slave packet transmissions (from [12]).

Some Bluetooth-specific user interface requirements are described as well. Another universal profile, although not required, is the Service Discovery Access Profile, which defines how a service discovery application on a device determines the services on other remote devices as well as the protocols, and associated parameters required to access them.

2.3 802.15.3 Description

There is an increasing demand for transmission of video and other multimedia applications over WLANs and WPANs. In the IEEE 802.15 WG, this demand led to the development of a standard for high-speed WPANs. The original 802.15.3 WPAN, known commercially as Wi-Media, is just now emerging in the physical products. Alternative hi-speed WPAN standards are the goal of the 802.15.3a and 802.15.3c TGs.

2.3.1 Original IEEE 802.15.3 High-Rate WPAN (Wi-Media)

The original concept of Bluetooth, the first WPAN standard, involved cable replacement, and the Bluetooth standard provides for wireless connections at data rates up to 723 Kbps. So also does the IEEE 802.15.3 WPAN standard [16], which was designed to meet the demanding requirements of portable consumer imaging and multimedia cable replacement applications, some of which are suggested in Figure 2.3.1. In addition to higher data rates, the new WPAN protocols offer enhanced operations. Features of the 802.15.3 system include

- Data Rates: 11, 22, 33, 44, & 55 Mbps
- Quality of Service isochronous protocol
- Ad hoc peer-to-peer networking
- Security
- Low power consumption
- Low cost

A total of five channels in two sets are assigned for operation. The first set is the high-density mode, which allocates four channels, while the second is an 802.11b co-existence mode that allocates three channels.

The base transmission rate in symbols/sec (sps) is 11 Msps, making the transmission bandwidth about 11 MHz. The higher bit rates are obtained respectively by transmitting modulation symbols with 1, 2, 3, 4, or 5 bits per symbol. The 802.11b coexistence mode consists of one or more of the following techniques [17]:

- Passive scanning: An 802.15.3 “device” (DEV) that is about to initiate the formation of a piconet scans the channels in the 2.4 GHz band and chooses the one that is least busy in terms of being used by other systems or piconets.
- Dynamic channel selection: The PNC periodically requests statistics from the DEVs in the piconet on the quality of communications at their locations; if necessary, the PNC can move the piconet’s operations to another channel that has better quality or to avoid interfering with another system, such as 802.11b.

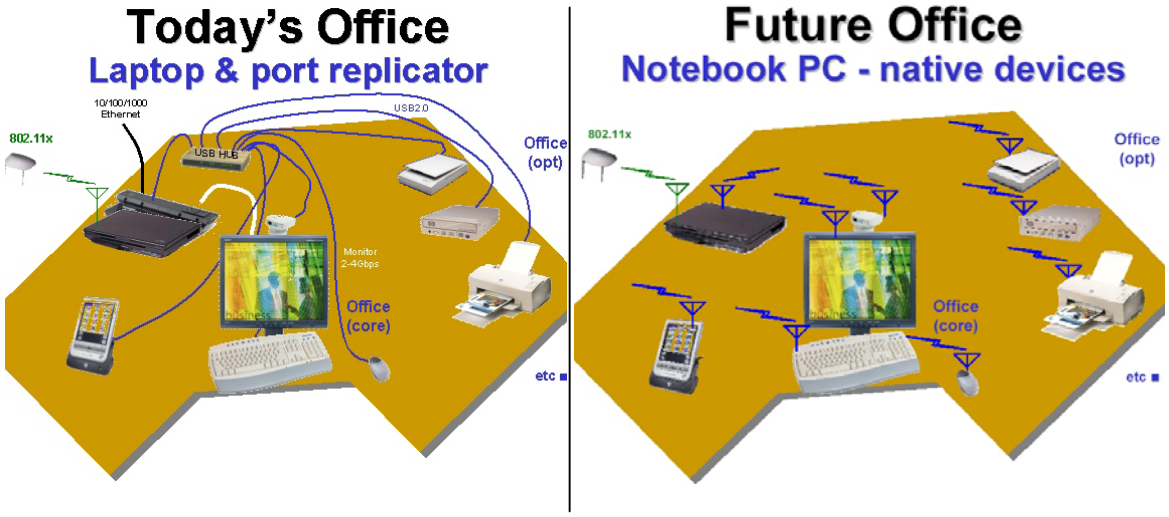


Figure 2.3.1 Multimedia cable replacement with high-rate wireless networking (from [18]).

- Link quality and RSSI measurement: The 802.15.3 physical layer (PHY) reports values of the received signal strength indicator (RSSI) and, at the higher rates, link quality information (LQI) in terms of packet loss statistics; the RSSI measurement can be used for power control and the combination of RSSI and LQI can detect the presence of interference in the channel.
- Nonoverlapping channel plan: If the PNC detects the presence of an 802.11b system in its operational area, it can choose the "coexistence" channel allocation plan in order not to transmit on frequencies that would involve contributing interference to two 802.11b channels at the same time.

802.15.3 piconets are formed from two elements: a piconet coordinator (PNC) and one or more other "devices" (DEVs), as illustrated in Figure 2.3.2. The physical extent of the piconet is determined by the radio range of the PNC, which broadcasts a beacon packet periodically that contains timing and other information needed by DEVs to participate in the piconet. Not every manufactured DEV will be capable of being a PNC, for example a DEV intended to receive audio signals at a speaker, but the PNC can participate as a communicator in the piconet like another DEV. Besides supplying a time reference for the piconet, the PNC controls admission to the piconet and authenticates entrants if a security policy is in force. The PNC can also take into account DEVs that "sleep" for certain periods (to save power) by assigning channel time to them when they are scheduled to be "awake."

The basic timing of a piconet is marked by superframes that have the structure represented in Figure 2.3.3. Following the beacon frame transmitted by the PNC, which contains timing information and network management parameters, there is a contention access period (CAP) in which DEVs can signal the PNC that they want to join the piconet, or in which short commands and messages can be sent without waiting for a scheduled transmission to be assigned by the PNC in one of the channel time allocations (CTAs) in a subsequent superframe. The protocol during the CAP is carrier-sense multiple access with collision avoidance (CSMA/CA),

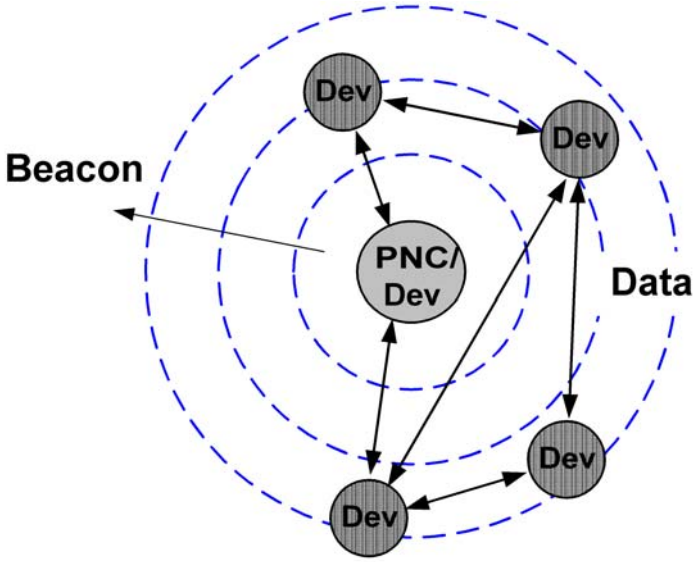


Figure 2.3.2 Elements of an IEEE 802.15.3 piconet (based on [17]).

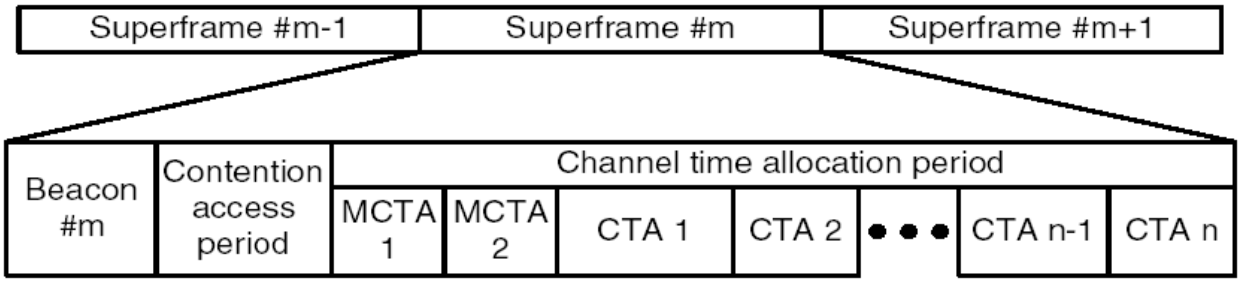


Figure 2.3.3 802.15.3 superframe structure (from [16]).

similar to what is used in 802.11 in the ad hoc mode. The MCTA frames indicated in Figure 2.3.3 are management CTAs that are used when the PNC has data to send to the piconet.[8]

Each DEV calculates the amount of channel time it needs for its application, and the PNC sorts out the different DEV requirements, usually scheduling periodic allocations of time to DEVs that, on average, provide them with the desired rates. The DEVs can adjust their modulation bit rates to match the rates needed by their applications and/or the channel conditions.

Using the superframe structure, it is possible to allocate channel time to a DEV that is acting as the PNC of a "dependent piconet," as illustrated in Figure 2.3.4. When a dependent piconet is setup, the "dependent PNC" broadcasts its own beacon during the channel time allocated to it, at a different time than that the beacon of the PNC. In this way, the operation of the piconet can be enhanced in one of the following ways:

[8] An optional use for the MCTA is to schedule a time for contention access using the slotted ALOHA protocol, which is suitable for DEVs that cannot perform carrier sensing (see the packet switching tutorial in Appendix 5.1).

- Implementing a multi-hop ad hoc network, in effect extending the physical range of the network
- Setting up a subnetwork for security purposes
- Allowing two separate piconets to share the same frequency channel when resources are scarce
- Allowing the formation of a subnetwork that has its own special timing requirements, such as a set of speakers and an amplifier.

2.3.2 Alternate PHYs for 802.15.3

Although the maximum data rate for 802.15.3 of 55 Mbps is quite high for many applications, the desire for even higher rates has led to an effort to define an alternative physical layer (PHY) for the system, to be designated 802.15.3a. There has been much interest in the industry in this project because of the possibility of using so-called "ultrawideband" (UWB) transmissions for this purpose.

In 2001, the FCC issued an amendment to its rules for transmission by unlicensed RF devices to add a section regarding UWB transmissions. The emission restrictions established by these rules are primarily those recommended by National Telecommunications and Information Administration (NTIA) analyses for protection of GPS and other government systems operating in the 960–1610 MHz band. As shown in Figure 2.3.5, this band is basically excluded for UWB devices, while emissions in the allowable bands have the limit of –41.3 dBm/MHz, equivalent to that for non-UWB systems. The emissions mask also reflects the desire to protect various other

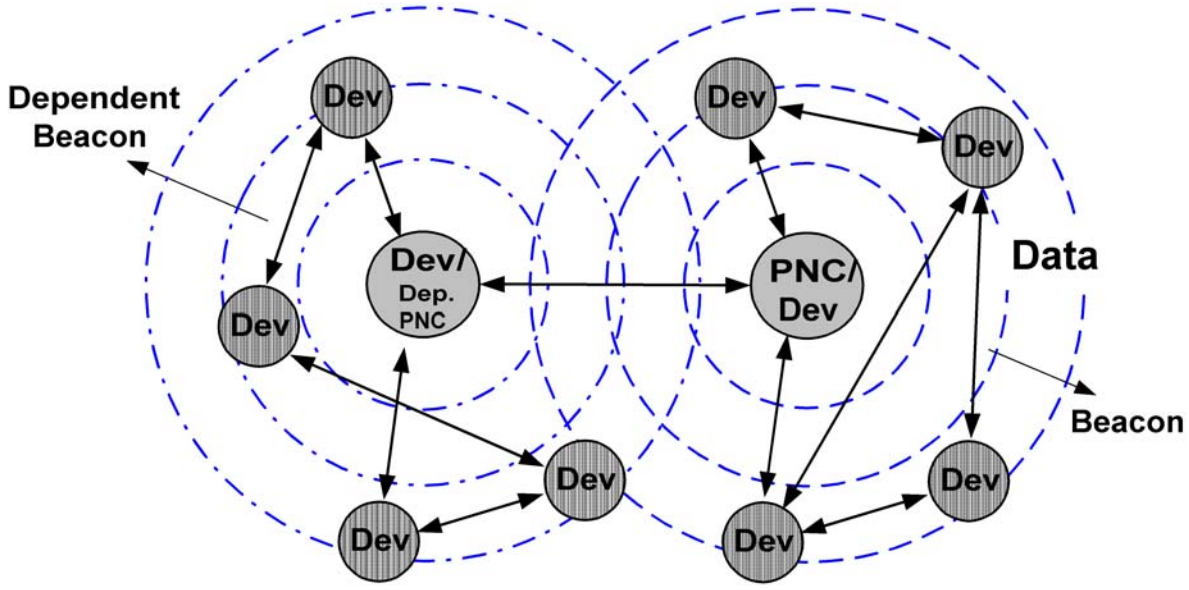


Figure 2.3.4 Example of a dependent piconet.

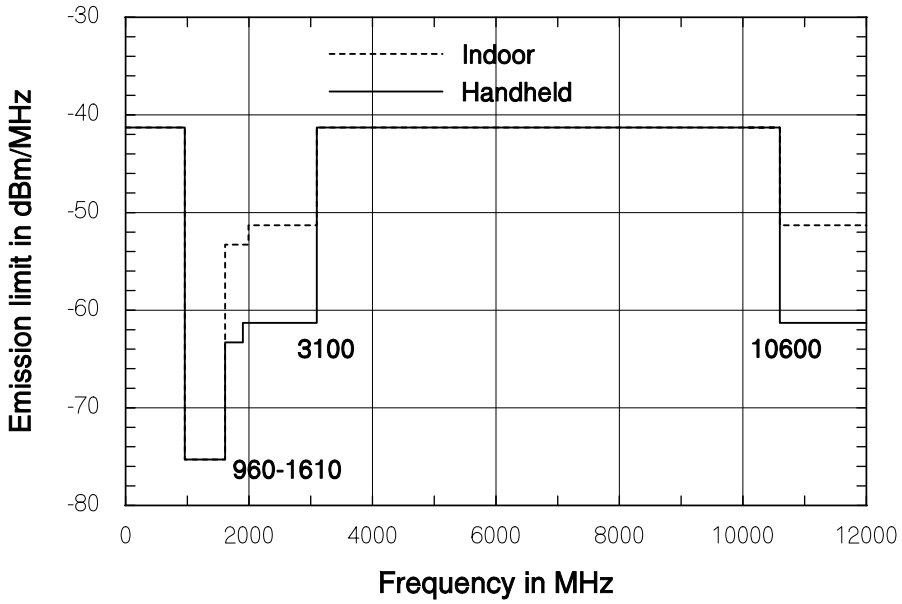


Figure 2.3.5 FCC emissions mask for average radiation by UWB devices (from [19]).

government systems in the 1610–3100 MHz band and satellite systems above 10600 MHz. Additional stipulations in this ruling include [19]

- Restriction of handheld (portable) UWB devices to the 3100–10600 MHz band, as determined by their 10-dB bandwidths.
- In addition to the limits on average power levels shown in Figure 2.3.5, there are limits on the peak levels of emissions above 1 GHz and on quasi-peak levels below 1GHz.

The availability of almost 7 GHz of unlicensed spectrum opens the possibility of extremely wide bandwidth systems, provided that they can qualify as UWB systems under FCC rules that are intended to protect the many pre-existing radio systems that are already using frequencies in that wide section of bandwidth.

One of the final two proposals for the alternate PHY featured binary and quaternary pulse modulations at very high rates and using spread-spectrum techniques to effect piconet separation by means of code-division multiple access (CDMA) [20]. This system was designed to achieve data rates up to 114 Mbps at 10 meters and up to 600 Mbps at 6 meters.

The other of the final two proposals featured orthogonal frequency-division multiplexing (OFDM) signaling over multiple bands to effect piconet separation by means of hopping patterns [21]. This system was designed to achieve data rates up to 480 Mbps.

To date, neither 802.15.3a proposal has been able to win the approval of 75% of the Working Group. Industrial associations have been formed to complete the specifications of the favored approaches and to market products based on them.

Meanwhile, TG 802.15.3c was established to explore the WPAN technologies that can be developed at millimeter wave frequencies (above 100 MHz). The work of this new TG is in its preliminary stage.

2.4 802.15.4 Description

At the same time that efforts were being made to increase the bandwidth available for transmission over WPANs, there was an interest in efficient short-range WPAN operations involving applications that do not involve significant mobility and do not require high data rates. These applications include wireless networks of sensors and other instrumentation devices, as illustrated conceptually in Figure 2.4.1. The new IEEE 802.15.4 standard is supported commercially under the trade name Zigbee.

2.4.1 IEEE 802.15.4 Applications

The "application space" for the IEEE 802.15.4/Zigbee system has been envisioned as including cable replacement and "last meter" connectivity and control networking for [22, 23]

- *Home automation and networking:* communication/control for consumer electronics, personal computer peripherals, interactive games, home security, lighting, appliances, and air conditioning.
- *Automotive sensing:* cable replacement for telematics applications, such as tire pressure monitoring.
- *Industrial networks:* wireless access for sensors to a wired industrial control network; wireless monitoring and control of industrial sensors and sensor networks.
- *Interactive toys:* cable replacement for peripherals, possible integration of games into personal computer instead of separate "box."

Figure 2.4.1 Example variety of objects networked using IEEE802.15.4 (from [22]).

- *Remote metering:* wireless stick-on sensors for monitoring, remote diagnostics, and/or control; wireless access for low-power, inexpensive sensors to a wired network.[9]The Zigbee approach is competing with other wireless technologies such as WLANs and RFID on the basis of the dedication of its design to low cost, flexible networking (reducing installation and maintenance costs), and adaptability to devices with varying capabilities. Types of traffic for which the system is well suited include periodic data at an application-defined rate (e.g. sensors), intermittent data at an application/external stimulus defined rate (e.g. light switch), and repetitive low-latency data requiring fixed allocation of time slots (e.g. mouse). To satisfy these different types of traffic, the access protocol accommodates two device classes:

- Full function devices (FFDs) that can operate under any topology, act as network coordinators, and communicate with any other device.
- Reduced function devices (RFDs) with very simple implementations that operate under a centralized (star) topology, cannot act as network coordinators, and can communicate only with a network coordinator

2.4.2 IEEE 802.15.4 Technical Features

IEEE 802.15.4 device specifications include operation in one or more of the following frequency bands, as illustrated in Figure 2.4.2: 16 channels in the 2.4GHz ISM band, 10 channels in the 915MHz band, and one channel in the 868MHz band.

The physical layer for the 2.4 GHz band utilizes offset QPSK modulation with a chip rate of 2.0 Mcps[10], transmitted using shaped symbols so that the signal occupies about 1 MHz. The spread-spectrum signaling scheme delivers a data rate of 250 kbps, to be divided among the network participants and the signaling overhead. A spread-spectrum gain of 32 (15 dB) or more can be realized with the appropriate receiver processing.

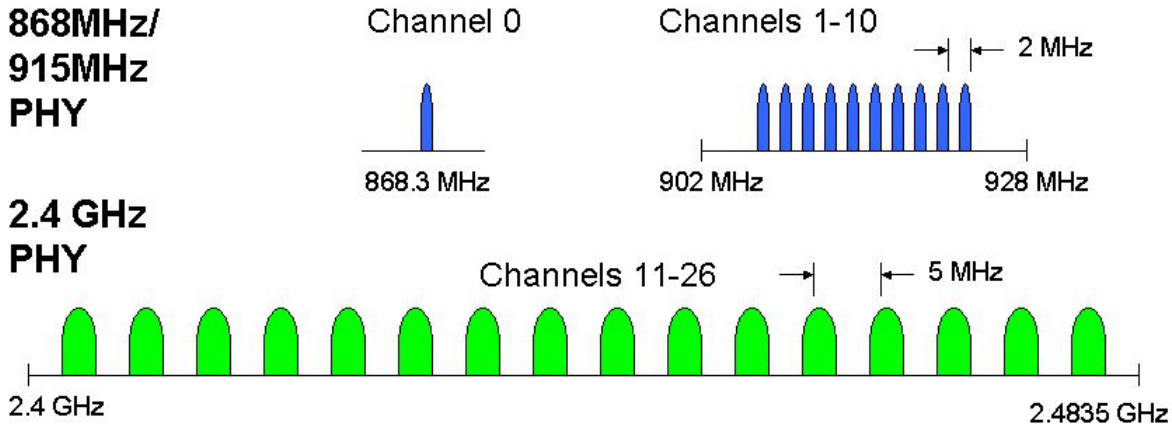


Figure 2.4.2 Channels available to 802.15.4 low-rate WPAN (from [22]).

[9] In this application, a IEEE 802.15.4 system can function much like an RFID system for a limited number of objects.

[10] A "chip" is the shortest pulse sent by the radio. Codes using groups of chips to form "symbols" are used to convey information (bits).

The physical layer for the 868 MHz and 915 MHz bands utilizes a binary modulation with a chip rate of 300 kcps or 600 kcps, respectively. The data rate achieved by the signaling scheme in the 868 MHz band is 20 kbps and that in the 915 MHz band is 40 kbps, to be divided among the network participants and the signaling overhead. A spread-spectrum gain of 15 (12 dB) or more can be realized with the appropriate receiver processing. As mentioned, these data rates are the "raw" data rates for transmission of all data. The available bandwidth is divided among the network participants by imposing the timeslot-frame structure illustrated in Figure 2.4.3, in which it is shown that the frame is defined by the rate at which the device acting as network coordinator sends beacons: every 15 ms or some power of two (up to 14) times 15 ms, so a frame can last from 15 ms to 246 sec. Variable portions of the frame (determined by the coordinator) are reserved for a beacon extension period to convey overhead or control messages, a contention access period for intermittent data or network entry attempts, and one or more guaranteed timeslots (GTSs) in the case that the frame lasts 15 ms. The GTSs permit assignment of regular burst transmissions of data by designated terminals at an average bit rate that is some fraction of the maximum bit rate.

The frame structure of Figure 2.4.3 suggests a star network topology in which a central node (the coordinator) communicates with, or controls the communications of, other nodes within its range. However, similar to the IEEE 802.15.3 WPAN multihop operational capability described in Section 2.3.1, the specification for IEEE 802.15.4 devices provides for setting up both star and peer-to-peer ("mesh") network topologies, as illustrated in Figure 2.4.4. The methods to form multihop cluster network topologies are not specified in IEEE 802.15.4, but the standard has been designed to allow for them.

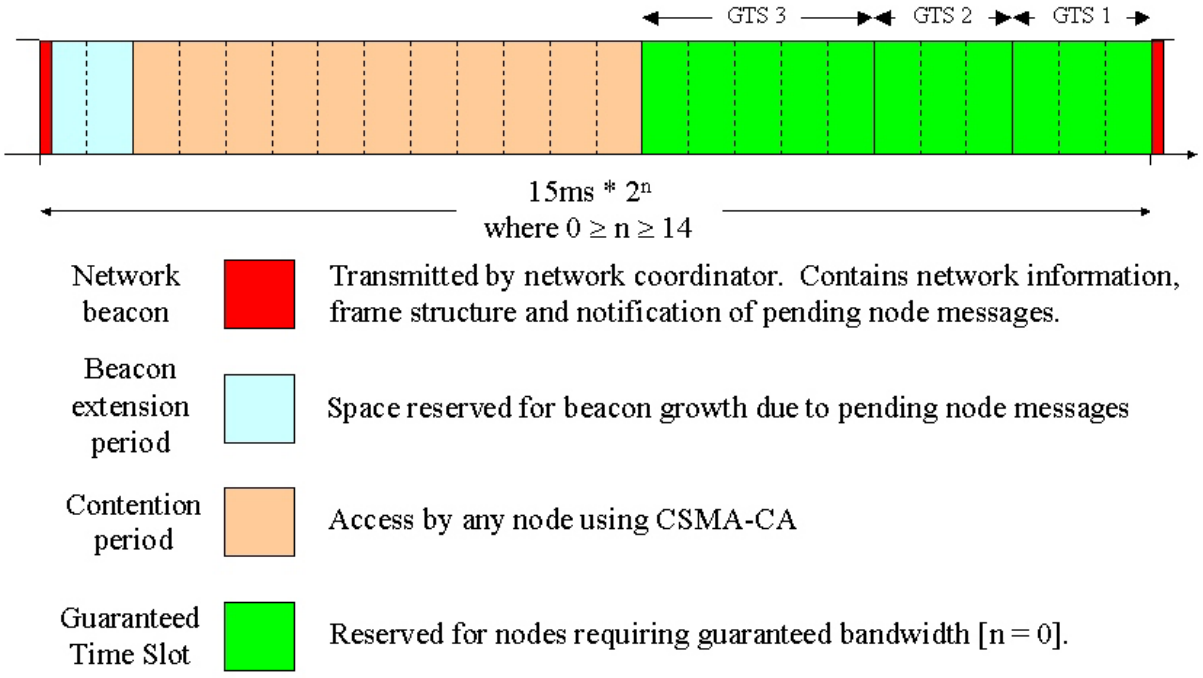


Figure 2.4.3 Optional IEEE 802.15.4 frame structure (from [22]).

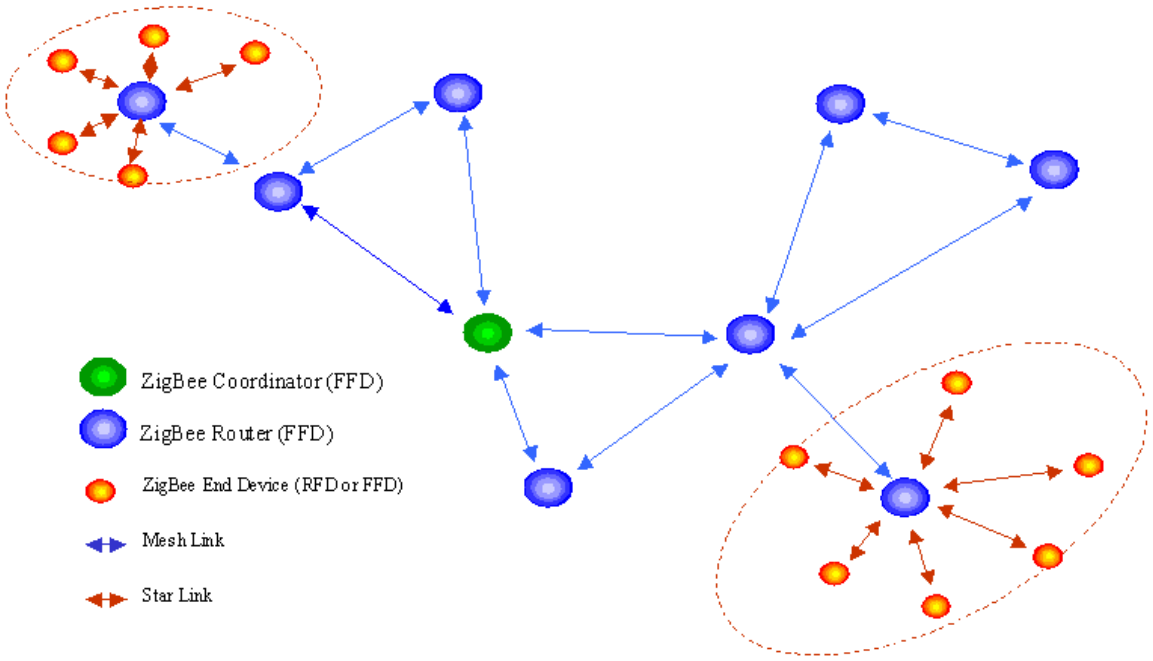


Figure 2.4.4 Types of Zigbee links based on nodes with different capabilities (from [24]).

3. Incident Area Network Technologies

Incident area networks (IANs) by definition must be capable of adapting to the physical circumstances of the incident. Connectivity must be provided among public safety communication devices (PCSDs) that enter and leave the incident area. Access to the jurisdiction area network (JAN) must be set up and maintained, or if the fixed JAN infrastructure has been taken out, the IAN must be able to set up a connection (bridge) to another network.

While wireless local area networks (WLANs) based on the IEEE 802.11 set of standards are well known as means for providing wireless access to a fixed network through an access point (usually indoors), the huge popularity of 802.11 devices has led to higher performing and more versatile networking possibilities using 802.11 equipment, indoors and outdoors. For example, creative law enforcement people have set up access points (APs) at department gasoline stations and have used pairs of 802.11 devices to provide a relatively high-speed link between buildings. In this section, we describe the many different versions of 802.11 that are available today or are in the process of being approved.

In this section, we give an overview of the existing 802.11 family of standards that have potential application to public safety communications use, explain the basics of WLAN networking, and introduce the concepts of ad hoc networking that make a network of 802.11 devices useful for IAN applications. The concepts involved in "mesh" networking, which has attracted a lot of interest recently for providing broadband services to a public services area, are discussed in Section 4.

3.1 The IEEE 802.11 Wireless Standards

From its beginning to now, the IEEE 802.11 Working Group has sponsored many different task groups (TGs) for specific projects. From an original objective of providing wireless access to local area networks (LANs) in much the same way as wired LANs, this wireless technology has evolved to include advanced functionalities such as ad hoc networking. The IEEE 802.11 TGs can be listed as follows:

- 802.11 Original task groups developed standards for medium access and three different physical layers: infrared, 2.4 GHz frequency hopping, and 2.4 GHz spread-spectrum.
- 802.11a Developed a version of the standard to operate in the 5.8 GHz band.
- 802.11b Developed a higher-speed version of the standard for the 2.4 GHz band (known commercially as Wi-Fi), with rates of 1, 2, 5.5, and 11 Mbps.
- 802.11c Developed protocols for bridge operations with the 802.11 medium access control (MAC) procedures.
- 802.11d Developed modifications for 802.11 WLANs to operate in more countries.
- 802.11e Developed enhancements of the MAC procedures to improve quality of service and security.
- 802.11f Developed details of networking access points in a distribution system.
- 802.11g Developed higher speed extension to 802.11b, to at least 20 Mbps.

- 802.11h Developed refinements to the MAC and to the 5 GHz physical layer (PHY) to work better in European regulatory environments.
- 802.11i Developed improvements to the MAC to enhance security.
- 802.11j Developed version of 802.11 for 4.9 GHz and 5 GHz in Japan.
- 802.11k In the process of developing radio resource measurement techniques to enable coexistence and other operations.
- 802.11m In the process of making technical and editorial corrections to the 802.11 standards.
- 802.11n In the process of defining a high throughput (greater than 100 Mbps) version of 802.11.
- 802.11p In the process of amending the 802.11 standards to make a version suitable for communication between vehicles in the 5.9 GHz band.
- 802.11r In the process of developing enhancements to 802.11 systems to reduce delays so that VoIP will work better.
- 802.11s In the process of developing protocols for an all-802.11 mesh network.
- 802.11T In the process of developing performance measuring and prediction methods for 802.11 WLANs.
- 802.11u In the process of amending 802.11 protocols to enable Interworking with other networks.
- 802.11v In the process of amending 802.11 protocols to enable distributed management of networks of APs.

3.2 Basics of WLAN Networking

The strengths and weaknesses of WLANs for various applications can be understood better in view of the basic operations of the protocols governing WLAN transmissions, according to the IEEE 802.11 standards.

3.2.1 WLAN Networking Modes

Under the IEEE 802.11 specification [25], a WLAN can operate in one of two optional modes, as illustrated in Figure 3.2.1:

- an *infrastructure* mode in which one or more "basic service sets" provide wireless user stations (STAs) with access to the wired network infrastructure through "access points" (APs), or
- an *ad hoc* mode in which terminals in an "independent basic service set" can communicate directly with each other.

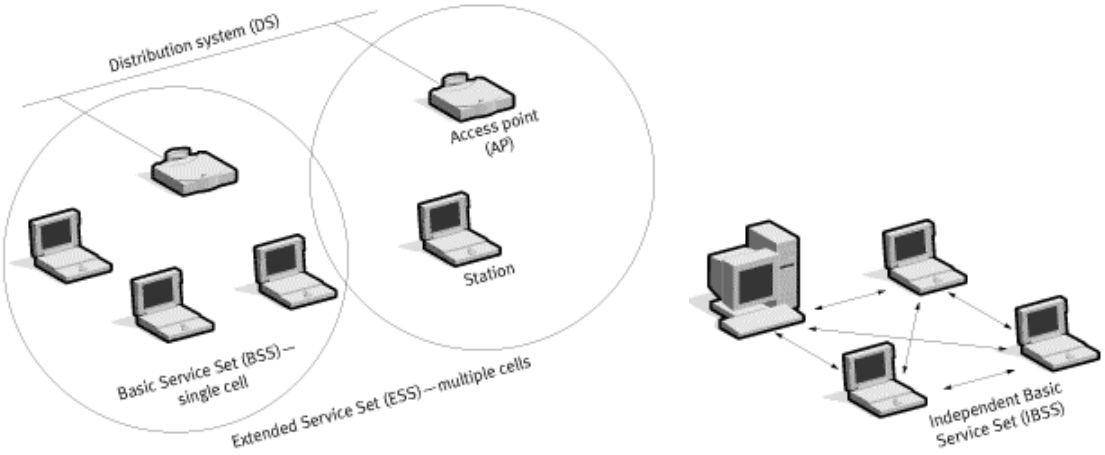


Figure 3.2.1 Infrastructure and ad hoc modes of WLAN operation (from [26]).

In the infrastructure mode, the transmissions by the mobile stations in the service area of a particular access point can be scheduled by the access point to minimize contention in the form of "collisions" between these transmissions that would cause loss of data and/or delays due to the need for repetition. Multiple access points can be located so as to cover a larger area, just as in a cellular telephone network, with means for "roaming" and "handoff" between APs. The network and individual APs are identified by codes that have been programmed into the system.

In the ad hoc mode, each mobile station transmits when it has data to send, provided that it does not sense that another stations is already transmitting (see Section 3.2.3 below for more discussion of this access mode). Operation as a WLAN therefore is possible without an access point or connection to a wired network, but the likelihood of data collisions is higher than for the infrastructure mode.

3.2.2 Data Handling for Wireless Transmission

In order to accomplish WLAN operation, it is necessary to organize the user data into frames or packets. If the user data (file, message, etc.) involves a large number of bits, the 802.11 Medium Access Control (MAC) layer will chop it into segments of the proper size for compatibility with the transmission protocols. Each original data packet, in the form of a MAC protocol data unit (MPDU) accrues additional overhead signaling bits before transmission by the unit's radio.

- First, the MPDU is "encapsulated" by adding header and tail bits. The header contains highly compacted information on the sequencing of the data and the details of the transmission, and the tail is reserved for information related to the error-correction and encryption encoding that is necessary because of the noise present on the wireless channel and the possibility of signal fading during transmission.
- Next, more bits (training symbols) are added to the beginning of the coded data packet to facilitate acquisition at the receiver, and bits may be added to the end of the packet to make it a convenient length.

- Finally, the transmitter takes the data and prepares it for radio transmission by converting combinations of bits into a sequence of modulation symbols. The beginning of the transmission is a "preamble" that gives the receiver the opportunity to acquire (latch onto) the signal and get synchronized with its timing so that it can properly separate and process each modulation symbol that is arriving.

3.2.3 Channel Access Techniques

As mentioned previously, in the infrastructure mode, the AP can be set up to regulate the transmissions of STAs in order to minimize collisions. The AP maintains a schedule of alternating contention-free and contention-access periods. During contention-free periods, the AP schedules the transmissions of STAs that have indicated in a previous contention-access period that they have data to send.

In the ad hoc mode and during contention-access periods of the infrastructure mode, STAs having data to send monitor the channel for other STAs' transmissions. As illustrated in Figure 3.2.2[11], after the end of one STA's transmission as indicated by an acknowledgement message (ACK), all STAs wait for a certain interval, after which a contention time-window becomes active. During the contention window, any STA having data to send may transmit after an additional random "backoff" delay if it does not sense that another STA has started its transmission. The use of a random backoff delay reduces the possibility that two STAs will start to transmit at the same time. This form of channel access is known as CSMA (carrier sense multiple access).[12]

Further techniques are used in 802.11 to render it a CSMA/CA (collision avoidance) system. First, information on the duration of a STA's transmission is embedded in its packet header, so that each listening STA can set a timer to count down to the next time that channel is expected to be idle. The successful operation of this technique depends on potential transmitting STAs' being able to "hear" the timing information and thereby to defer their own transmissions. It is possible that some STAs will not defer because they are too far away from the currently transmitting STA to sense its transmission; if they are, and if they also are in range of the STA

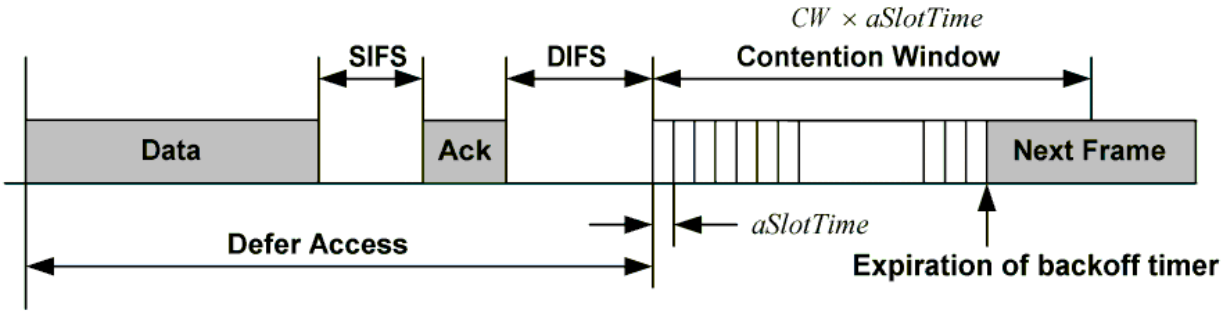


Figure 3.2.2 Contention Access in IEEE 802.11

[11] In Figures 3.2.2 and 3.2.4, IFS = interframe space, DIFS = distributed coordination function IFS, SIFS = short IFS, RTS = request to send, and CTS = clear to send.

[12] A tutorial on packet switching techniques is provided in Appendix 5.1.

that is the intended receiver of the packet, they are known as "hidden terminals." Figure 3.2.3 illustrates the hidden terminal problem as well as the related "exposed terminal" problem, in which a STA defers its transmission unnecessarily. The 802.11 MAC protocol attempts to alleviate the hidden terminal problem by providing for optional RTS (request to send) and CTS (clear to send) messages preceding the data transmission.

Figure 3.2.4 illustrates how the RTS/CTS mechanism works. Instead of transmitting its data packet, a STA transmits a small RTS packet, which is in carrier-sensing range of all the STAs that would normally sense its data packet. The intended receiving STA answers with a small CTS message, which can be sensed by STAs that would be hidden terminals for this particular transmission. It is still possible for the RTS packet to collide with a hidden terminal's transmission, but the effect on the WLAN's throughput is reduced because the RTS packet is small compared to the data packet.

3.2.4 Bridging and Wireless Distribution System

The conventional use of an infrastructure WLAN is to provide wireless access to a wired network and the Internet; wireless terminals communicating with each other may do so through the wired "backbone" or distribution system (DS) that connects the APs. However, it is possible to form a multi-AP system that is completely wireless—does not connect with a wired network—in which wireless terminals communicate with each other via APs that are wirelessly

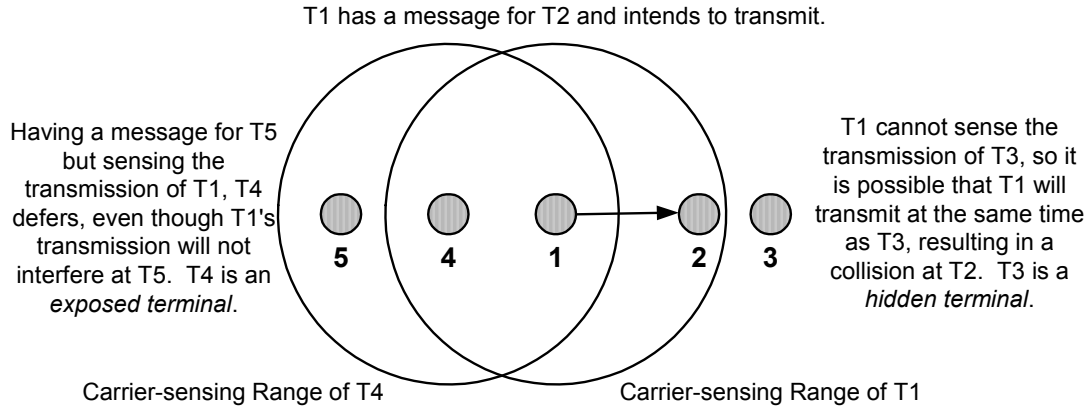


Figure 3.2.3 Hidden terminals and exposed terminals.

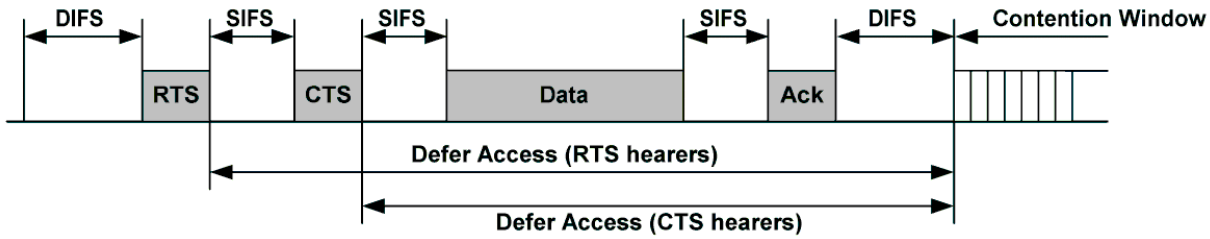


Figure 3.2.4 Carrier-sense Multiple Access (CSMA) with Collision Avoidance (CA)

connected. In effect, using this Wireless Distribution System (WDS) feature of the IEEE 802.11 standard (the 2003 edition of the 1999 standard), multihop networks and relays (wireless bridges) can be configured using 802.11b or later APs. An example is shown in Figure 3.2.5, in which an AP in one building communicates with a relay AP in another building in order to access the Internet through a third AP.

WDS applications are made possible by two provisions in the 802.11 standard: designation of packets as being both from and to the DS, and the specification of intermediate packet destination addresses [27]. The exploitation of these provisions to create bridges and other WDS applications requires proprietary processing at the upper layers of the protocol stack to develop information on the network configuration into WDS routes. The wireless traffic between the APs uses the same channel as that for communication between WLAN terminals and the APs, so that WDS decreases the fraction of network capacity available to the latter.

3.3 Ad Hoc Networking

A wireless ad hoc network is a collection of autonomous nodes or terminals that communicate with each other by forming a multihop radio network and maintaining connectivity in a decentralized manner. Since the nodes communicate over wireless links, they have to contend with the effects of radio communication, such as noise, fading, and interference. In addition, the links typically have less bandwidth than in a wired network [28, 29]. If packet switching is used for controlling radio transmissions, there is an additional loss of capacity (and potential delays) because of the overhead involved in this mode of operation, as discussed in the previous subsection.

In many respects, mobile ad hoc networks (MANETs) are the successors to packet radio networks, with the additional requirement of high mobility and with the additional assumption of a much higher computing capability for each terminal due to advances in electronic circuitry. The open literature on MANETs typically assumes a very challenging scenario such as the one depicted in Figure 3.3.1, in which an ever-increasing demand for bandwidth is present as radio

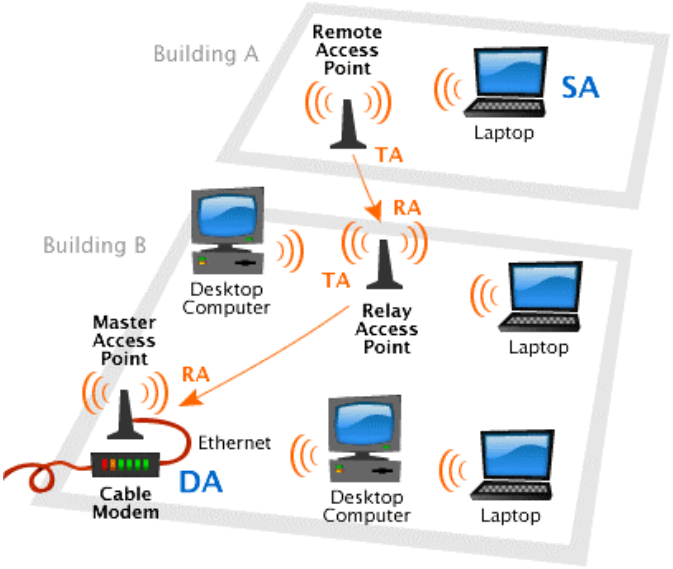


Figure 3.2.5 Multihop WDS (from [27]).

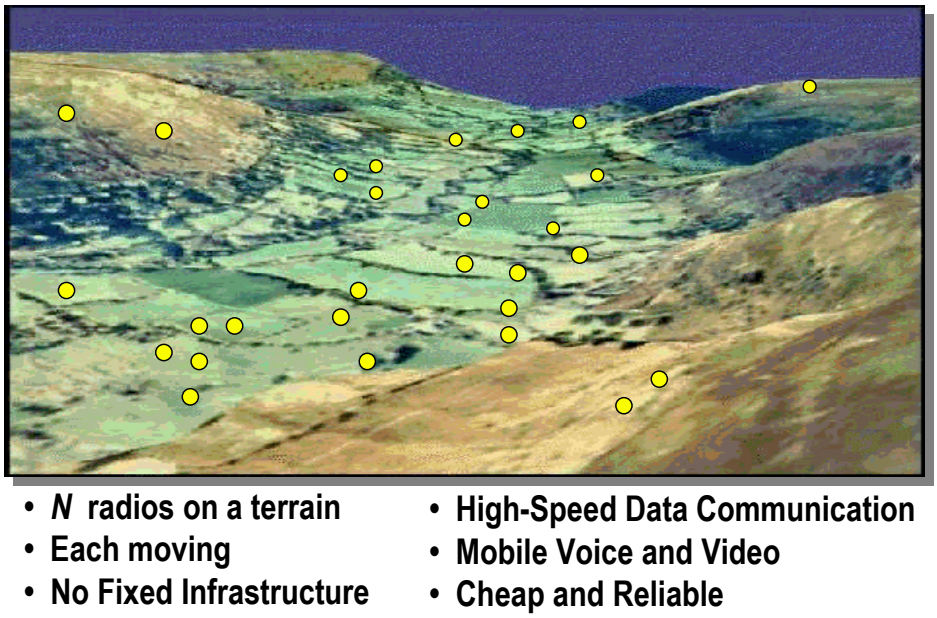


Figure 3.3.1 Mobile ad hoc network scenario (from [30]).

technology continues to progress. In addition to those suggested in Figure 3.3.1, MANETs are usually assumed to have the following operational requirements [28]:

- Since the nodes are mobile, the network topology may change rapidly and unpredictably over time. The network is decentralized, where all network activity, including discovering the topology and delivering messages, must be executed by the nodes themselves, i.e., routing functionality will be incorporated into mobile nodes.
- MANETs need efficient distributed algorithms to determine network organization, link scheduling, and routing. However, determining viable routing paths and delivering messages in a decentralized environment where network topology fluctuates is not a well-defined problem. While the shortest path (based on a given cost function) from a source to a destination in a static network is usually the optimal route, this idea is not easily extended to MANETs. Factors such as variable wireless link quality, propagation path loss, fading, multiuser interference, power expended, and topological changes, become relevant issues. The network should be able to adaptively alter the routing paths to alleviate any of these effects.

3.3.1 The Potential of Ad Hoc Networks

While certain types of wireless systems have enjoyed unprecedented commercial success based on consumer acceptance, which has fueled fast development of competing hardware and software (protocol) components, the development of MANETs has been relatively slow. The military (and public safety) advantages of a well functioning MANET are obvious, but a commercial "killer application" with powerful economic incentives has yet to appear for such a system with all the adaptive capabilities that are typically associated with MANETs.

The "vision" for wireless ad hoc networks is well expressed in a military context as [30]

> Every node in such a network has sufficient intelligence to continuously sense and discover other nearby nodes, dynamically determine the optimal path for forwarding data packets from itself hop by hop through the network to any other node in the network, and automatically heal any ruptures in the network fabric that are caused by ongoing movement of the nodes themselves, changes in RF propagation, destruction of nodes, etc. In essence, one need merely launch such radio nodes into some space and they will not only organize themselves into a network but also adapt continuously to changes in the network's connectivity.

The potential advantages of wireless ad hoc networks in terms of performance include the following:

- *As-needed and robust connectivity*. What if every mobile radio terminal (including cell phones) was capable of relaying transmissions? The possibilities for routing messages over multihop connections would be enormous, practically guaranteeing that some "path" from the message source to the message destination exists and is available at a given time.
- *Enhanced capacity*. For fixed networks, hierarchically organized (connection-oriented) networks are very efficient for assumed traffic conditions. However, if the network nodes are moving and/or the traffic distribution is itself rapidly varying, the optimal organization of routes among nodes cannot be fixed. As illustrated in Figure 3.3.2, wireless ad hoc networking offers enhanced network performance by permitting traffic to flow over network paths as needed, rather than through pre-configured paths that may contain bottlenecks. With this degree of "spatial re-use," it would even be possible to split the traffic from a high-bandwidth source into several parallel streams that flow over separate paths.

3.3.2 MANET Routing Protocols

MANETs, as a field of study, has largely been defined by the search for efficient routing protocols that can take full advantage of the possibilities for "as needed" multihop connections between autonomous terminals in a mobile network. The challenge has been to devise efficient

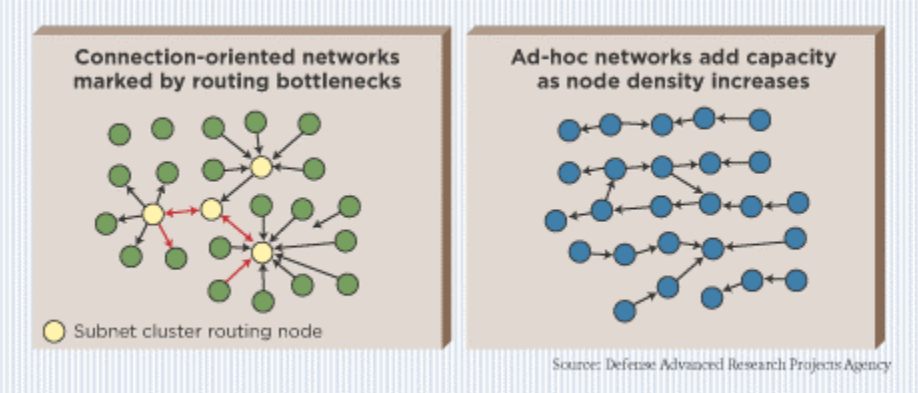


Figure 3.3.2 Increased wireless system performance using ad hoc networking (from [31]).

signaling techniques to accomplish the distributed routing without unduly increasing the overhead on the channel. The routing protocols developed for wireless ad hoc networks are based on the various assumptions that are made by the protocol. For example [32]:

- *State information*. How much information on the topology of the network is available at each node?
  - For link-state protocols, every node advertises its connectivity with each of its neighbor nodes and this information is propagated throughout the network so that each node can calculate end-to-end routes based on topology.
  - For destination-based protocols, nodes do not maintain information on the topology of the network as a whole. Instead, a "distance vector" table is maintained for "active routes" that indicates the hop distances to other nodes and the next node in an efficient path to each destination.
- *Scheduling*. Is route information continually maintained for each destination?
  - For proactive or table-driven protocols, nodes exchange route information periodically and/or in response to a topology change. At the expense of overhead traffic, these protocols have a route or distance vector ready to use for any destination node, as suggested in Figure 3.3.3.
  - For reactive or on-demand protocols, routes are developed only when needed by a "route discovery" process that introduces delay but minimizes overhead traffic, as illustrated in Figure 3.3.4.

Many ad hoc routing protocols have been proposed with different combinations and degrees of these characteristics. Figure 3.3.5 gives one possibly "family tree" for the protocols, identified by acronyms (see [33] for details of the protocols themselves).

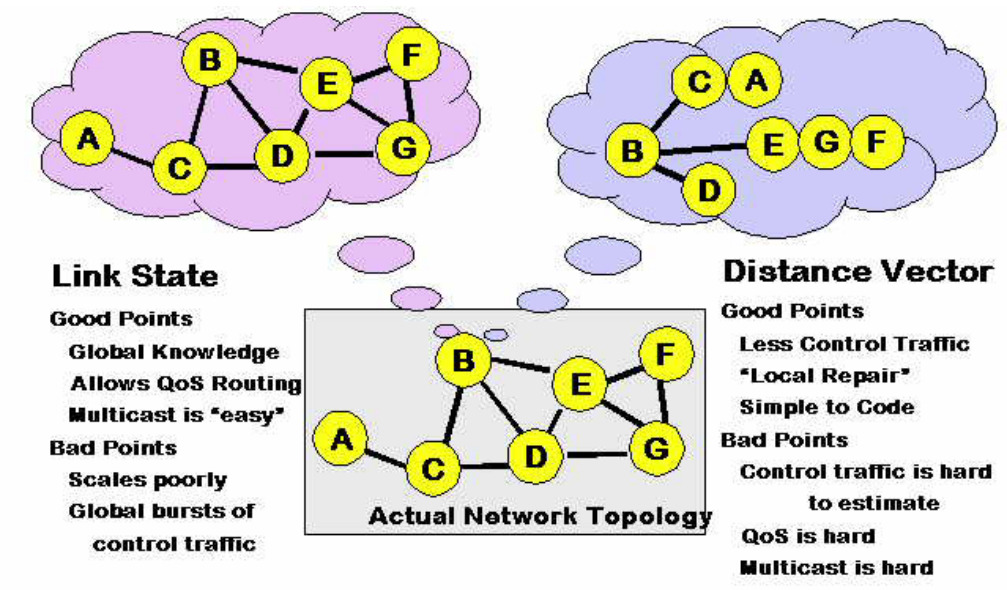


Figure 3.3.3 Proactive MANET routing protocol comparisons (from [30]).

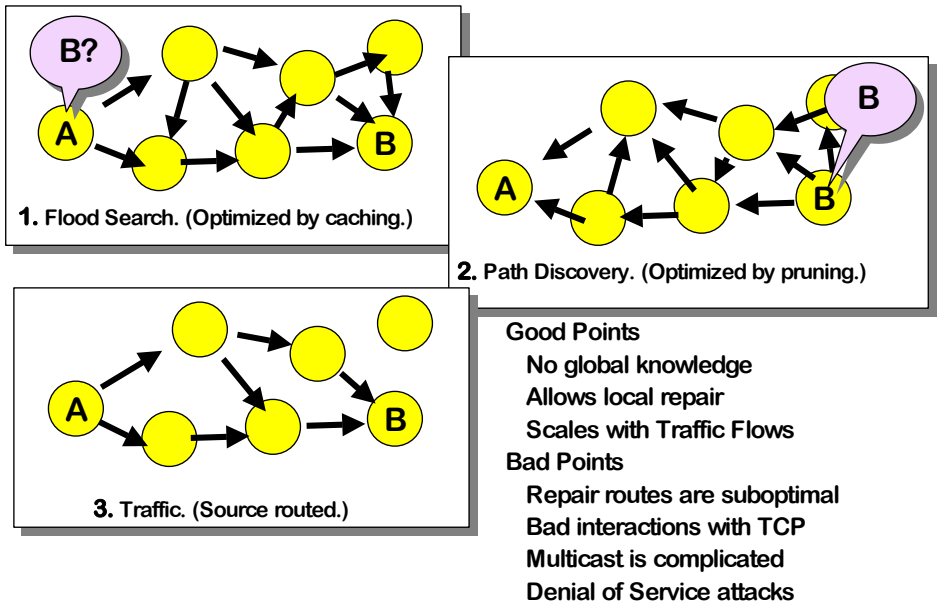


Figure 3.3.4 On-demand MANET routing protocol properties (from [30]).

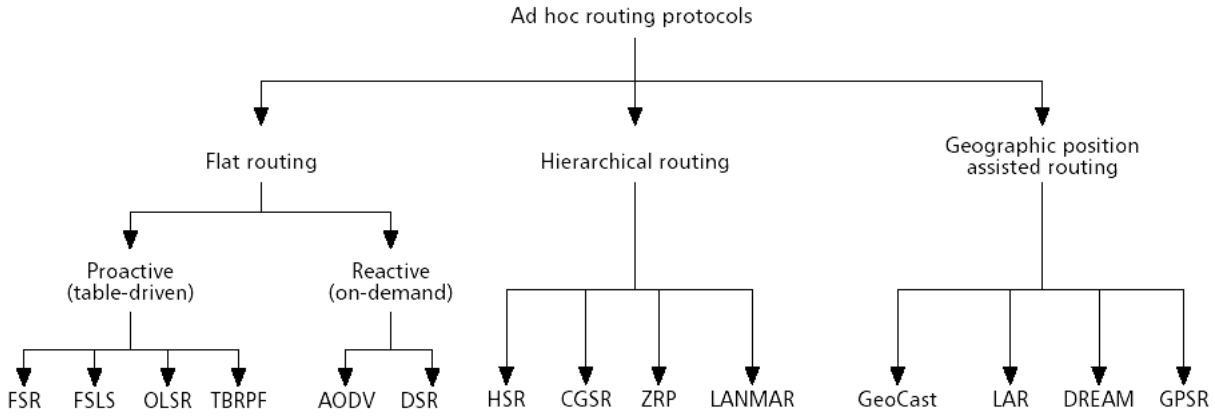


Figure 3.3.5 A possible classification of ad hoc routing protocols (from [33]).

Note that the classification in Figure 3.3.5 includes a class of MANET routing protocols that make use of geographic position information, while the majority of protocols included do not make use of such information. For mobile wireless networks, increasingly it is being understood that "cross-layer" techniques,—in which information from the physical layer (PHY), such as location and received signal power, are made available to the routing and other upper layers and quality of service and other parameters are made available to the MAC and PHY layers,—are necessary to realize the full potential of multihop communications. In other words, when designing a wireless ad hoc network, a better solution is more likely when all factors are taken into consideration at each level of network operation, as difficult as it may be to manage this rather large optimization problem and to maintain interoperability with standard networking protocols.

For example, many simulations and experimental MANETs assume or utilize a given routing protocol operating over a wireless network with the IEEE 802.11 (WLAN) MAC and PHY layers in the distributed coordination mode. Even with the collision-avoidance mechanisms of 802.11, including the exchange of RTS and CTS messages, the sensing of network topology is not sufficient to eliminate inefficiencies due to hidden and exposed terminals. Depending on the scenario and specific network topology, it has been shown [34] that the 802.11 MAC layer mechanisms are not sufficiently aware of hidden terminal problems that can occur. Also, the 802.11 MAC cannot guarantee quality of service (QoS) to any user, in terms of network delay; an advanced MAC/PHY contention access scheme based on a careful analysis of carrier-sense and collision distances in a wireless network is shown in [35] to provide such QoS guarantees.

4. Jurisdiction Area Network Technologies

As defined in the SAFECOM SoR, a Jurisdiction Area Network (JAN) is the permanent network infrastructure in a particular city or area that is dedicated to public safety communications (PSC) and is capable of connecting to larger area networks. Historically, such networks have consisted of analog voice capabilities provisioned to cover specific geographical areas using land mobile radio (LMR). The economic and engineering factors of PSC have traditionally favored centralized (broadcast) facilities with rather long-distance radio links compared to commercial cellular and telecommunication systems that use short-distance links to effect higher user capacity through spatial re-use of frequency resources. In recent years, however, PSC users, besides being more numerous, have begun to demand more than voice connectivity—they want broadband data services that cannot be supported by the traditional PSC systems.

In this section, we briefly describe the current prospects for implementing broadband PCS, then summarize the enabling technologies for broadband PSC in a JAN (WiMAX and mesh networking).

4.1 Prospects for Broadband PSC

Although there are some PSC systems experimenting with data networks in the unlicensed 2.4GHz and 5.8 GHz bands using 802.11 technology and mesh networking, the prospects for high-speed data networking for PSC are more promising in the frequency bands that have dedicated to public safety use, at 700 MHz and at 4.9 GHz, since those bands will not have to be shared with commercial and consumer systems.

4.1.1 Opportunities at 700 MHz

The FCC has allocated 24 MHz of spectrum for public safety services at 764-776 MHz and 794-806 MHz (referred to as the 700 MHz band). On August 6, 1998, the FCC adopted a *First Report and Order and Third Notice of Proposed Rule Making* that established a band plan and service rules for this spectrum. That plan was later modified three times with the current *Fourth Memorandum Opinion and Order* serving as the basis for current spectrum use and rules. Table 4.1.1 breaks out plans for how the spectrum will be allocated [36].

Interoperability standards for the public safety communications channels in the 700 MHz were recommended by the public safety National Coordination Committee (NCC) [37]. For the wideband channels required to be interoperable, the NCC recommended a system using Scalable Adaptive Modulation (SAM) [38], a form of multicarrier TDMA signaling with quadrature amplitude modulation (QAM) in various combinations to achieve high data rates on the 50 kHz channels while controlling adjacent channel interference. Figure 4.1.1 illustrates the flexibility of the per-carrier modulations in SAM in carrying from 2 to 6 bits per symbol, while Table 4.1.2 shows the adaptability of SAM to different bandwidths by adding or subtracting subcarriers.

For example, the eight carriers of a 50-kHz system, each transmitting 4800 symbols per second, achieve an aggregate symbol rate of $8 \times 4800 = 38{,}400$ sps = 38.4 Ksps. Thus for the QPSK (2 bits/symbol) per-carrier modulation the aggregate bit rate is $2 \times 38.4 = 76.8$ Ksps, and for 16-QAM (4 bits/symbol) the aggregate bit rate is $4 \times 38.4 = 153.6$ Ksps

Table 4.1.1 Band plan for 700 MHz public safety spectrum (from [36]).

Designated Purpose	**Amount of Spectrum**	**Narrowband (6.25 kHz)**	**Wideband (50 kHz)**
General Use	12.5 MHz (52.1%)	7.7 MHz (1232 channels)	4.8 MHz (96 channels)
Interoperability	2.6 MHz (10.8%)	0.8 MHz (128 channels)	1.8 MHz (36 channels)
Secondary Trunking	0.2 MHz (0.8%)	0.2 MHz (32 channels)	—
State License	2.4 MHz (10.0%)	2.4 MHz (384 channels)	—
Low Power	0.3 MHz (1.3%)	0.3 MHz (48 channels)	—
Reserve	6.0 MHz (25.0%)	0.6 MHz (96 channels)	5.4 MHz (108 channels)
Total	24 MHz (100%)	12 MHz (1920 channels)	12 MHz (240 channels)

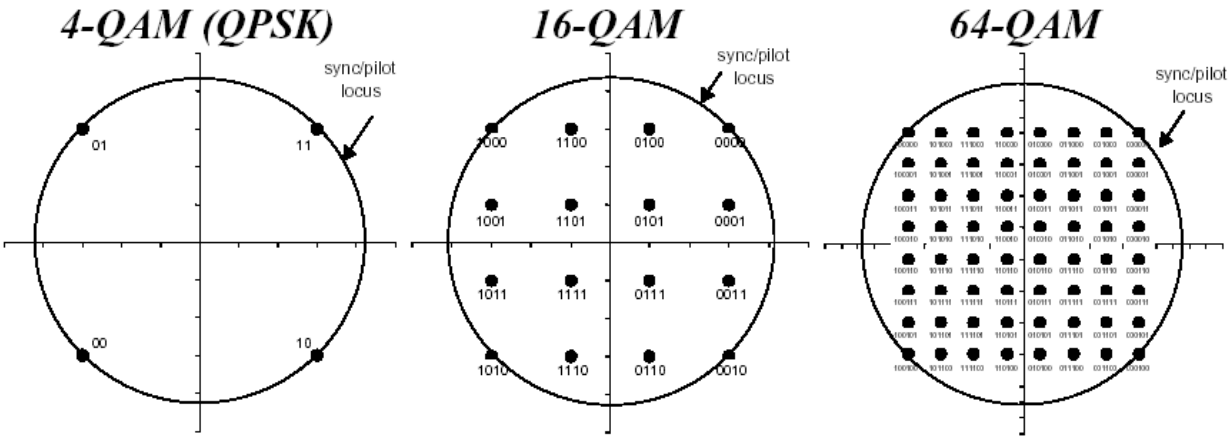


Figure 4.1.1 Selectable per-carrier modulations in the SAM system (from [38]).

Table 4.1.2 Total data rates for SAM for different available bandwidths (based on [38]).

Available bandwidth	50 kHz	100 kHz	150 kHz
Number of carriers	8	16	24
Symbol rate	4800 symbols/sec		
Aggregate data rates using			
* QPSK (2 bits per symbol)	76.8 Kbps	153.6 Kbps	230.4 Kbps
* 16QAM (4 bits per symbol)	153.6 Kbps	307.2 Kbps	460.8 Kbps
* 64QAM (6 bits per symbol)	230.4 Kbps	460.8 Kbps	691.2 Kbps

While the commercial communications market is advancing at a rapid pace, with the trend toward marrying 802.11 and third-generation cellular technologies, the bandwidth offered by cellular systems does not match the rates usually referred to as "wideband," although they are significantly higher than those that have been available to PSC until recently. Instead of utilizing the combination of existing cellular infrastructure and 802.11 equipment, the public safety community may be able to construct or lease its own infrastructure, with the bandwidth needed to guarantee reliable access (connection on demand) and low latency (delay). In the following paragraphs, we summarize current wideband data networking projects that are specifically oriented to PSC.

4.1.1.1 The Greenhouse Project

The Greenhouse is next generation technology being incrementally developed by Motorola in a test environment hosted by Pinellas County, Florida public safety [39, 40]. The Greenhouse provides a prototype wideband system to support 460 kbps wireless voice and data communications in the 700 MHz band. The project uses a 150 kHz experimental license in the 700 MHz public safety band that was commonly used for television channels 63, 64, 68 and 69. The technology utilizes the Scalable Adaptive Modulation (SAM) air protocol (described above), which has been adopted by TIA as a wideband data standard. IP networking is used throughout, including voice over IP with full duplexing and streaming video.

The system was developed not only to test wideband communication techniques but also the potential uses of wideband data by the public safety community. Some possibilities include

- a picture or sketch of a missing child or criminal suspect
- surveillance video of robberies shortly after they occur
- building plans and hydrant locations to firefighting vehicles
- fingerprints
- live video feeds of police pursuits
- Videoconferencing between dispatchers and mobile units
- The ability to conduct remote situation analysis

Other benefits of a wideband data capability include those that extend a public safety agency's host computer applications to the field, permitting, for example, the equivalent of police station roll-call briefings to be conducted without officers coming to the station house and allowing officers to conduct all the computer work in the field that they otherwise might have to conduct at the station. Wideband data supports email, including instant messages and attachments. It supports other networking applications such as automatic vehicle location, computer-aided dispatch, and access to national and state crime databases.

The Greenhouse system is installed in selected Pinellas County Sheriff's Office cruisers, a county EMS ambulance, the Largo Fire Department's rescue truck, a deputy chief vehicle and a mobile unit. Users operate the system via a touch-screen, color display panel mounted in the vehicles. Each unit can communicate and share information with the other agencies. Specially equipped police and EMS dispatch positions support these units.

4.1.1.2 Progress Toward PSC in the 700 MHz Band

As discussed above, the uses of the portions of the radio spectrum in the 700 MHz band that are allocated for public safety communications (formerly assigned to UHF TV) are being coordinated by regional planning committees (RPCs) with the help of the CAPRAD database system [36]. Details of the channel plan to divide the 24 MHz of spectrum into either narrowband (6.25 kHz) and wideband (50 kHz) channels are shown in Table 4.1.1. Interoperability standards for this band feature the SAM modulation; the Pinellas County, Florida test system described in the previous section uses the developing 700 MHz standards.

A recent report by the 700 MHz Advocacy subcommittee of the NPSTC spectrum management committee [41] listed ongoing developments that include the following:

- 700 MHz TV channel clearing: public safety groups are urging early clearing of the channels so that the spectrum can be used by public safety communications as planned; the FCC may impose a deadline of January 2009 for this process, but NPSTC and others are urging a 2006 deadline for stations now in channels 60-69.
- In some localities, FCC waivers on channel spacing rules are being sought to allow operation of public safety LMR in the 700 MHz band along with local TV stations; while this is not a substitute for clearing the band, public safety groups are supporting these waivers and seeking guidelines for "short spacing" in the interim.
- Even though the TV channels are to be cleared, the FCC is still issuing licenses to public TV stations; this policy is opposed by public safety organizations because it tends to delay the channel clearing.
- The NCC-recommended standards for 50 kHz wideband digital radio (TIA 902) have yet to be approved by the FCC.
- APCO and others are asking the FCC to change its rules against making or using dual-mode 12.5 kHz/6.25 kHz digital radios after January 2007.
- Steps are being taken to make the station ID rules in the 700 MHz band conform to those for the 800 MHz band.
- NPSTC is asking the FCC to clarify whether the 800 MHz band's rules for fixed secondary operations will apply to public safety radio in the 700 MHz band.

4.1.2 PSC Opportunities at 4.9 GHz

More and more consideration is being given to allocating frequencies above 800 MHz to public safety use, generally by deallocating them from other uses. Currently, the only example of such a deallocation is the transfer of 60 MHz in the 4.9 GHz band from Federal Government use to public safety use [42, 43], including the frequencies listed in Table 4.1.3. The intent of this transfer is to promote effective public safety communications and innovation in wireless broadband services in support of public safety. The rules for licensing the 4.9 GHz band are intended to accommodate a variety of new broadband applications such as high-speed digital technologies and wireless local area networks for incident scene management, dispatch

Table 4.1.3 State and Local Public Safety Frequency Allocations Above the 800 MHz Band.

Frequency Band (MHz)	Public Safety Allocation (MHz)	Number of Public Safety Channels	Comments
4940–4990 4.9GHz Band	50	TBD	Supports new broadband applications such as high-speed digital data and wireless local area networks for incident scene management. The spectrum also can support dispatch operations and vehicular or personal communications.

operations and vehicular operations, as well as to foster interoperability by providing a regulatory framework in which traditional public safety entities can pursue strategic partnerships with both traditional public safety entities, such as the Federal Government, and non-traditional public safety entities, such as utilities and commercial entities. [43]

Planning for the use of the 50 MHz of spectrum in the 4.9 GHz band that was transferred from Federal Government use to public safety use is underway. Some of the issues are discussed in the following article [44]:

> The public-safety community faces a dilemma: Does it make widespread Wi-Fi deployments in the unlicensed 2.4 GHz band today despite the security risks or wait for a better solution? The Federal Communications Commission has allocated a significant amount of spectrum in the 4.9 GHz band for exclusive use by the public-safety community. The vision is to deploy 802.11-compliant technology in the band so that public-safety groups can realize all the benefits of Wi-Fi without competing with other users clamoring to get on the band.
>
> …But the road to the 4.9 GHz band contains hurdles. Public-safety organizations are working with 802.11 equipment manufacturers and standards bodies to create a tweaked 802.11 series standard in order to leverage economies of scale and Wi-Fi functionality. But the effort may be thwarted, because the FCC adopted emission mask standards that are incompatible with emission standards established by the 802.11 community. The National Public Safety Telecommunications Council (NPSTC) and various public-safety agencies are urging the FCC to adopt a scaled orthogonal frequency division multiplex-based emission mask that would ensure Cisco and other 802.11 vendors also would build to the 4.9 GHz band.
>
> …If the FCC relaxes the emission guidelines, which it initially adopted on the recommendation of Motorola, public-safety organizations immediately could access equipment. Japan already supports Wi-Fi in the 4.9 GHz band, while chipsets are plentiful from global commercial vendors for the 802.11a standard and HiperLAN[13] standard at 5 GHz, which also can be used in the 4.9 GHz band.
>
> Further complicating matters is the commission's adoption of a geographic licensing scheme for the 4.9 GHz band that allows a public-safety entity to seek a non-exclusive license to operate throughout the geographical area within its political jurisdiction. That means a number of agencies must share access to a particular hot spot, which could slow deployments….

It is clear from Figure 4.1.2 that the issue of the mask is not the slight increase in effective bandwidth using the IEEE 802.11 mask; it is the use of an existing open standard that is likely to reduce the cost of equipment available to public safety users. As explained by the then NPSTC frequency planning chairman [45],

[13] HiperLAN is a European WLAN standard.

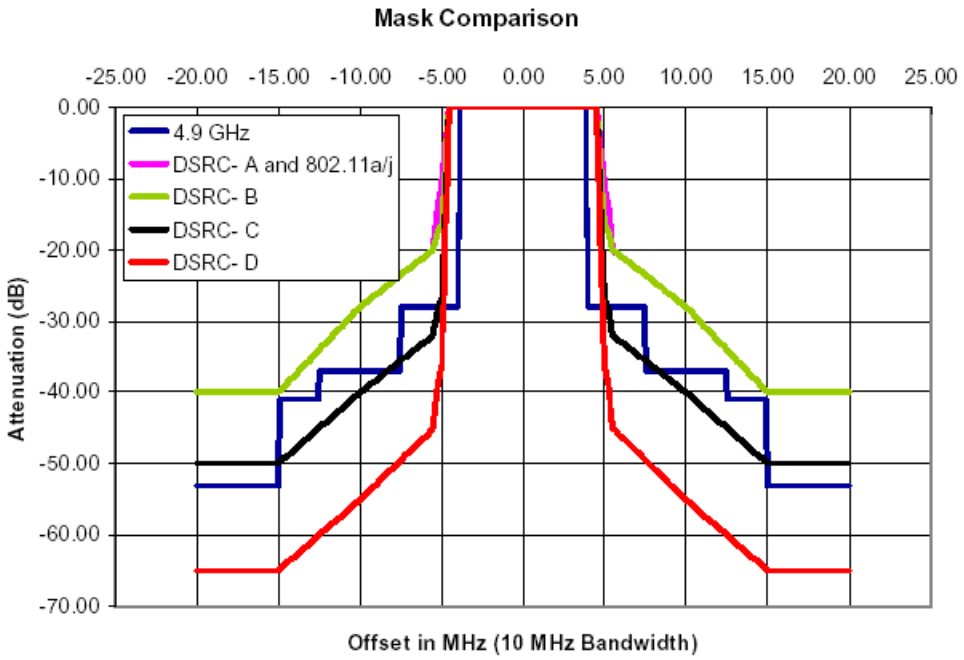


Figure 4.1.2 Comparison: FCC mask for 4.9 GHz with 802.11, DSRC masks (from [45]).[14]

> "[Vendors…] don't want to see nine vendors on a bid…and we don't want to send our a request for proposal and get two bids." The concern is that a limited number of vendors cannot possibly maintain the pace of innovation that will be realized in the market,….

4.2 Enabling Technologies for Broadband PSC JANs

Besides the improved LMR digital systems featuring scalable adaptive modulation and the appropriation of 802.11 technology from WLAN use to wider-area networking, the realization of broadband PSC for JANs is expected to gain from the deployment of IEEE 802.16 (WiMAX) technology. For both 802.11 and 802.16 networks, "mesh networking" concepts are being developed by several vendors and research institutions. In the following subsections, we summarize the characteristics of WiMAX and the concepts of mesh networking.

4.2.1 WiMAX (IEEE 802.16)

The IEEE 802.16 standard [46], trademarked by the IEEE as WirelessMAN and promoted commercially as one of two WiMAX technologies [47], was originally developed to specify the air interface, including the medium access control (MAC) and physical (PHY) layers, of fixed point-to-multipoint broadband wireless access systems providing multimedia services [48]. The system functions in many ways as a wireless version of the "last mile" of a fiber-optic cable system. Using synchronized burst transmissions, different users time share the same channel,

[14] DSRC = Dedicated Short Range Communications, a variant of 802.11 adapted for vehicular networking at 5.9 GHz.

and the uplink and downlink can be on the same frequency as in time-division duplexing (TDD) or on different frequencies as in frequency-division duplexing (FDD). The primary frequency bands of interest for the system, which affect the design of the MAC and PHY, include

- Licensed spectrum at 10 to 66 GHz, using adaptable-rate single-carrier (SC) quadrature amplitude modulation (QAM) using 2, 4, or 6 bits per symbol, respectively QPSK, QAM-16, or QAM-64, depending on the radio channel conditions, as illustrated in Figure 4.2.1. Depending on the bandwidth of the frequency channels used, this system can provide users with raw data rates up to 100 Mbits/s or slightly more, to be shared by the active users.
- Licensed or unlicensed spectrum below 11 GHz, using one of three schemes:
    - A SC modulation similar to the one used at 10 to 66 GHz, but including BPSK (1 bit per symbol) or spread BPSK (less than one bit per symbol) plus error-correction coding to accommodate possibly more severe environmental conditions of non-line-of-sight (NLOS) operations.
    - A multiple carrier modulation—orthogonal frequency-division multiplexing (OFDM)—with powerful error-correction coding to combat fading and other NLOS effects. As illustrated in Figure 4.2.2, in OFDM instead of a single carrier with a relatively fast modulation rate, multiple (256) carriers are used, each with a relatively slow modulation rate that is more robust in multipath propagation situations. Also, some of the carriers can be "pilots" with no data to enable measurement of the radio channel effects. As with the SC scheme,

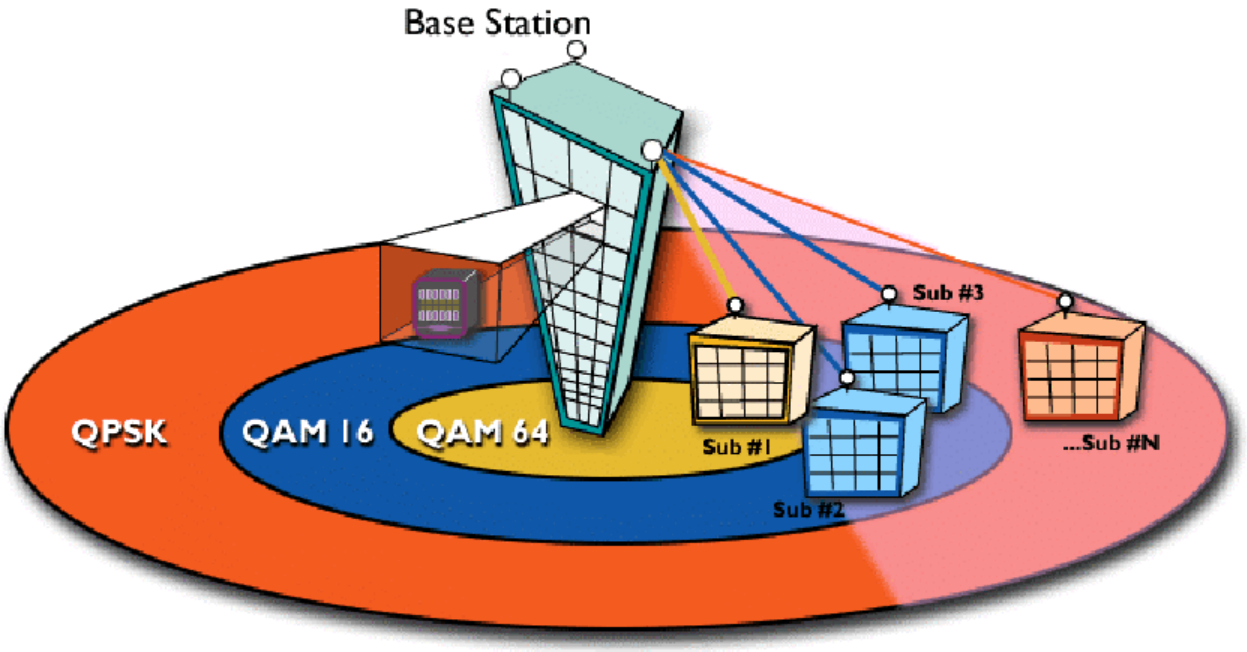


Figure 4.2.1 Adaptation of 802.16 data modulation to link conditions (from [48]).

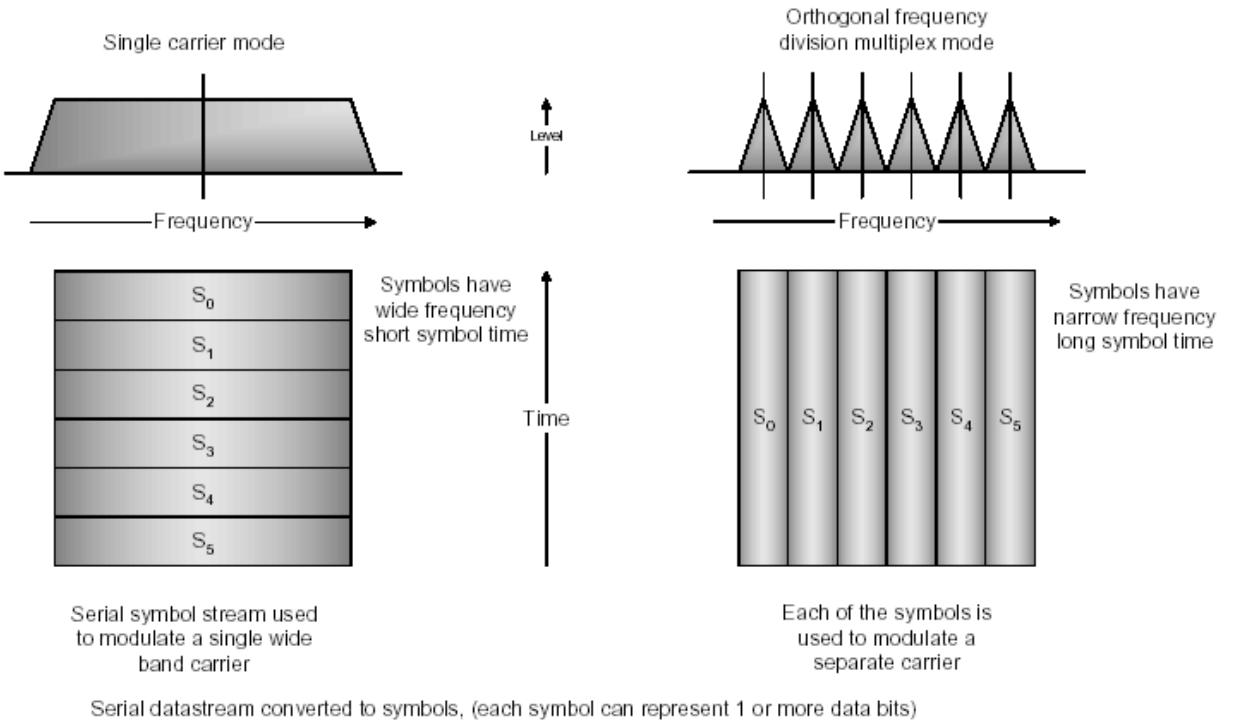


Figure 4.2.2 Comparison of single-carrier and OFDM modulations (from [50]).

different users time-share the radio channel by sending bursts of data at assigned times. This version of 802.16 can operate in an optional mesh networking mode.

- An alternative OFDM scheme (orthogonal frequency-division multiple access or OFDMA) that specifically provides for simultaneous access to the radio channel by multiple users by assigning their transmissions to different OFDM carriers for certain intervals instead of occupying the whole channel by turns.

The 802.16 standards are designed to apply to a variety of situations within the category of fixed wireless services, and the data rate that is delivered to users is dependent on the bandwidth of the frequency channels as well as propagation conditions. The below-11GHz variations all can use the following options [46]:

- Adaptive antenna system (AAS): uses more than one antenna element to improve range and system capacity by adapting the antenna pattern and concentrating the transmitter's energy to individual subscribers.
- Automatic repeat request (ARQ): allows resending of data that was received in error.
- Space-time coding (STC): provides for repetition of data for transmission over two different antennas to achieve a diversity gain.

For PSC use, rather than fixed users it is more appropriate to anticipate mobile users. The IEEE 802.20 working group is developing a standard specifically for mobile broadband wireless access

(MBWA) in licensed bands below 3.5 GHz. The 802.20 air interface will be optimized for the transport of Internet protocol (IP)-based services [51], unlike synchronous (streaming) P25 digital radio systems. By contrast, 802.16 wireless data systems in addition to "connectionless" IP services can support connection-based services such as ATM (asynchronous transfer mode) that are considered to be more suitable for serving both low-latency data and voice applications [52]. A task group in the 802.16 working group of the IEEE is now nearing completion of a standard to be known as 802.16e that provides "mobility enhancements" for 802.16 systems that make it a candidate for JAN applications, since it will support combined fixed and mobile operation in licensed bands. The enhancements to 802.16 that will be supported by 802.16e are said to include the following [53]:

- Addition of overhead information to facilitate mobility, handoffs, etc.; allowance for user speeds up to 150 kph (95 mph).
- A scalable version of OFDMA (SOFDMA) that provides for many more than the current 256 OFDM symbol frequencies in the same bandwidth, each with slower modulation that is more robust in the mobile radio channel. The number of frequencies is variable from 128 to 2048 [54].
- Data rates up to 11 Mb/s in a 3.5 MHz channel, to be shared by the users [54].
- Addition of Advanced Encryption System (AES) functionality for better security.

4.2.2 Mesh Networking

While MANETs and packet radio systems are usually conceived as applying to very general wireless communication scenarios, recently there has been interest not so much in mobility as in optimizing the design of ad hoc wireless networks for the purpose of implementing on-demand, adaptive configuration of radio networks that must cover a certain geographical area and/or provide connectivity for a certain kind of data traffic. This interest has led to the development of "mesh" networking concepts. The term "mesh" refers to a grid pattern of connectivity, as opposed to a "star" pattern. The outstanding difference between the two kinds of networks is that the mesh offers many alternative paths between arbitrary pairs of nodes, whereas the star has much fewer paths, all of which much go through the central node. For that reason, mesh network connectivity is regarded as a means to provide reliable coverage.

Wireless mesh networks (WMNs) have been developed as an alternative technology for providing broadband Internet "last mile" access that is competitive with cable, high-speed telephony (DSL), wireless local loop, and satellite. For the network of Figure 4.2.3, the mesh is the network of users (homes) connected to the broadband system, either directly or via multiple hops. For the network illustrated in Figure 4.2.4, the mesh is the network of users as well as the Internet access points (gateway nodes). Typically, in a WMN, each node operates not only as data source/destination (host) but also as a wireless router. As in wireless ad hoc networks and MANETs, the network is capable of dynamic self-organization and reconfiguration, with the nodes in the network autonomously finding and maintaining routes among themselves. WMNs are relatively inexpensive to start up, and as more nodes are added, the reliability and network coverage increase [56].

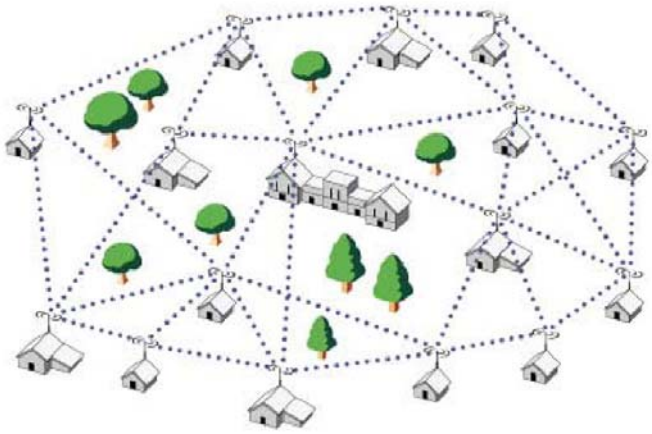


Figure 4.2.3 Mesh network for residential broadband access system (from 55]).

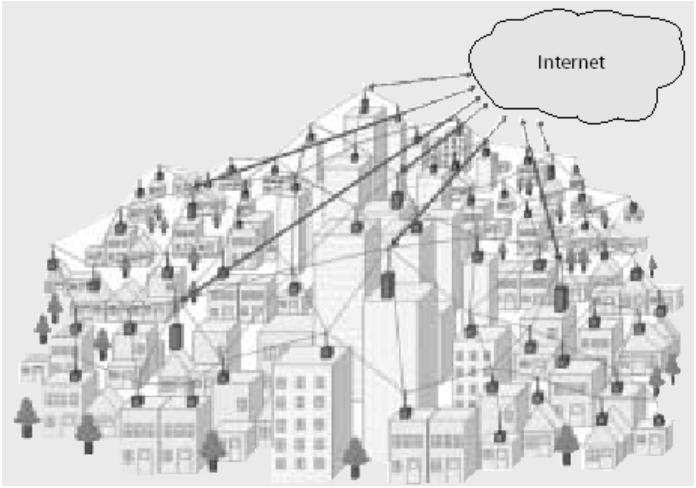


Figure 4.2.4 Mesh network providing broadband access to a city (from [56]).

Wireless mesh networking emulates a wired internet. For that reason, the propagation-related distance limitations that are often the worry of radio systems can actually be an advantage if used to engineer a network topology in which the degree of each node (the number of its neighbors) is low, like that of a mesh. Also, the multihop capabilities of mesh networking can simplify the deployment of the network, as suggested in Figure 4.2.5.

In addition to the broadband application, mesh networking concepts are being considered to extend WLAN coverage by enabling multihop connectivity, as illustrated in Figure 4.2.6. In fact, many of the mesh networking initiatives are based on supplementing 802.11 WLAN "hot spot" hardware with software that implements the ad hoc features of the mesh network, in effect creating an area coverage network of APs from different local area networks (BSSs). Standardization of mesh networking procedures for WLAN access points to form extended service sets is being pursued by the new IEEE 802.11s task group.

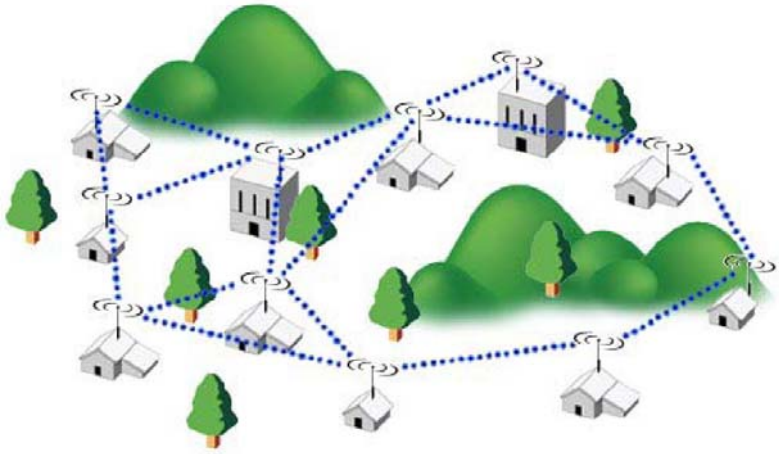


Figure 4.2.5 Mesh connectivity around obstacles to propagation (from [55]).

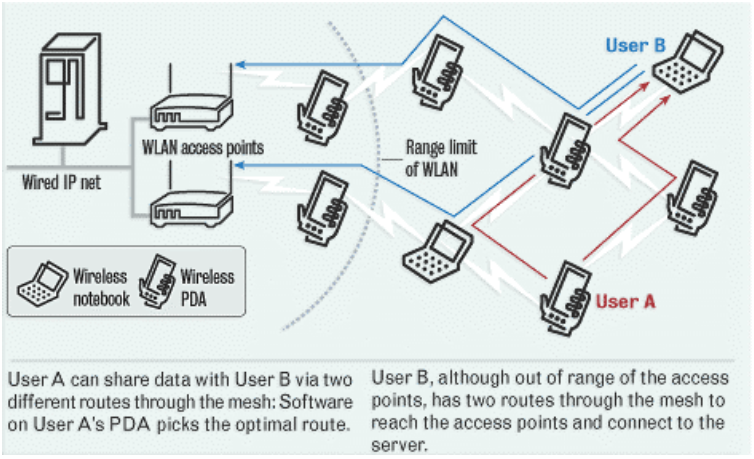


Figure 4.2.6 Use of mesh technology to extend the range of a WLAN (from [57]).

Mesh networking can be implemented in two basic modes: infrastructure and/or client (user) meshing; both are important and both are illustrated in Figure 4.2.7. Infrastructure meshing creates a wireless backhaul mesh network among wireless access points connected to the wired network, plus a tier of additional wireless relay (router) nodes as needed to provide connectivity. Client meshing enables formation of wireless ad hoc multihop networks of user devices, independent of any infrastructure. [58]

For large-area communication systems, even with extensive use of mesh networking it is almost inevitable that the overall network will have some hierarchical aspects, depending on the typical flows of information. For example, in the wireless broadband Internet access application the flow of data tends to be asymmetric in that most of the data is being sent from a few points (the Internet or PSTN access points) to many users. Another example is a system designed around a command and control organizational structure; in that case, the data flows are also

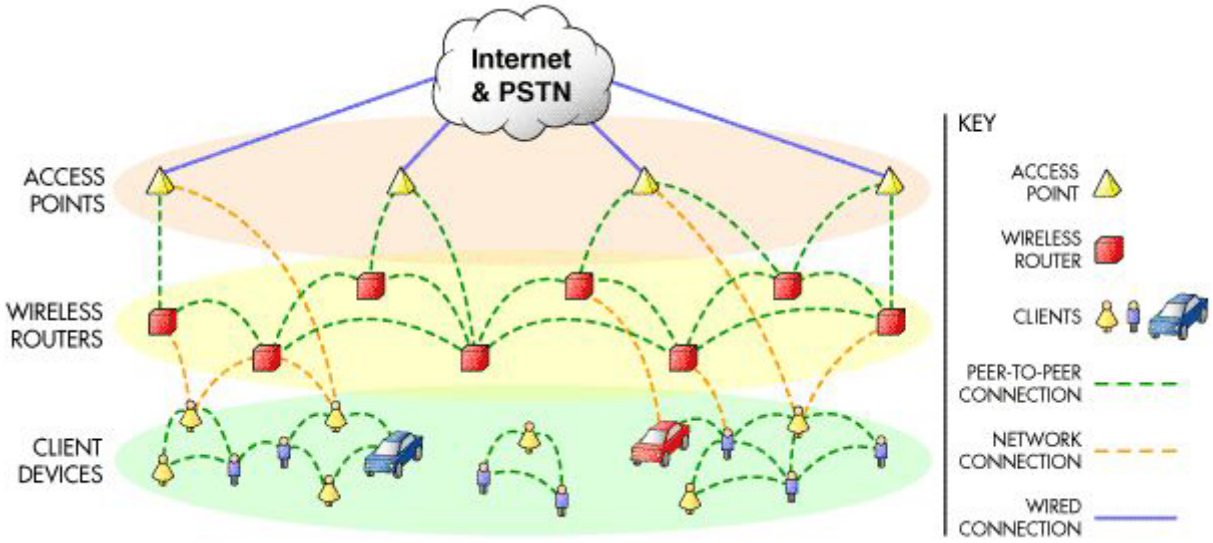


Figure 4.2.7 Mesh networking control of ad hoc connectivity (from [58]).

asymmetrical, but flowing from many points to a few collection points. In other cases, the hierarchy is a natural consequence of organizing the network coverage. For example, the U. S. Army's Near Term Digital Radio [30, 59] uses ad hoc networking techniques for both local "clusters" of mobile users and, on a different RF channel, a backbone network of tactical operations centers.

> The bulk of communications within the network is performed at very low power, i.e., from one cluster member directly to another or to a cluster head. This low power allows a great deal of spatial reuse, and thus boosts the overall network capacity. A smaller fraction of the traffic must traverse a "long haul" route from a cluster member to its cluster head, then across the backbone by a series of hops between cluster heads, and finally the ultimate delivery to its destination member. In this case, the first and last hops are performed on the local channel, and the backbone hops on the other channel. The backbone links are formed at relatively high power in order to form "giant steps" across the network. This arrangement of local transmissions at low power combined with long-haul transmissions at high power gives the balance between overall capacity and delay. [30]

As it is for packet radio, the use of multiple channels and/or radios in each terminal greatly enhances the flexibility and capacity of mesh networks, especially when a degree of hierarchy is involved in the application scenario. Using a single radio limits the capacity because the bandwidth of the radio channel has to be divided between communications at one network level or tier and another.

5. Appendix: Tutorials on Wireless Technology

In this appendix to the report, we supplement the description of wireless technologies that are candidates for implementing the SAFECOM SoR's vision of increased functionality and performance for public safety communication (PSC) systems by including selected background tutorial materials that relate to the theory and operation of the candidate technologies. A good understanding of the theory and operation of such systems is not absolutely necessary for PSC users and decision-makers to buy and use the technologies, but it is definitely key to forming a reasonable expectation of what is to be gained from using the technologies.

The selected background materials in this appendix include a brief description of the operation and performance of packet radio, a review of the technology supporting digital radio voice transmissions, and a summary of voice-over-Internet-Protocol (VoIP) technology.

5.1 Tutorial on Packet Radio

The purpose of this tutorial on packet radio is to enable the reader to appreciate the difference between real-time, continuous transmission of voice or other traffic over multiple dedicated radio channels—whether digital or analog—and "contention" among multiple users for access to a common channel using the principles of packet switching, such as used in computer networking, the Internet, and modern high-speed data networks.

Before "ad hoc networking," there was "packet radio." Many of the basic protocols used in current wireless systems were designed to make networks of wireless transceivers (nodes) operate together efficiently as a packet radio system. The problem to be solved by the protocols can be stated as follows [60]:

> A packet radio network consists of many packet radio units sharing a common radio channel such that when one unit transmits, many other units will hear the packet, even thought it is addressed to only one of them. This feature, inherent in broadcast systems, in conjunction with the fact that we have no control over access to the channel, results in destructive interference when several packets are received [from different transmitters] simultaneously.

5.1.1 Channel Access Protocols

In the early 1970s, unsatisfied with the high error rates for remote computer access on the local telephone lines, researchers at the University of Hawaii developed a radio access system using burst UHF transmissions to transmit packets of data between the terminals and the university's computer. The system, illustrated in Figure 5.1.1, became known as the ALOHA system. Communications from the uncoordinated remote terminals to the university computer took place on a single channel using a contention access scheme. Under this scheme, each terminal transmitted whenever it had a packet to send, such as when the user entered a keystroke on the keyboard of the remote terminal. If there was no collision with another user's transmission (or some other impairment), the university's terminal sent an acknowledgement over a separate radio channel. If no acknowledgement was issued, the sending terminal waited for a random amount of time and re-transmitted the packet.

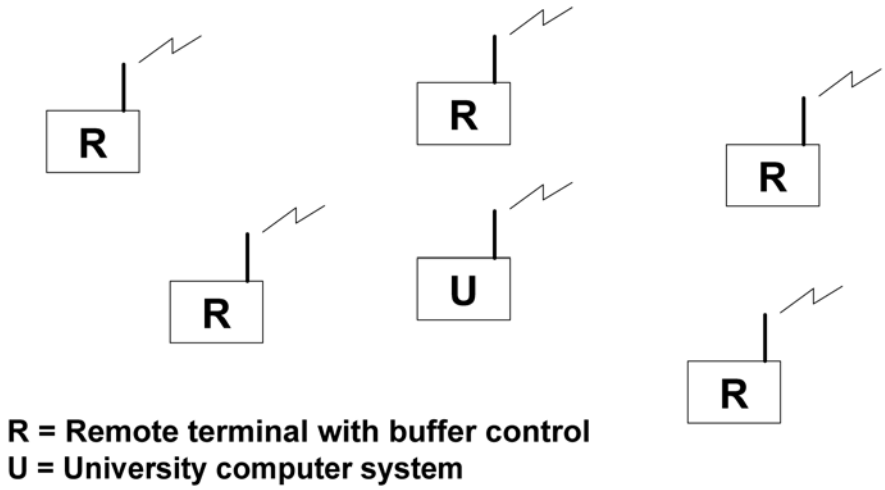


Figure 5.1.1 ALOHA packet radio network (based on [61]).

Suppose that the capacity of the radio link for the ALOHA contention access channel is C packets/sec, which would be achieved for a constant stream of back-to-back, non-colliding packets. Relative to C, the maximum throughput of the system is 1.0. Since the ALOHA terminals are not coordinated, there is a certain probability of collision that increases with the number of terminals having data to send, so it is to be expected that the practical limit on throughput is less than 1.0. A theoretical analysis of the system [62, 63] revealed that the highest relative throughput for ALOHA is only about 0.18, occurring when the rate of packets is half the packet capacity. To improve on this poor efficiency it was suggested [64] that, instead of allowing terminals to transmit at any arbitrary time, terminals should be restricted to transmitting at regular times or "slots." In this way, the type of collision would be eliminated in which the end of one packet interferes with another. As shown in Figure 5.1.2, theoretically this modification to ALOHA, called Slotted ALOHA, doubles the maximum throughput of the system; moreover, the peak occurs at a higher value of relative demand for the channel.

Since the ALOHA system, many protocols for contention access in wired and wireless networks have been developed. An important difference for wireless networks is that channel impairments such as noise and fading can cause packets to be lost, in addition to collisions. Some of the "classic" channel access (sometime called medium access control—MAC) protocols are the following:

- Carrier-sense multiple access (CSMA), in which a terminal "listens" to the channel before transmitting in order to defer or "back off" for a random interval if another terminal is already using the channel. This technique is designed to prevent packet collisions.
- CSMA with p-persistence [65], in which a terminal initially sensing that the channel is idle transmits with a certain probability p, or waits one slot with probability $1 - p$; if after waiting the terminal finds that the channel is busy, it backs off according to some random backoff distribution. If the terminal initially senses that the channel is busy, it waits until

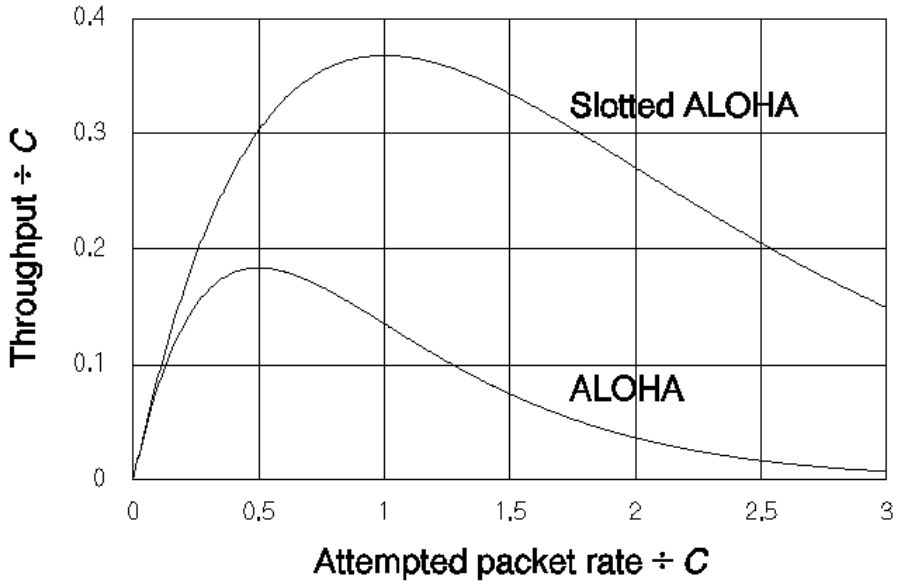


Figure 5.1.2 Theoretical performance of ALOHA and Slotted ALOHA.

the channel is idle and restarts the process of deciding whether to transmit. This protocol is designed to enhance CSMA by reducing the percentage of time that channel is idle between transmissions and therefore unproductive.

- CSMA with various mechanisms for collision detection (CD) and/or collision avoidance (CA). The IEEE 802.11 WLAN MAC protocol uses CSMA/CA.
- CSMA with various mechanisms to deal with hidden terminals, such as adding a signaling channel in which any terminal transmits a "busy tone" [66] if it senses that the message channel is busy; in this manner, terminals that cannot hear the channel activity of a distant terminal very likely will hear the busy tone and back off.
- Various backoff schemes designed to improve network efficiency.
- Various modulation techniques selected to make possible the "capture" of a packet by the intended receiver, with increased robustness to interference, thereby enabling correct detection of a packet in some cases even if a collision occurs.

The design of channel access schemes continues to be a subject of current research.

Figure 5.1.3 compares CSMA and 1-persistent CSMA under the ideal condition of zero propagation delay, implying that carrier-sensing is perfect except for hidden nodes; the non-unity relative throughput is due to wasted idle times when terminals are backing off. The Figure indicates that the persistent scheme does improve efficiency for reasonable amounts of demand by reducing such waste.

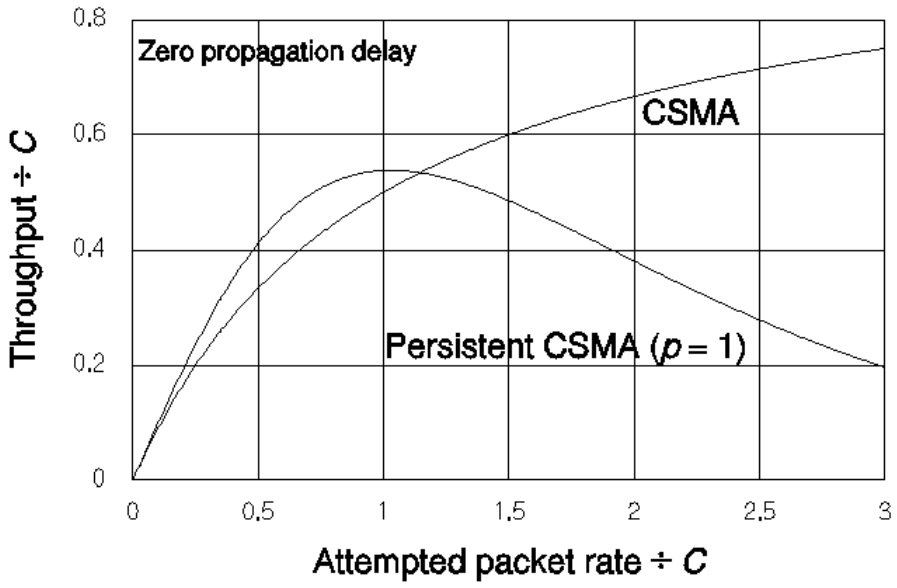


Figure 5.1.3 Throughput performance of CSMA for ideal condition of zero propagation delay.

5.1.2 Multihop Packet Routing Protocols

For various reasons, it may not be desirable for all the terminals in a packet radio network to be able to hear one another. The physical extent of the network may simply be too large for the desired transmitter power levels and/or battery-life requirements. Or, the design goal may be to implement a kind of spatial re-use of the radio channel [67], similar to that on which cellular telephone systems are based. In any event, in addition to the RF propagation and interference environment, the underlying topology of a packet radio network is a function of the radios' transmitter powers and receiver sensitivities—inexpensive radios tend to require more power at the receiver for successful communication.

Figure 5.1.4 shows a 100-node (terminal) network of identical terminals for which the transmitter power has been increased until it is just enough to make every terminal able to communicate with every other terminal, assuming that direct communication can take place between any two terminals that are no farther apart than a certain distance and that each terminal is able to relay packets between terminals that are far apart, as illustrated in Figure 5.1.5. The figure is an example of a network "graph" that is "connected;" for this example, the average number of "neighbors" for a node (other nodes with which it can communicate) is 3.3 and the average number of "hops" to connect any two nodes is 8.4.

As the study of packet radio networks progressed, researchers discovered approximate relations for network parameters that are necessary to support "multihop" (multiple hop) communications in which each node is capable of relaying a message intended for another node. For example, the "magic number" is the average number of neighbors to maintain connectivity for the whole network and to optimize throughput, and varies between six and eight, depending on several assumptions, including the rate at which signal power attenuates with distance. The

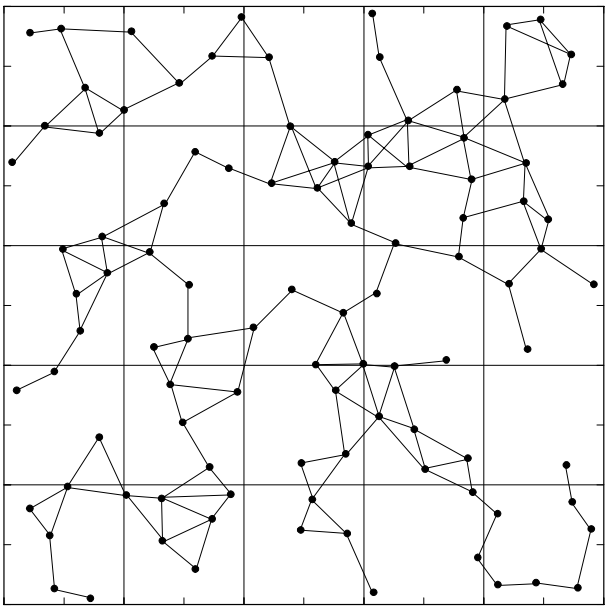


Figure 5.1.4 100-node mobile network topology having full connectivity (from [68]).

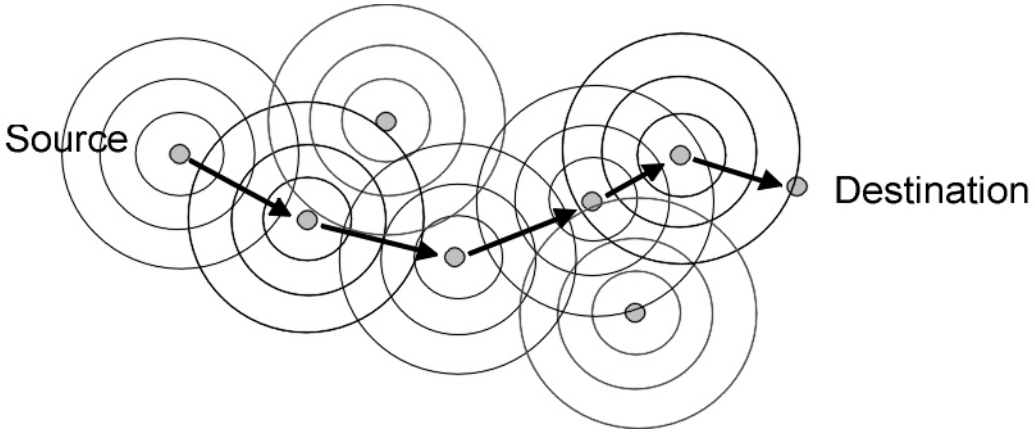


Figure 5.1.5 Multihop communication

average number of neighbors is, in turn, a function of transmitter power; as depicted in Figure 5.1.6, network throughput and delay are thus related to power. The analyses supporting these studies was based on one or more assumed methods for implementing multihop routing.

In addition to methods for assigning network addresses to terminals and for managing network flow, the task of devising a routing scheme to enable multihop communication in a packet radio network involves the following objectives [69]:

- Reliability: to assure, with a high probability, that a message launched into the network will arrive at its destination
- Low latency: to assure that messages will be delivered with a relatively small time delay

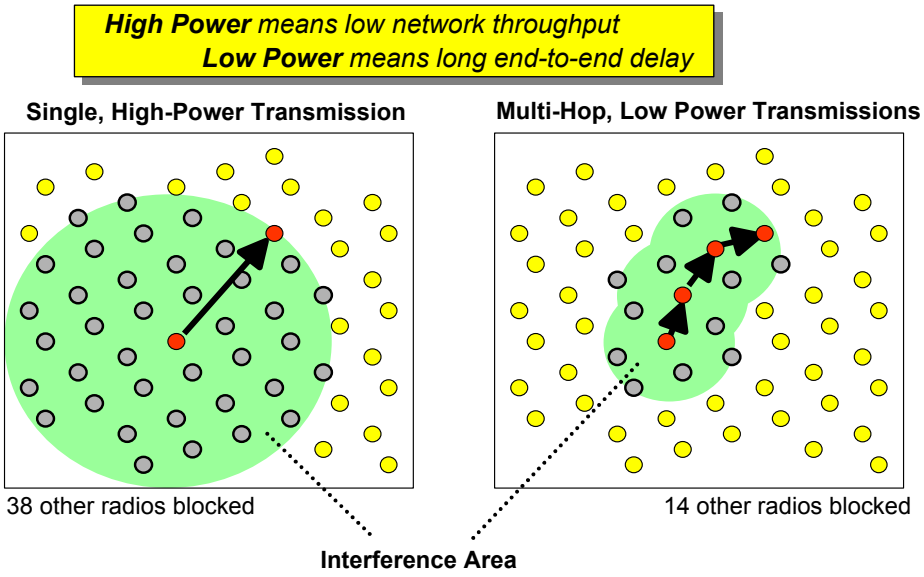


Figure 5.1.6 Effect of radio transmitter range on throughput and delay (from [30]).

- Low overhead: to assure that control traffic does not consume large amounts of channel capacity.

An obvious but significant constraint on routing schemes is the fact that, usually, a single radio channel is utilized and therefore the packet radio terminals cannot transmit and receive at the same time. Thus, for example, a terminal acting as a relay must wait until the entire reception of a packet to be forwarded is complete before retransmitting it. Some of the routing approaches considered in the early days for packet radio are the following [69][15]:

- Broadcast routing: the packet is "flooded" through the network as each node forwards it (only the first time it hears it) up to a certain number of hops. This scheme is very reliable, but involves a large number of unnecessary transmissions. Various techniques have been proposed to limit the unnecessary transmissions, mainly by increasing the capability of the nodes to learn and store information about the topology of the network and the relative locations of particular nodes.
- Hierarchical routing: the network is organized as a "tree" and labels (addresses) are given to each node in such a way as to embed the route from any particular node to the "root," as illustrated in Figure 5.1.7.
- Directed broadcast routing: Each node is assumed to know its distance from every other node, in hops. A node's broadcast of a message for a particular destination node is forwarded only by other nodes that are closer to the destination.
- Stationless routing: No central controlling node (station) is present, so each node must develop and retain its own information on the topology of the network and the routes to

[15] Mobile ad hoc networks (MANETs), as the current successors to packet radio networks, are now being designed with more sophisticated capabilities.

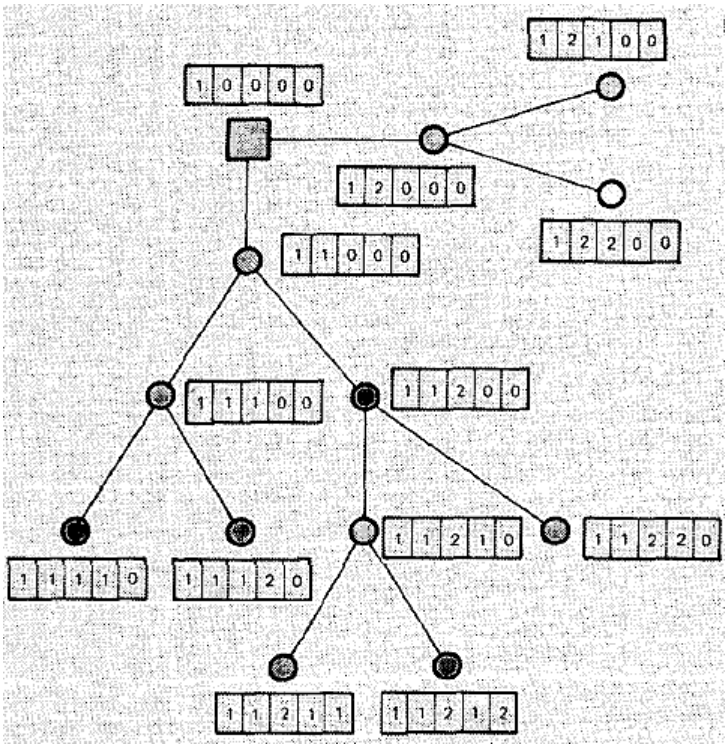


Figure 5.1.7 Hierarchical labels of repeaters and stations (from [69]).

other nodes. For example, a source node can flood a "route-finding packet" in the network, intended for a particular destination node, which returns a "route setup packet" that contains the addresses of the nodes that connect the source and destination.

- Multiple-station routing: An early version of cluster/zone-based routing.

5.2 Tutorial on Digital Voice

The purpose of this tutorial on digital voice technology is to introduce readers to the underlying engineering concepts so that they can appreciate the difference between conventional digital voice implementations and voice-over-IP implementations.

In 1996, the Technology Subcommittee of the PSWAC reported regarding public safety voice communications that [70]

> Most public safety communications systems use analog FM technology operating in 25 or 30 kHz channels to carry their voice signals. Public safety communications systems normally operate using a variant of one of two basic methods: repeater and trunked. While digital voice is a technological possibility, it is little used today in public safety communications. It is expected that digital voice systems will be offered by several manufacturers in the public safety market in the next few years.

It is well known that digital encoding of audio signals (including speech) can enhance the fidelity of the sound reproduction because it is less immune to certain types of noise and channel impairments. Since there is considerable redundancy in speech, theoretically it is possible to compress

the speech data in order to reduce the data rate required for real time transmission, and various compression (voice coding) modems have been developed with this objective. The quality of different techniques for digitally reproduced speech is somewhat subjective and is measured in terms of "mean opinion scores" by listeners in tests. As indicated in Figure 5.2.1, the state of the art in voice coding for a long time was such that near-toll-quality digital voice (quantified by the measure described in Table 5.2.1) is achieved for a base data rate of about 8 kilobits/sec (kbps), using "hybrid coding" that features compression (vocoding) of certain parts of the voice signal and non-compression (waveform coding) of other parts of the signal. [71]

In the last ten years many advances have been made in the design and implementation of low-rate vocoders, enabled in part by the increased power of computer chips. Using sophisticated signal processing algorithms, it is now possible to achieve acceptable speech quality for mobile applications using vocoder processing techniques to produce compressed speech at bit rates from 2 to 4 kbps. For Project 25, the TIA compared several low-rate vocoders, and selected an algorithm called Improved Multiband Excitation (IMBE), a proprietary digital signal processing approach from Digital Voice Systems, Inc. As illustrated in Figure 5.2.2 for different bit error rate and fading channel characteristics, this algorithm provided consistently better voice quality for the mobile channel than the other techniques evaluated.

Increasing demand for mobile radio channels has required the adoption of various techniques to improve spectrum efficiency, short of using digital voice modems, largely because the mobile radio market supported only existing, low-cost technology. When cellular radio developed "second generation" (2G) digital voice systems and reduced their cost by selling millions of cell phones, digital voice modems started appearing also in LMR products.

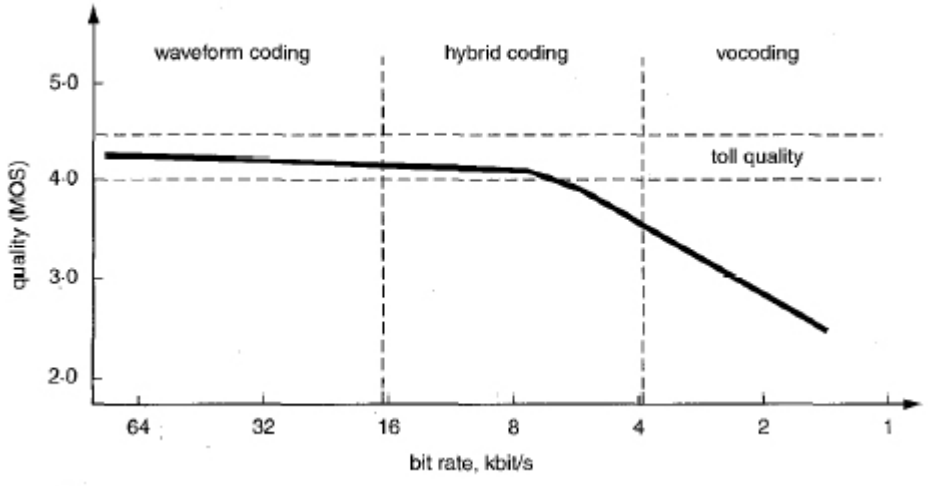


Figure 5.2.1 Quality of digital speech in terms of MOS ("mean opinion score") vs. bit rate for different types of voice coding (from [71]).

Table 5.2.1 MOS ranking and quality scale (from [72]).

Quality Scale	Excellent	Good	Fair	Poor	Bad
Score	5	4	3	2	1

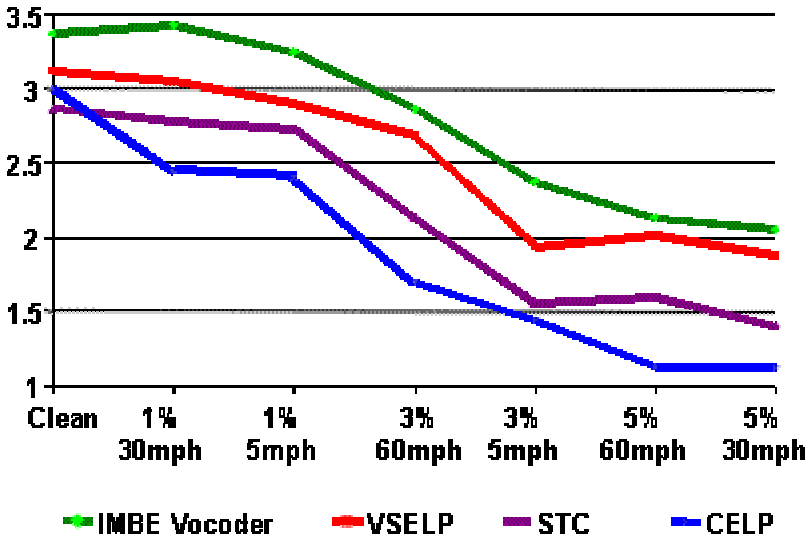


Figure 5.2.2 MOS ranking of different vocoders for Project 25 selection (from [73]).

In addition to voice coding to digitize speech, it is necessary to use forward error correction coding (FEC) techniques to combat impairments that are common on the mobile radio channel, such as multipath-induced fading and shadowing. All such coding introduces "overhead" because FEC is accomplished using redundancy. Typically, given a frame interval of speech data with a certain number of bits, as many as twice as many bits exit a FEC coder for that frame. Thus, while the voice source coding reduces the bit rate needed to carry high fidelity speech, the mobile channel error-correction coding increases the rate. In order to maintain a fixed signaling rate at the transmitter while introducing error-correction coding, the radio can use a digital modulation waveform that can carry multiple bits per pulse.

5.3 Tutorial on VoIP

The purpose of this tutorial is to provide the reader with background on the development of VoIP that will promote a good understanding of the issues involved with this technology.

In the circuit-switched PSTN, each call requires a dedicated 64-kbps connection between the two telephones for the duration of the call, regardless of voice activity from either telephone. The telephone company cannot use this bandwidth for any other purpose during the call and must bill the parties for consuming its resources. Data networking, on the other hand, has the capability to use bandwidth only when it is required. This difference, although seemingly small, is a major benefit of packet-based voice networking. [74] However, Internet protocol (IP) networks guarantee neither sufficient bandwidth for the voice traffic nor constant, acceptable delay; dropped packets and varying delays introduce distortions not found in traditional telephony [75]. Reconciling the potential and the reality of VoIP has led to standards for VoIP over wired networks—in this domain, developments have recently been accelerated by the adoption of the power over Ethernet (PoE) standard that enables telephones that plug only into an ordinary (wired) LAN connection [76]. VOIP development also has been taking place for wireless Ethernets (WLANs), with the additional challenges of connecting over wireless links.

5.3.1 VoIP Basics

For transmission of voice over a digital data network, a packet infrastructure, usually IP, replaces the telephone system's circuit-switching infrastructure. IP is attractive as the packet infrastructure because of its ubiquitous nature and the fact that it is the de facto application interface. Software applications running over IP do not have to be known; IP simply transports the data end to end, with no cognizance of the payload. On a congested IP network, the packets are subject to variable delays[16], which distort the received voice data, so to carry voice and other real-time applications, the IP network must have some knowledge of the applications in order to give them priority to compensate for delay and delay variation (jitter). [74]

Packets may travel by multiple paths in a wired network, and can even arrive out of order. To enable reconstruction of the correct sequence of packets and to assist in removing jitter, Real-time Transport Protocol (RTP) is utilized in addition to the usual User Datagram Protocol (UDP)/IP header to provide time stamping. [74]

In IP networks, packet losses occur as the network becomes congested. The Transmission Control Protocol (TCP) measures packet loss and controls the flow of packets from the source to relieve congestion in real time. In TCP/IP, if a packet is lost, it is retransmitted; however, in most real-time applications, retransmission of a packet is worse than not receiving a packet, due to the time-sensitive nature of the information—if the receiving station must request that a packet be re-transmitted, the delay will be too large, and large gaps and breaks in the conversation will occur. [74]

The main VoIP call-control protocols include the following [74, 77, 78]:

- H.323 is part of a broad family of standards developed by ITU. It describes how audio, video, and data communications take place among terminals, network equipment, and services on IP networks. Because it was originally developed for multimedia applications, H.323 does burden VoIP systems with unnecessary overhead, but its wide use makes it a common choice for interoperability among VoIP equipment. The standard describes four major functions of networked communications:
    - LAN client terminals that enable two-way communication.
    - Gateways designed for real-time, two-way communication between H.323 terminals on a network and other ITU terminals residing on a switched-based network or on another H.323 gateway.
    - Gatekeepers—Within a given zone, gatekeepers are the nexus for calls, providing services to endpoints.
    - Multipoint control units (MCUs) functioning as endpoints for three or more terminals and gateways, enabling multipoint conference communication.
- Simple Gateway Control Protocol (SGCP) was developed starting in 1998 to reduce the cost of endpoints (gateways) by having the intelligent call-control data processing procedures occur in a centralized platform (or gateway controller).
- Internet Protocol Device Control (IPDC) is similar to SGCP but has many other mechanisms for operations, administration, management, and provisioning (OAM&P).

[16] The ITU-T recommends a one-way delay of no more than 150 ms.

- Media Gateway Control Protocol (MGCP) is basically SGCP with a few additions for OAM&P. Created by the IETF, MGCP is a proposed standard to convert audio signals on the PSTN to data packets that traverse the Internet. The protocol is based on an architecture to move call-control intelligence away from the gateway for processing by external call-control or call agents. MGCP allows media gateways to communicate.
- Megaco/H.248 is a new protocol born of a joint effort between the ITU and the IETF. Functionally, the proposed standard enables a control of media gateways. Megaco/H.248 is designed to succeed MGCP, adding peer-to-peer interoperability and ensuring a way to control IP telephone devices operating in a master/slave manner. The standard breaks the H.323 gateway function into separate subcomponents. It also determines the protocols employed by each communication component.
- Session Initiation Protocol (SIP) is a media-based protocol that enables end devices (endpoints or gateways) to be more intelligent, to accommodate enhanced services at the call-control layer. This IETF standard addresses the call setup and teardown, error handling, and interprocess signaling that are functions of every point-to-point connection. It also changes and terminates multimedia sessions, including conferences, Internet telephony, distance learning, and other applications. SIP enables VoIP gateways, client endpoints, PBXs, and other systems to communicate over packet networks from an equipment perspective. Compared with H.323, SIP is a simpler protocol with less overhead.

The voice coding techniques used to generate VoIP packets have been standardized by the ITU Telecommunications Standardization Sector (ITU-T) in its G-series recommendations. Example coder/decoder (codec) standards include [79]

- G.711: 64 Kbps PCM voice coding compatible with conventional PBX or PSTN voice transmissions.
- G.729: 8 Kbps compressed digital voice using code-excited linear prediction (CELP).

The quality of digital voice using G.729 codecs diminishes with repeated coding and decoding.

5.3.2 Wired and Wireless IP-PBX

While VoIP can be used by "Internet phones" connected directly to the Internet, the most common application is in the implementation of "local premises" or "private branch exchange" (PBX) telephone services for large and small businesses. The traditional (wired) office telephone system architecture features telephone handsets connected by twisted wire pairs to a central PBX box containing [80]

- line cards which convert traffic from the handsets into the internal format needed for switching;
- trunk cards which interface to the public switched telephone network (PSTN) via analog or digital trunk lines;
- a switching fabric for making connections between line cards for premises calls, or between line and trunk cards for off-premises calls; and

- a computer control system that manages call setup and provides advanced features.

Note how much of this system involves proprietary (vendor-specific) specifications and hardware. In an IP-PBX system, propriety equipment is or can be replaced by standard office LAN networking plus a network management application to exercise call control and a gateway device to interface with the PSTN.

Prior to the current trend toward VoIP, wireless PBXs (not to be confused with wireless local loops) have been implemented as versions of conventional PBX architectures, but with proprietary cordless phones. The mobility provided by the wireless implementation has been a very useful and popular feature, and the concept of the same cordless phone being capable of being used in different physical locations is one of the features of the personal communication services (PCS) concept. This technology initiative has merged with advanced cellular communications efforts such as 3G. A wireless version of the IP-PBX architecture takes a different direction by requiring phones that are wireless terminals in a LAN.

5.3.3 Voice Over WLAN

Voice over WLAN (VoWLAN) is a natural extension of VoIP. Yet VoWLAN presents its own unique QoS (quality of service) challenges relating to fluctuating wireless throughput and phone users roaming among APs (access points). For that reason, most of the current local wireless voice system solutions offered by vendors tend to have some propriety features in hardware and in software. [81]

VoWLAN systems can be configured to work in one of two basic ways [81]. One approach is to utilize the WLAN infrastructure as simply the means to access the wired LAN on the business premises. Calls then are placed on the PSTN through a conventional VoIP gateway—one that may already be in use to deliver VoIP over the wired network. This approach facilitates a mix of wired and wireless IP phones in the organization and allows all regular PBX functions that are available on workers' wired desk phones to be available on the VoWLAN phones.

The second basic approach to configuring a VoWLAN system is to route calls outside the premises over the Internet instead of the PSTN, although a PSTN gateway will still be needed to place calls to other organizations. Traveling members of the company could use their wireless IP phone, or Internet phone software on their PDAs or laptops, to place "free" calls from any WLAN hotspot, routing the call entirely over the Internet. However, the control over call quality that is ensured using the PSTN is not available using this approach. [81]

At the heart of a typical WLAN IP phone unit is the digital signal processor (DSP), which is responsible for the VoIP processing functions. It is used for low-bit-rate codecs, such as G.729 and G.723, as well as for echo cancellation and tone generation. In the future DSP processing power also will support wide-band codecs, such as WB-AMR, which promise users better voice quality. A CPU is used for control and signaling, as well as services such as call-hold, mute, call-transfer and conferencing. A wireless LAN module offers support for the various versions of 802.11, including a, b and g, and quality of service via wireless multimedia extensions and 802.11e. [82]

The next logical step in WLAN IP phones is a dual-mode wireless LAN/cellular phone offering both mobile and VoIP technology on 802.11 networks. Dual-mode phones allow users

the flexibility of accessing the company network while in the office and using the cellular network outside, all with a single number. Consumer use of WLAN IP phones is expected to rise when broadband is available to the wireless home. Prototypes of such phones are being tested in connection with trials of mesh networks for public safety and government systems.

6. References and bibliography

In this section, we list the numbered references that are cited in the report and appendix. Also, a bibliography of additional articles and books are given that are relevant to the topic of this report, but are not cited.

6.1 Cited References

[1] ——, "Interoperability Continuum," SAFECOM graphic. Available online at http://www.safecomprogram.gov/SAFECOM/library/interoperabilitybasics/1229_interoperabilitycontinuum.htm

[2] ——, TIA web pages on Project 25 at http://www.tiaonline.org/standards/project_25/

[3] G. Hobar, "First Responders and Interoperability," presentation at SUPERCOMM 2003. Available online at http://www.tiaonline.org/standards/project_25/Hobar_F1.pdf

[4] ——, TIA/EIA Telecommunications Systems Bulletin TSB102-A, APCO Project 25 System and Standards Definition, November 1995.

[5] ——, TIA Project MESA web page at http://www.tiaonline.org/standards/mesa/

[6] ——. "Statement of Requirements for Public Safety Wireless Communications and Interoperability," SAFECOM, Version 1.0, 10 March 2004. Available online at http://www.safecomprogram.gov/files/PSCI_Statement_of_Requirements_v1_0.pdf

[7] ——, "Summit on Interoperable Communications for Public Safety," 26-27 June 2003. Web pages of ITS at http://pssummit.its.bldrdoc.gov/

[8] ——, "The State of Public Safety Communications," SAFECOM presentation at International Symposium on Advanced Radio Technologies, 2 March 2004. Available online at http://www.its.bldrdoc.gov/meetings/art/art04/slides04/cot_t/tutorial_c_slides.pdf

[9] ——, Project MESA "Service Specification Group Services and Applications, Statement of Requirements." Available online at http://www.projectmesa.org/ftp/Specifications/MESA_70.001_v3.1.1_SoR.doc

[10] Project MESA description for work item DTR/MESA-SYS0070012v311. Available online at http://webapp.etsi.org/WorkProgram/Report_WorkItem.asp?WKI_ID=20334

[11] T. Coty, "SAFECOM Program Review," ISART 2005 presentation, March 2005. Available online at http://www.its.bldrdoc.gov/isart/art05/slides05/cot_t/tutorial_b_slides.pdf

[12] ——, IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements: Part 15.1: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Wireless Personal Area Networks (WPANs), 2002 (IEEE 802.15.1 standard).

[13] J. Kardach, "Bluetooth Architecture Overview," Intel Technology Journal, 2nd quarter 2000. Available online at http://www.intel.com/technology/itj/archive/2000.htm

[14] ——, Bluetooth SIG web pages at http://www.bluetooth.com/

[15] R. Spaker, "Bluetooth Basics," *Embedded Systems Programming*, 2001.

[16] ——, IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems—LAN/MAN Specific Requirements, Part 15.3: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for High Rate Wireless Personal Area Networks (WPANs), 2003 (IEEE 802.15.3 standard).

[17] J. P. K. Gilb, *Wireless Multimedia: Guide to the IEEE 802.15.3 Standard*. New York: IEEE Press, 2004.

[18] C. Brabenac, "Intel CFA SG3a Response – Wireless Peripherals," IEEE 802.15 WPAN Working Group document 02/139, 8 March 2002. Available online at http://grouper.ieee.org/groups/802/15/pub/2002/Mar02/02139r0P802-15_SG3a-Intel-CFA-Response-Wireless-Peripherals.ppt

[19] L. E. Miller, "Why UWB?" NIST Wireless Communication Technologies Group report to DARPA, April 2003. Available online at http://www.antd.nist.gov/wctg/manet/NIST_UWB_Report_April03.pdf

[20] M. Welborn, "XtremeSpectrum CFP Document," IEEE 802.15.3a document 03/154r3, July 2003.

[21] A. Batra, "Multi-band OFDM Physical Layer Proposal for IEEE Task Group 3a," IEEE 802.15.3a document 03/268r2, November 2003.

[22] P. Gorday, J. Gutierrez, and P. Jamieson, "IEEE 802.15.4 Overview," IEEE 802.15 Wireless Personal Area Networks Working Group document 01/509, 12 November 2001. Available online at http://grouper.ieee.org/groups/802/15/pub/2001/Nov01/01509r0P802-15_TG4-Overview.ppt

[23] J. A. Gutierrez, E. H. Callaway, and R. L. Barrett, *Low-Rate Wireless Personal Area Networks*. New York: IEEE Press, 2004.

[24] J. Adams, "Designing With 802.15.4 and Zigbee," presentation and Industrial Wireless Applications Summit, 9 March 2004.

[25] ——, Supplement to IEEE Standard for Information Technology – Telecommunications and Information Exchange between systems – Local and metropolitan networks – Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: (1) [original 802.11 specification] 1997; (2) Higher-Speed Physical Layer Extension in the 2.4 GHz Band, 1999 (IEEE 802.11b specification); (3) High-Speed Physical Layer Extension in the 5 GHz Band, 1999 (IEEE 802.11a specification).

[26] ——, "IEEE 802.11b Wireless LANs: Wireless Freedom at Ethernet Speeds," 3Com Corporation white paper 50307201, 2000.

[27] G. Fleishman, "Back to the Future: New Wi-Fi Bridges Uses 1999 Standard," O'Reilly Network, 28 August 2003. Available online at http://www.oreillynet.com/pub/a/wireless/2003/08/28/wireless_bridging.html

[28] N. Moayeri and M. W. Subbarao, "Background," NIST Wireless Communication Technologies Group web page for wireless ad hoc network project, at http://www.antd.nist.gov/wahn_home.shtml

[29] M. W. Subbarao, "Mobile Ad Hoc Networks for Emergency Preparedness Telecommunications—Dynamic Power-Conscious Routing Concepts," NIST Wireless Communication Technologies Group interim report to National Communication System, April 2000. Available online at http://w3.antd.nist.gov/wctg/manet/subbarao-ncs.pdf

[30] C. Elliott and B. Heile, "Self-Organizing, Self-Healing Wireless Networks," *Proc. IEEE 2000 International Conf. On Personal Wireless Communications*, pp. 355-362.

[31] R. Merritt, "DARPA Looks Past Ethernet, IP Nets," *EE Times*, 26 April 2004. Available online at http://www.eet.com/showArticle.jhtml?articleID=19200111

[32] L. M. Feeney, "A Taxonomy for Routing Protocols in Mobile Ad Hoc Networks," Swedish Institute of Computer Science Technical Report T99/07, October 1999. Available online at ftp://ftp.sics.se/pub/SICS-reports/Reports/SICS-T--99-07--SE.ps.Z

[33] X. Hong, K. Xu, and M. Gerla, "Scalable Routing Protocols for Mobile Ad Hoc Networks," *IEEE Network*, July/August 2002, pp. 11-21.

[34] S. Xu and T. Saadawi, "Does the IEEE 802.11 MAC Protocol Work Well in Multihop Wireless Ad Hoc Networks?" *IEEE Communications Magazine*, June 2001, pp. 130-137.

[35] J. L. Sobrinho and A. S. Krishnakumar, "Quality-of-service in ad hoc carrier sense multiple access wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 17, pp. 1353-1368 (August 1999).

[36] ——, "700 MHz Frequency Database System," NPSTC web page for the CAPRAD system, at http://caprad.nlectc.du.edu/login/home

[37] K. M. H. Wallman, letter to FCC containing recommendations for 700 MHz interoperability standards, 25 July 2003. Available online at http://wireless.fcc.gov/publicsafety/ncc/ncc_releases/2finalrecommendations.pdf

[38] Motorola, Inc., "Scalable Adaptive Modulation (SAM) Physical Layer Technology," presentation, 2001. Available online at http://www.motorola.com/greenhouse/standards/motorola_sam_overview.pdf

[39] D. Bishop, "Mobile Data Ideas Grow in 'Greenhouse Project'," *MRT Online*, 29 August 2001. Available online at http://mrtmag.com/news/radio_mobile_data_ideas/index.html

[40] ——, Motorola, Inc. web pages on the Greenhouse Project at http://www.motorola.com/greenhouse/

[41] S. Devine, "Update to Governing Board: NPSTC Spectrum Management Committee," 15 June 2004. Available online at http://www.npstc.org/meetings/Devine%20Spectrum%20Mgmt%20Committee%20Update%20061504.pdf

[42] ——, FCC Second Report and Order and Further Notice of Proposed Rulemaking in the matter of the 4.9 GHz Band Transferred from Federal Use, 27 February 2002. Available online at http://wireless.fcc.gov/releases/fcc0247.pdf

[43] ——, FCC Ruling in the Matter of the Transfer of 4.9 GHz from Government Use, 2 May 2003. Available online at http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-03-99A1.pdf

[44] L. Luna, "4.9 GHz Networks More Secure, But a Long Way Off," *Mobile Radio Technology*, 1 January 2004. Available online at http://mrtmag.com/mag/radio_ghz_networks_secure/index.html

[43] D. Jackson, "Emissions Mask for 4.9 GHz Under Fire," First Responder Communications supplement to *MRT*, August 2004.

[45] S. O'Hara, "Regulatory Activities to Follow," presentation to NPSTC, June 2004. Available online at http://www.npstc.org/meetings/OHara%20Regulatory%20Activities%20Update%20061404.pdf

[46] ——, IEEE Standard for Local and Metropolitan Networks – Part 16: Air Interface for Fixed Broadband Wireless Access Systems, October 2004.

[47] ——, WiMAX Forum web pages at http://www.wimaxforum.org/

[48] R. Marks, et al., "The 802.16 WirelessMAN MAC: It's Done But What Is It?" IEEE 802.16 document 01/58r1, 12 November 2001. Available online at http://ieee802.org/16/docs/01/80216-01_58r1.pdf

[49] H. Sari and G. Karam, "Orthogonal Frequency-Division Multiple Access and Its Application to CATV Networks," *European Transactions on Telecommunications*, vol. 9, pp. 507-514 (November/December 1998). Available online at http://dev.aei.it/ETT.pdf

[50] ——, "WiMAX's Technology for LOS and NLOS Environments," WiMAX Forum white paper, 2004. Available online at http://www.wimaxforum.org/news/downloads/WiMAXNLOSgeneral-versionaug04.pdf

[51] ——, IEEE 802.20 Mobile Broadband Wireless Access (MBWA) web pages at http://www.ieee802.org/20/

[52] ——, "MBWA and 802.16e: Two Markets – Two Projects," IEEE 802.16 document 02/16. Available online at http://www.ieee802.org/16/mobile/docs/80216sgm-02_16.pdf

[53] ——, "IEEE 802.16e Standard: What Will It Mean for Fixed Wireless Applications?" SR Telecom white paper 033-100669-001, 2005. Available online at http://www.srtelecom.com/imports/pdf/en/white-paper/16e-Standard-Jan2005.pdf

[54] M. Thelander, "WiMAX: Opportunities and Challenges in a Wireless World," CDMA Development Group white paper, July 2005. Available online at http://www.cdg.org/resources/white_papers/files/WiMAX%20July%202005.pdf

[55] D. Beyer, "Wireless Mesh Networks for Residential Broadband," presentation at 2002 National Wireless Engineering Conference, 4 November 2002. Available online at http://www.iec.org/events/2002/natlwireless_nov/featured/tf2_beyer.pdf

[56] J. G. Jun and M. L. Sichitiu, "The Nominal Capacity of Wireless Mesh Networks," *IEEE Wireless Communications*, October 2003, pp. 8-14.

[57] ——, "Mesh Networks Winning Converts," *Network World Fusion*, 3 May 2004. Available online at http://www.nwfusion.com/news/2004/0503mesh.html

[58] ——, "Ad-hoc Peer-to-Peer Routing Technology," MeshNetworks web page, 2004.

[59] ——, U.S. Army Signal Center and Fort Gordon, Near Term Data Radio web page at http://www.gordon.army.mil/tsmtr/ntdr.htm

[60] L. Kleinrock and J. Silvester, "Optimum Transmission Radii for Packet Radio Networks or Why Six is a Magic Number," *Proc. IEEE 1978 Natl. Telecomm. Conf.*, pp. 4.3.1-4.3.5.

[61] R. E. Kahn, "The Organization of Computer Resources into a Packet Radio Network," *IEEE Trans. On Communications*, vol. COM-25, pp. 169-178 (January 1977).

[62] N. Abramson, "The ALOHA System—Another Alternative for Computer Communications," *Proc. 1970 Fall Joint Computer Conf.*

[63] A. S. Tanenbaum, *Computer Networks*. Englewood Cliffs, NJ: Prentice-Hall, 1981.

[64] L. Roberts, "Extensions of Packet Communication Technology to a Hand Held Personal Terminal," *Proc. SJCC*, 1972.

[65] L. Kleinrock and F. A. Tobagi, "Packet Switching in Radio Channels: Part I—Carrier Sense Multiple-Access Modes and Their Throughput-Delay Characteristics," *IEEE Trans. On Communications*, vol. COM-23, pp. 1400-1416 (December 1975).

[66] F. A. Tobagi and L. Kleinrock, "Packet Switching in Radio Channels: Part II—The Hidden Terminal Problem in Carrier Sense Multiple-Access and the Busy-Tone Solution," *IEEE Trans. On Communications*, vol. COM-23, pp. 1417-1433 (December 1975).

[67] L. Kleinrock and J. Silvester, "Spatial Reuse in Multihop Packet Radio Networks," *Proceedings of the IEEE*, vol. 75, pp. 156-167 (January 1987).

[68] L. E. Miller, "Distributional Properties of Inhibited Random Positions of Mobile Radio Terminals," presentation at 36th Conf. on Information Sciences and Systems (CISS 2002), Princeton, March 2002 Available online at http://www.antd.nist.gov/pubs/lemciss02.ppt

[69] J. J. Hahn and D. M. Stolle, "Packet Radio Network Routing Algorithms: A Survey," *IEEE Communications*, November 1984, pp. 41-47.

[70] ——, Final Report of the Public Safety Wireless Advisory Committee to the Federal Communications Commission and the National Telecommunications And Information Administration, 11 September 1996. Available online at http://pswac.ntia.doc.gov/pubsafe/publications/PSWAC_AL.PDF

[71] F. A. Westall, "Review of speech technologies for telecommunications" *Electronics & Communication Engineering Journal*, vol. 9, issue 5, Oct. 1997 pp.197-207.

[72] C. Redding, N. DeMinco, and J. Lindner, "Voice Quality Assessment of Vocoders in Tandem Configuration," NTIA report 01-386, April 2001. Available online at http://www.its.bldrdoc.gov/pub/ntia-rpt/01-386/

[73] ——, "DVSI Vocoder Independent Evaluation Results," web page of Digital Voice Systems, Inc. at http://www.dvsinc.com/papers/eval_results.htm

[74] J. Davidson and J. Peters, "Overview of the PSTN and Comparison to Voice Over IP," Chapter 1 of *Voice Over IP Fundamentals*. Cisco Press, 2001. Available online at http://searchnetworking.techtarget.com/searchNetworking/Content_Types/White_Paper/VoIPFundamentals.PDF

[75] T. A. Hall, "Objective Speech Quality Measures for Internet Telephony," *Proceedings of the SPIE*, vol. 4522: *Voice Over IP (VoIP) Technology*. Available online at http://www.antd.nist.gov/pubs/speechq.pdf

[76] D. G. Morrison, "Power-Over-Ethernet Chips Give LANs a New Outlet," *Electronic Design*, 13 October 2003, pp. 51-62. Available online at http://www.elecdesign.com/Articles/Index.cfm?ArticleID=5844

[77] ——, "VoIP Family," web page of Protocols.com at http://www.protocols.com/pbook/VoIPFamily.htm

[78] Texas Instruments, "Voice Over Internet Protocol," Chapter 28 in *Online! TheBook: Because the Internet Does Not Come With a Manual*, J. C. Dvorak, C. Pirillo, and W. Taylor, New York: Prentice-Hall PTR, 2004. Chapter available online at http://www.ti.com/corp/docs/landing/speakvoip/677_696.pdf

[79] Cisco Corp., "Voice-over-IP Overview." Available online at http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/1700/1750/1750voip/intro.htm

[80] K. Wanichkorn and M. Sirbu, "The Economics of Premises Internet Technology," in McKnight, L. et al, eds, *Internet Telephony*, (MIT Press: Cambridge 2001). Available online at http://www.ini.cmu.edu/ITC/PremisesIPTelephony.pdf

[81] N. Gohring, "Voice Over WLAN—Ready or Not?" *InfoWorld*, 12 September 2003. Available online at http://www.infoworld.com/article/03/09/12/36FEvowlan_1.html

[82] I. S. Ghai and A. Johnston, "Wireless LAN IP Phones—Simplifying Communications?" *New Telephony*, 29 April 2004. Available online at http://www.newtelephony.com/newsvoices/121708ED-5FD6-42D0-92BA-37EAA9822BAA.html?wts=20050714082418&hc=1&req=ghai

6.2 Additional Bibliography

——, "Bringing Wireless Data Applications to the Patrol Car," PSWN Program Information Brief 0401, February 2001. Available online at http://www.cslj.net/library/dk_files/Law%20Enforcement/L%20E%20Technology/L%20E%20Telecom%20Technology/Wireless/2001%20PSWN%20Wireless%20Apps%20to%20Car%20PIB%200401.doc

——, "Can We Talk? Public Safety and the Interoperability Challenge," *NIJ Journal*, April 2000. Available online at http://www.agileprogram.org/documents/jr000243d.pdf

——, Cisco Systems *Public Safety Wireless Solutions Guide*.

——, "Coos Bay Police Department Uses Wireless Technology to Beat Catch 22," *APCO Bulletin*, December 1998.

——, "Digital Public Safety Radio Communications: The Wireless Industry to the Rescue," TIA Industry Update Session at SUPERCOMM 2003. Available online at http://www.tiaonline.org/standards/project_25/at_supercomm.cfm

——, "FCC Issues Narrowband Mandate Below 512 MHz," APCO news release, February 2003. Available online at http://www.apcointl.org/frequency/narrowbandmandate.htm

——, *National Incident Management System*, US Department of Homeland Security, 1 March 2004. Available online at http://www.dhs.gov/interweb/assetlibrary/NIMS-90-web.pdf

——, "An Overview of the SMR Service from the Perspective of Public Safety," PSWN Report, 2001. Available online at http://radioscanning.wox.org/Scanner/other_info/PDF_files/smr_serv_assmnt.pdf

——, "San Mateo County Beefs Up Security For Peterson Trial With New Wi-Fi Video Surveillance of Public Areas In And Around The Courthouse," Sony press release, 26 May 2004. Available online at http://news.sel.sony.com/pressrelease/4860

——, "Syracuse Police Dept. Extends its WLAN to Field Officers," Mobile Village (online), 8 September 2003. Available online at http://www.mobilevillage.com/news/2003.09.23/syracuse.htm

——, "When They Can't Talk, Lives Are Lost," NTFI brochure. Available online at http://www.agileprogram.org/ntfi/ntfi_brochure.pdf

——, "Why Wireless for Public Safety?" page on Wireless Ready website. Available online at http://www.wirelessready.org/safety.asp

——, "Why Can't We Talk: Working Together to Bridge the Communications Gap to Save Lives," NTFI publication. Available online at http://www.agileprogram.org/ntfi/ntfi_guide.pdf

——, "Wi-Fi with a PS Twist," *APCO Bulletin* article. Available online at http://www.apco911.org/frequency/4-9GHz/WiFiPS.htm

——, "Wireless Bridges and Repeaters," Practically Networked web pages at http://www.practicallynetworked.com/networking/wireless_bridge.htm

J. Ashley, "Trunking the EDACS Way," *Mobile Radio Technology*, 1 February 1999. Available online at http://mrtmag.com/mag/radio_trunking_edacs/index.html

J. Barthold, "Small-town Police Force Thinks Big," *MRT*, 1 April 2004, p.6. Available online at http://mrtmag.com/mag/radio_smalltown_police_force/index.html

N. Borisov, I. Goldberg, and D. Wagner, "Intercepting Mobile Communications: The Insecurity of 802.11," *Proc. Mobicom 2003*. Available online at http://www.isaac.cs.berkeley.edu/isaac/mobicom.pdf

S. Bruzzese, "Public Safety Tilts Toward Wireless," M-Business Daily (online), 9 August 2001.

B. Charney, "Helping cops keep tabs on wireless data," CNET News.com, 17 March 2003. Available online at http://zdnet.com.com/2100-1103-992832.html

J. P. Craiger, "802.11, 802.1X, and Wireless Security," 23 June 2002. Available online at http://www.sans.org/rr/papers/index.php?id=171

A. Davidson and L. Marturano, "The Impact of Digital Technologies on Future Land Mobile Spectrum Requirements," *Proc. IEEE Vehicular Technology Conf.*, May 1993, pp. 560-563.

P. DeBeasi, "Wireless LAN Security Protocols," Wireless Design and Development, April 2004, pp. 42-48. Available online at http://www.wirelessdesignmag.com/ShowPR.aspx?PUBCODE=055&ACCT=0000100&ISSUE=0404&RELTYPE=PR&Cat=0&SubCat=0&ProdCode=00000&PRODLETT=F&SearchText=security%20protocols

T. Dees, "Information and Communications Technology for Public Safety," IQ Service report to International City/Council Management Association, January 2000. Available online at http://www.timdees.com/articles/icma.htm

M. DiCristofano, "Wireless Use Helps to Meet Public Safety Budget Limits," *MRT*, 1 August 1997. Available online at http://mrtmag.com/mag/radio_wireless_helps_meet/index.html

M. Douglas, "Incident Management in Many Forms," *MRT*, July 2004. Available online at http://mrtmag.com/mag/radio_incident_management_forms/index.html

M. Douglas, "Pocket Policing," *MRT*, 1 May2003. Available online at http://mrtmag.com/mag/radio_pocket_policing/index.html

J. Duffy, "Wireless Data Service Options Explode," Network World Fusion, 19 April 2004. Available online at http://www.nwfusion.com/news/2004/0419specialfocus.html

G. R. Emery, "DHS to start wireless pilot projects," *Washington Technology*, 20 February 2004. Available online at http://www.washingtontechnology.com/news/1_1/daily_news/22843-1.html

D. Frank, "Montana Puts Vehicle Data Online," FCW.com, 26 February 2004. Available online at http://www.fcw.com/geb/articles/2004/0223/web-montana-02-25-04.asp

M. Greczyn, "NCC Panels Look to Wideband Data for Public Safety at 700 MHz," *Communications Daily*, November 2001. Available at http://www.fcca.info/Newletter/NCCPANELS.htm

C. Greenman, "A Well-Equipped Patrol Officer: Gun, Flashlight, Computer," *New York Times*, 21 January 1999. Available online at http://www.nytimes.com/library/tech/99/01/circuits/articles/21howw.html

D. Grip, "A Group Effort: Public Safety Consortiums Help Small-Town Agencies Deploy Wireless Technology," *APCO Bulletin*, August 2000.

R. Hixson, "IP and E9-1-1," *Mission Critical Communications*, June 2004, pp. 78-79.

IBM, "TCP/IP Tutorial and Technical Overview," August 2001. Available online at http://www.redbooks.ibm.com/redbooks/pdfs/gg243376.pdf

D. Jackson, "Public-Safety Communications Has Increased Prospects, Tougher Choices," *MRT*, 29 March 2004. Available online at http://mrtmag.com/news/radio_publicsafety_communications_increased/index.html

D. Jackson, "Panel: 4.9GHz Band Promising, Challenging," *MRT*, 30 March 2004. Available online at http://mrtmag.com/news/radio_panel_ghz_band/index.html

J. Jackson, "Colorado City Switches Protocols to Keep Vehicles on Track," *Government Computer News*, 2 August 2004. Available online at http://www.gcn.com/23_21/news/26800-1.html

J. Jackson, "NASA Tests WiFi Mesh Networks," *Government Computer News*, 22 March 2004. Available online at http://www.gcn.com/23_6/tech-report/25272-1.html

A. Joch, "Digital Radios: A New Calling Plan," *Federal Computer Week*, 21 June 2004. Available online at http://www.fcw.com/supplements/homeland/2004/sup2/hom-project-06-21-04.asp

J. Jones, "Reach for the Sky: South Dakota Proves That Big Dreams Can Lead to Big Successes" [about SD radio system], *Federal Computer Week*, 30 August 2004.

C. Kain, "Commercial Mobile Radio Services for Public Sector Agencies," Mitretek Systems, Inc., prepared for the USDOT ITS Joint Program Office, October 2003. Available online at http://www.itspublicsafety.net/docs/MitretekFinalCMRS_PublicSafety.pdf

D. A. Keckler, "The Future of Fire Mobile Data," *MRT*, 1 August, 1999. Available online at http://mrtmag.com/mag/radio_future_fire_mobile/index.html

W. Leland, "TR-8: Mobile and Personal Private Radio Standards," presentation at SUPERCOMM 2003. Available online at http://www.tiaonline.org/standards/project_25/LelandR1.pdf

J. R. McMillian Jr., *The Primer of Public Safety Telecommunication Systems*, 3rd ed. Daytona Beach, FL: APCO International, 2000.

K. Middaugh, "No More Towers," *Government Technology*, May 2004. Available online at http://www.govtech.net/magazine/story.php?id=90189

B. O'Hara and A. Petrick, *802.11 Handbook: A Designer's Companion*. New York: IEEE Press, 1999.

L. Krishnamurthy, S. Conner, M. Yarvis, J. Chhabra, C. Ellison, C. Brabenac, and E. Tsui, "Meeting the Demands of the Digital Home with High-Speed Multi-Hop Wireless Networks," *Intel Technology Journal*, November 2002. Available online at http://www.intel.com/technology/itj/archive/2002.htm

C. E. Perkins, *Ad Hoc Networking*. New York: Addison-Wesley, 2001.

D. Pfohl, R. Schwartz, and A. Wilson, "The Importance of the Project 25 Common Air Interface and Its Potential Impact on Interoperability," *APCO Bulletin*, May 1999.

R. Prasad and L. Munoz, *WLANs and WPANs: Towards 4G Wireless*. Boston: Artech House, 2003.

I. Ramirez and R. Coffey, "Enhancing Law Enforcement Efficiency with Mobile Data: The Wireless Interoperability Advantage," *9-1-1 Magazine*, July/August 2002. Available online at http://www.9-1-1magazine.com/ArticleDetail.asp?ArticleID=102

M. Rauf and F. Lefebvre, "Keeping the Wireless Connection Running," E-9-1-1 Magazine, January/ February 2003. Available online at http://www.novaroam.com/downloads/nr_911article.pdf

N. Reid and R. Seide, *802.11 (Wi-Fi) Networking Handbook*. New York: McGraw-Hill/Osbourne, 2003.

J. Rendon, "Notebooks and Wi-Fi Keep Colorado Cops on the Beat," SearchMobile.com, 8 March 2004. Available online at http://searchmobilecomputing.techtarget.com/originalContent/0,289142,sid40_gci953936,00.html?track=NL-315&ad=477866&Offer=t3.8

E. M. Royer and C.-K. Toh, "A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks," *IEEE Personal Communications*, April 1999, pp. 46-55.

S. Ring, "Mobile Digital Communication for Public Safety, Law Enforcement, and Non-Tactical Military," ETSI document. Available online at http://www.etsi.org/T_news/Documents/TETRA-TETRA2-MESA.pdf

D. Robb, "The Cellular Option: Cellular PC Cards Give You Another Choice for Wireless Data Transmission," *Government Computer News*, 8 September 2003. Available online at http://www.gcn.com/22_26/mobile-wireless/23396-1.html

S. Rupley, "Wireless: Mesh Networks," *PC Magazine*, 1 July 2003. Available online at http://www.pcmag.com/article2/0%2C4149%2C1130864%2C00.asp

D. Sarkar, "Mobile Units Aid Small City in Big Way," *Federal Computer Week*, 20 February 2004. Available online at http://www.fcw.com/geb/articles/2003/0217/web-pratt-02-20-03.asp

D. Sarkar, "Oregon City Builds Safety Net," *Federal Computer Week*, 22 March 2004. Available online at http://www.fcw.com/fcw/articles/2004/0322/tec-oregon-03-22-04.asp

D. Siegle and R. Murphy, "Interoperability Report Card: PSWN Grades the Progress," *MRT*, 1 June 2001. Available online at http://mrtmag.com/mag/radio_interoperability_report_card/index.html

B. Smith, "Police Drive Into Next Gen," *Wireless Week*, 1 August 2003. Available online at http://www.wirelessweek.com/article/CA314158

A. S. Spanias, "Tutorial Review of Speech Coding," University of Arizona, 1994. Available online at http://www.eas.asu.edu/~spanias/papers/review.ps

D. Storey, "Digital Two-Way Radios Address Interoperability Dilemma," *Government Procurement*, June 2004. Available online at http://www.relm.com/Sections/PressReleases/Articles/Dave_Interop_Article.pdf

S. Stroh, "802.11s – IEEE Standard for Wireless Mesh Networks," Corante Tech News, 22 June 2004. Available online at http://www.corante.com/bwia/archives/004499.html

E. Sutherland, "Wireless As a Tool for Improving Public Safety," *Wireless IM* (online). Available online at http://www.instantmessagingplanet.com/wireless/article.php/1468001

M. J. Taylor, R. C. Epper, and T. K. Tolman, "Wireless Communication and Interoperability Among State and Local Law Enforcement Agencies," National Institute of Justice *Research in Brief*, January 1998. Available online at http://www.ncjrs.org/pdffiles1/168945.pdf

A. Theil and H. Stambaugh, "Improving Firefighter Communications," FEMA report tr-099. Available online at http://www.usfa.fema.gov/downloads/pdf/publications/tr-099.pdf

S. Tucker, J. Oblak, and A. Wilson, "The Technologies, Applications and Attributes of a Project 25 Trunking System," *APCO Bulletin*, May 1999.

M. D. Wade, "Cellular and Trunking in Disaster Areas," *APCO Bulletin*, May 1998.