
Telecommunications and Information Technology Planning

The telecommunications and information technology planning function represents the highest-level system or network perspective of the Institute. This work can be characterized generally as planning and analyzing existing, new, and proposed telecommunications and information technology systems, especially networks, for the purpose of improving efficiency and enhancing the technical performance and reliability of those systems. In many cases, ITS performs this work for both wireline and wireless applications. This portion of the ITS technical program encompasses work that is frequently referred to in industry as “systems engineering.”

All phases of strategic and tactical planning are conducted under this work area; problem solving and actual implementation engineering also are done. ITS engineers identify or derive users' functional requirements and translate them into technical specifications. Telecommunication system designs, network services, and access technologies are analyzed, as well as information technologies (including Internet and Internet-related schemes). Associated issues, such as network management and control and network protection and privacy, also are addressed. Integration of individual services and technologies is a common task in many projects, along with the application of new and emerging technologies to existing applications.

Areas of Emphasis

Broadband Wireless Standards The Institute develops new radio propagation algorithms and methods that improve spectrum usage of wireless systems. Technical standards are prepared that support U.S. interests in third generation (3G) broadband wireless systems. The project is funded by NTIA.

Emergency Telecommunications Service (ETS) A two-prong approach addresses ETS. The Institute develops and verifies ETS Recommendations for ITU-T Study Group 9. Computer simulation, laboratory studies, security analyses, and traffic engineering are used to support Critical Infrastructure Protection initiatives related to broadband cable television networks. A second project provides ETS expertise relating to Network Survivability for Technical Subcommittee T1A1. These two projects are funded by the National Communications System (NCS).

Networking Technology The Institute characterizes and analyzes the fundamental aspects of networks, and network interoperability, “from the bottom, up.” Networking technology methodologies and tools are developed to address discovery, monitoring/measurement, simulation, management, and security/protection issues. This project is funded by NTIA.

Justice/Public Safety/Homeland Security Telecommunications Interoperability Standards The Institute conducts a technical program aimed at facilitating effective telecommunications interoperability and information-sharing among dissimilar wireless and information technology systems of local, state, and Federal government agencies. The main thrust is the development of interoperability standards. The NCS, Public Safety Wireless Network (PSWN), and NIST’s Office of Law Enforcement Standards (a Technology Center of the National Institute of Justice) fund the program.

Railroad Telecommunication Planning The Institute performs radio infrastructure system planning in support of a high-speed rail pilot program, and demonstrates newly designed digital land mobile radio technology and infrastructure, compliant with TIA-102 standards, along the Pacific Northwest rail corridor. The Federal Railroad Administration funds this project.

Voice Over Packet The Institute develops technical contributions related to Internet Protocol (IP) telephony gateways and their supporting infrastructure for the TIA TR41 Standards Formulating Group. Work is conducted to ensure that user interfaces being developed for IP telephony satisfy national security and emergency preparedness communications requirements. This project is funded by NCS.

Broadband Wireless Standards

Outputs

- Preparation of technical standards and documents for the ITU-R that support the U.S. interest in broadband wireless systems.
- Development of new radio propagation algorithms or methods that improve spectrum usage of wireless systems.

The wireless industry made projections on how they expected the rollout of technology to progress, as shown in Tables 1 and 2. Both the number of users and the types of services (beyond just voice communications) are increasing, with more emphasis on Internet-type uses. These new services require greater bandwidths (and more radio spectrum).

In order to predict wireless signal coverage more accurately, ITS and other research organizations are developing and evaluating propagation models that are more responsive to the needs of cellular and private land mobile radio service providers. A common model used by system planners is the ITS Irregular Terrain Model (ITM), also known as the Longley-Rice model. While a good predictor in irregular terrain, it does not have the capability to utilize land-use, land-cover databases to predict losses due to man-made objects. Another common model is the Okumura-Hata model. It is a good predictor in urban and suburban environments, but it does not handle irregular terrain nor does it handle changing environments, e.g., from urban to suburban to rural.

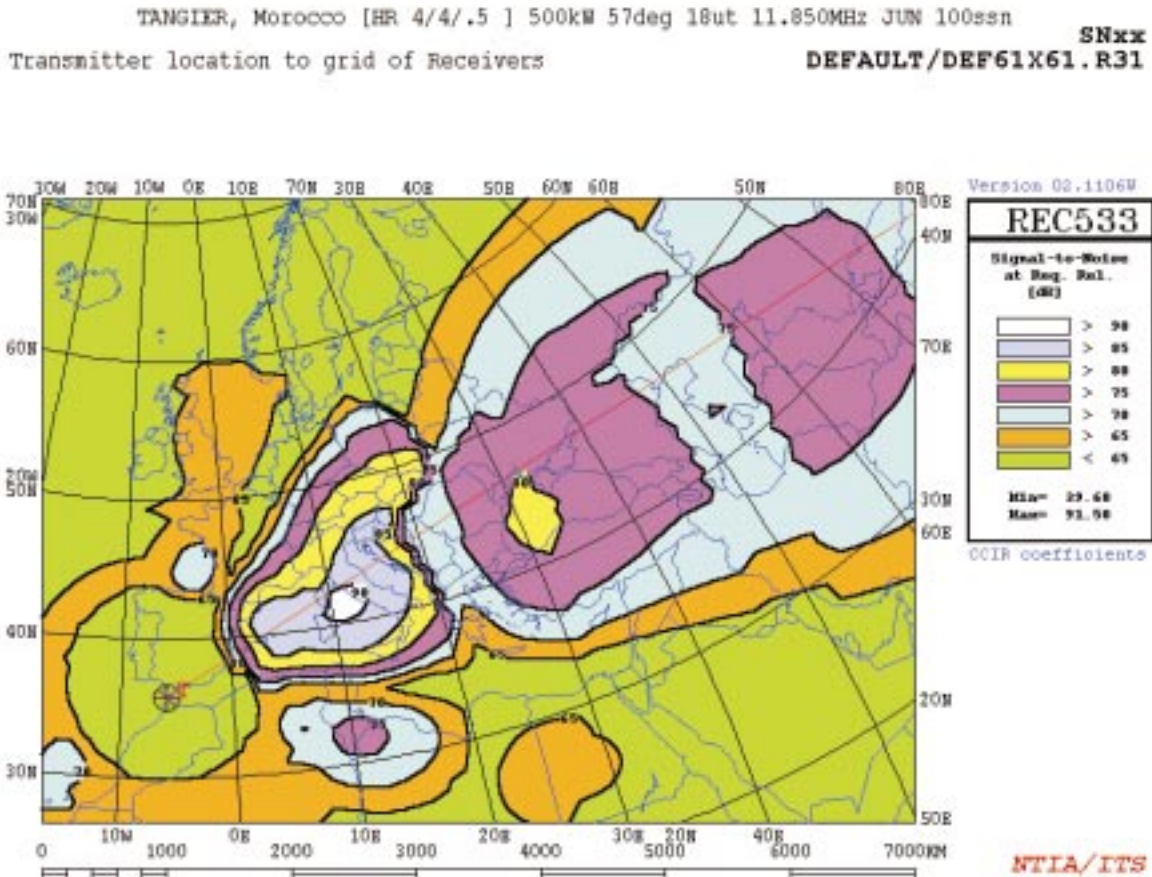
Table 1. Growth in Subscriber Penetration for Wireless Services

	1998	2000	2002
Wireless service subscriber penetration in the U.S.	24%	35%	42%

Table 2. Growth in Subscribers (North America) by Wireless Service Technology

Technology	1998	2000	2002
Advanced mobile phone service (AMPS), analog	53 million	42 million	24 million
Time Division Multiple Access (TDMA), digital	10 million	27 million	44 million
Code Division Multiple Access (CDMA), digital	8 million	27 million	52 million
GSM, a TDMA standard developed in Europe with worldwide use	4 million	10 million	20 million

Radio propagation predictions made using land-use, land-cover databases should estimate signal losses due to objects on a propagation path more accurately than predictions calculated without knowledge of the obstacles. The improved predictions allow service providers to better evaluate locations for base stations and to predict where additional base stations might be needed to fill in areas of inadequate signal coverage. ITS is evaluating the incorporation of land-use, land-cover databases into the ITM propagation prediction model to provide better estimations of signal loss. Although better databases are now available for land-use, land-cover descriptions, the signal loss associated with the various land-use, land-cover categories is not well known, nor is the loss versus frequency well known. ITS is also evaluating the means of incorporating terrain obstacle information into the Okumura-Hata model, to make it more responsive to the changing environment.



Example output from the High Frequency propagation software developed by the ITU for international frequency coordination and maintained by ITS.

Another effort supported by ITS is the international development of propagation prediction models that can be used by spectrum managers and system planners of both land mobile, terrestrial broadcast, maritime mobile and certain applicable fixed (e.g., point-to-multipoint) services. As these services are becoming more similar in terms of RF equipment characteristics, it is appropriate to use the same propagation model for planning and coordination of these services.

The ITU-R Study Group 3 on Radio Propagation has recently developed and adopted such a model, ITU-R Recommendation P.1546, which blends features that the services had previously used independently of one another, thereby clarifying and unifying planning and coordination activities across the services.

ITS is a member of the ITU Study Group 3 Working Party 3L. This study group deals with Ionospheric Propagation. ITS is responsible for maintaining the

High Frequency (HF) (3-30 MHz) propagation software developed by the ITU for international frequency coordination. The ITU web site:

<http://www.itu.int/ITU-R/software/study-groups/rsg3/databanks/ionosph/index.html>

links to an ITS web site with the following reference: HF sky-wave propagation (Rec. P.533) (available from the website of the U.S. Department of Commerce NTIA/ITS)

<http://elbert.its.blrdoc.gov/hf.html>

An example of the type of output the software can produce is shown in the above figure.

For more information, contact:

Paul M. McKenna
 (303) 497-3474
 e-mail pmckenna@its.blrdoc.gov

Emergency Telecommunications Service (ETS)

Outputs

- Technical contributions to ANSI Working Group T1A1.2.
- Technical contributions to ITU-T Study Group 9.
- Letter report to NCS on NS/EP Communications over Metropolitan Area Networks (MANs).

In the aftermath of the recent terrorist attacks, the Federal Government has refocused its interests on priority treatment of emergency communications. While the Government Emergency Telecommunications Service (GETS) has served emergency workers well for many years, it is limited to the Public Switched Telephone Network (PSTN) within the United States. ETS is envisioned as a GETS-like service that will be available internationally and will encompass virtually all wireless and wireline communications networks. Types of traffic to be carried include voice, video, database access, text messaging, email, file transfer protocol (FTP), and web-based services.

The ETS effort at ITS encompasses several projects including Packet-Switched Networks and Network Survivability. For these projects, computer simulation, laboratory studies, security analyses, and traffic engineering are used to support Critical Infrastructure Protection (CIP) initiatives. These two projects are funded by the National Communications System (NCS). This work supports NCS in its mission to protect the national security telecommunications infrastructure, and to ensure the responsiveness and survivability of essential telecommunications during a crisis.

For the first project, Packet-Switched Networks, the Institute develops and verifies ETS Recommendations for International Telecommunication Union — Telecommunication Standardization Sector (ITU-T) Study Group 9 (integrated broadband cable and television networks). The major goal of this project is to ensure that future ETS mechanisms will interoperate over broadband cable television networks. Additionally, the project is working to facilitate the evolution of GETS over the IP/Cablecom network.

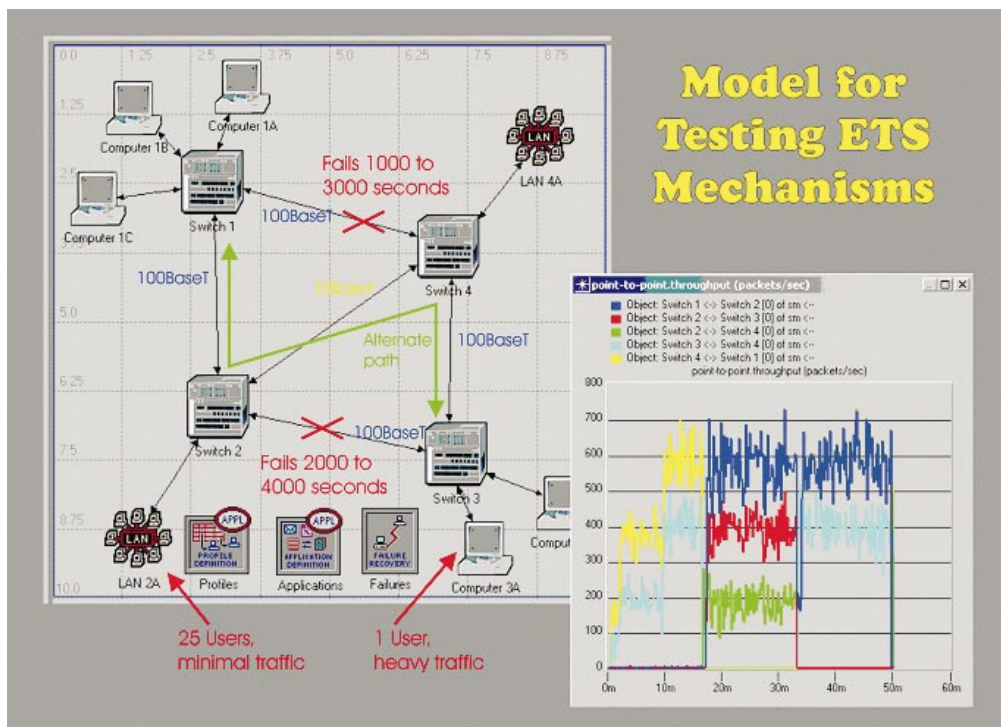


Figure 1. Simulation for testing ETS protocols.

The second project, Network Survivability and Restoral, provides ETS expertise relating to Network Survivability for ANSI-accredited Technical Subcommittee T1A1 (performance, reliability, and signal processing). Within this project, ITS serves as co-editor of a new T1 Technical Report: "Overview of Standards in Support of Emergency Telecommunications Service (ETS)."

Traditional analysis methods are not adequate to predict the effects of large service outages in the current and future network environments. Therefore, ITS is using network modeling and simulation tools to address the needs of Working Group T1A1.2 (network survivability performance), national security and emergency preparedness (NS/EP), and the nation. While modeling and simulation are powerful tools for the assessment of threats and mitigation techniques, the simulations need to be well grounded in the physical measurement of important parameters. One of the goals of the project has been to produce baseline models for reference network architectures that can be used both in standards development and in future network research by ITS and others. Figure 1 shows one such reference model developed to test proposed ETS mechanisms.

The standardization work in ITU-T Study Group 9 is focused on the IP-Cablecom family of Recommendations. These Recommendations define the protocols and signaling to be used on broadband cable television networks to support telephony, multimedia, and Internet access. The IP-Cablecom Recommendations have just recently been standardized and are currently in production worldwide. One goal of this project is to identify where additions or changes might be needed to support ETS. This effort also involves work with the Internet Engineering Task Force (IETF) since many of the underlying protocols used in IP-Cablecom (as well as some of the ETS mechanisms) are under development in the IETF.

Another important activity underway at ITS is a series of tests utilizing GETS over IP-Cablecom networks. The evolution of GETS from a PSTN-only

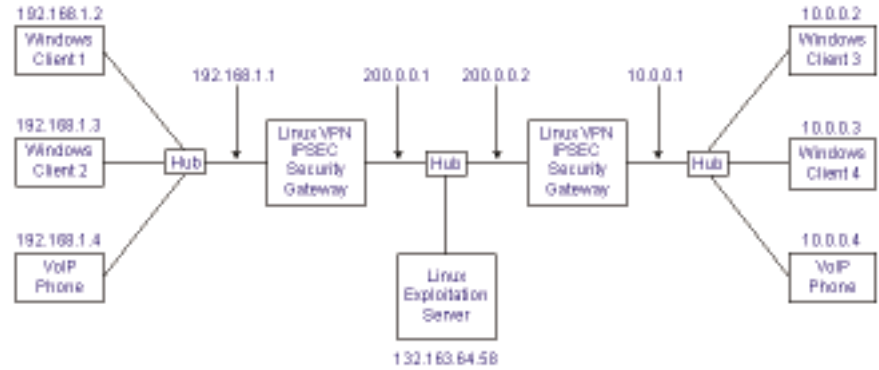


Figure 2. Laboratory setup for testing security and ETS protocols.

service to one that will interoperate over the wireless, IP-Cablecom, and Next Generation Networks (NGN) is one of the goals of NCS.

Determining the security needs of ETS in IP-Cablecom networks is another goal of this effort. Figure 2 shows a laboratory setup to test proposed ETS mechanisms over virtual private networks (VPNs) and through firewalls. The setup is currently used to test the performance of Videoconferencing and Voice over IP (Internet protocol) over SIP (session initiation protocol). Proposed ETS mechanisms will be coded and tested over the same network to determine if they are viable from a Quality of Service (QoS) standpoint.

During FY 2002, ITS presented numerous technical and editorial contributions to T1A1.2 and ITU-T Study Group 9. Some of these were included in the new T1 ETS Technical Report mentioned above. In FY 2003, ITS will continue to participate in the development and standardization of ETS in T1A1, the IETF, and ITU-T Study Group 9. The projects will address technologies in the Next Generation Network and interactions with the IP-Cablecom networks. This work on ETS must of necessity be conducted with the help of representatives from network providers, cable television equipment manufacturers, and NCS. Additionally, the work in FY 2003 will focus on survivability and security in the NGN ETS as well as GETS in the IP-Cablecom networks.

For more information, contact:
Arthur A. Webster
(303) 497-3567
e-mail awebster@its.bldrdoc.gov

Networking Technology

Outputs

- Definition of structured planning process for telecommunication and information technology networks.
- Suggestions for types of tools to assist in network design and administration.
- Handbook for telecommunication and information technology network planning (will be available in 2003 on ITS programs webpage <http://www.its.blrdoc.gov/home/projects.html>)

The Institute has a long history of performing telecommunication planning and assessment studies for other organizations, but the complexity of today's telecommunication and information technology (hereafter "telecom and IT") requirements, and the technology available to satisfy those requirements, create demands for enhanced sophistication in the methodologies and tools used to perform these studies. The Networking Technology project has defined a structured planning process for such studies, examined many tools that can be used in conducting such studies, and identified those tools most likely to provide the greatest benefits. Last year's Technical Progress Report showed the use of these tools in discovering the topology of a network, the loads on segments of the network, and simulating the migration of the topology and loads to a new topology. Efforts in FY 2002 focused on two of the most important aspects of network design and administration: Network Management and Network Security.

Network Management

Network management can be defined as the ability to control the activities required in managing a network from a single point on that network. This point can be at several locations, thus allowing management staff to quickly perform functions from many locations on the network. Good network management can help any organization achieve its goals of availability and performance. Poor network management will not only *not* help an organization reach its goals but may also contribute to the problems which prevent the achievement of those goals.

A logical approach to network management is to break down the management function into its component parts and ensure that each part can be performed efficiently using tools and trained personnel. The International Organization for Standardization (ISO) defines five types of network management functions:

1. *Fault management* refers to detecting, isolating, reporting, diagnosing, and correcting faults on the network. A variety of tools exist to meet these fault management requirements, including monitoring tools, polling tools, alarming tools, report generation tools, and protocol analyzers.

2. *Performance management* is the ability to measure network behavior and effectiveness. This includes protocol performance, application performance, response times across the network, and the reachability of network components. Tools that monitor and measure performance include network analyzers, RMON monitors, and tools that utilize built-in capabilities of many network devices.

3. *Security management* protects network components and interconnections from unauthorized access, unauthorized use, and other damage. This function maintains audit logs, records logins and logouts, and records attempts by users to change their level of authorization. Tools for security management include firewall, intrusion detection systems, perimeter routers, and virtual private networks.

4. *Configuration management* allows the manager to control the configuration of the network and manage the network assets in a logical, systematic, and organized manner. Configuration tools allow the network manager to keep track of operating system configurations and local configurations of devices as well as changes to devices.

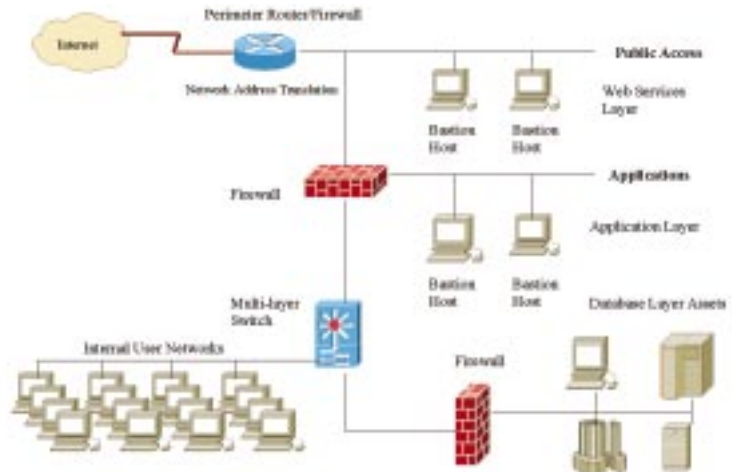
5. *Accounting management* allows the administrators to collect statistical information on network usage and load on a component, user, or group level. This facilitates usage-based billing of network customers and can be an aid in detecting abuse of network resources. Another practical reason for accounting management is to track network load levels so that future capacity planning can be undertaken with more confidence in the predicted levels of growth.

Network Security

Every organization has a mission. In this “information age,” as individuals and organizations use information technology systems to process information and further their mission, security management is critical in protecting each organization’s assets, and thus its mission, from damage. In recent years and especially since September 11, 2001, security has become a major concern of network designers and administrators. The cost of lost data and time, as well as the potential damage to an organization’s image and stability, requires that the network administrator or designer place a very high emphasis on network security. To ensure that a comprehensive, detailed, relevant, and effective security management system is developed, it is important to start by creating a procedure for its creation that covers all aspects of security planning and implementation. This procedure will provide a baseline that organizations can reference when the network security is regularly re-evaluated. A logical approach to security management follows the steps listed below:

1. Define clear principles and practices for securing the IT system.
2. Define an IT security framework for implementing the security management system.
3. Identify overall security requirements.
4. Identify existing assets to be secured.
5. Identify the security risks and consequences of failure of these assets.
6. Analyze security trade-offs and costs for required security level for these assets.
7. Develop a security plan.
8. Develop a security policy.
9. Document procedures and controls for implementing the security plan and policy.
10. Implement the policy through adequate training and resource allocation.
11. Integrate the policy with the organization’s overall security management system.
12. Review and reassess the security management system periodically or as the network or security requirements change.

Security considerations have a major impact on network topology and the experience of the network designer is critical in this effort. When designing a network, the designer must consider trade-offs of



A layered secure network topology.

cost with the level of performance and security provided. Since this is the case, there are many ways that a network solution and design can be implemented. A basic secure network design assumes that the organization’s assets will be broken down into three layers of access and sensitivity. This configuration is shown in the figure. The three layers are:

Layer 1 - Public access layer. This layer allows public access to those services and data that the security plan permits. The security policy and risk assessment dictate how that access is achieved, who is permitted access, and how the assets are managed. Data and services at this layer have the lowest sensitivity and the lowest level of security.

Layer 2 - Application layer. This layer supports the services in layer 1 without allowing direct access to the services by the requesting user. This protects the application assets from unauthorized access or modification. Services in layer 1 are permitted to access the applications in layer 2 via a bastion host and firewall. Data and services at this layer have moderate sensitivity and a moderate level of security.

Layer 3 - Database layer. This layer supports database requirements of applications operating in layer 2. These assets are considered very sensitive and must be given the greatest level of security. Direct access to this layer by users is prohibited or at least severely restricted.

For more information, contact:

Robert O. DeBolt
(303) 497-5324
e-mail rdebolt@its.bldrdoc.gov

Justice/Public Safety/Homeland Security Telecommunications Interoperability Standards

Outputs

- Voice and data encryption standards for Project 25 digital radios.
- XML data element dictionary.
- TIA Telecommunications Systems Bulletins for testing Project 25 radios.

ITS is conducting a technical program aimed at providing effective interoperability and information sharing among dissimilar wireless telecommunications and information technology (IT) systems within the justice/public safety/homeland security community. The key to the program is the identification and/or development of interoperability standards to allow local, State, and Federal agencies to exchange information, without requiring substantial changes to internal systems or procedures. The ITS program is sponsored by two Federal agencies and one Federal program: National Communications System (NCS), National Institute of Justice (NIJ) (through its Advanced Generation of Interoperability for Law Enforcement (AGILE) Program), and Public Safety Wireless Network (PSWN) program (jointly sponsored by the Departments of Justice and Treasury). The tripartite ITS program is summarized below.

National Communications System Support

The Institute is assisting NCS's Technology and Programs Division in developing a comprehensive series of interoperability standards for digital land mobile radio (LMR) for public safety applications. Next generation LMR standards are being developed by the Federal Government, in conjunction with industry and local and State governments, within a group called Association of Public-Safety Communications Officials/National Association of State Telecommunications Directors/Federal (APCO/NASTD/FED) Project 25. This project consists of three phases. Phase 1, which has been completed, included the development of a comprehensive set of standards for 12.5-kHz digital LMRs. Phase 2, in progress, is developing a set of interoperability standards for narrowband (6.25 kHz) digital LMRs;

standards defining TDMA radios with an equivalent 6.25 kHz/channel efficiency are also being developed. ITS efforts have mainly supported Phase 2. Phase 3 (also referred to as "Project 34") has also begun, and is focused on the development of standards for wideband mobile data applications.

NCS, Federal law enforcement agencies, and the National Security Agency, with assistance from ITS, are participating in the development of these standards, and are taking the lead in the development of related Information System Security (INFOSEC) standards. An ITS representative chairs the Project 25 Encryption Task Group and works closely with its members in developing Project 25 INFOSEC standards. ITS participates on the Telecommunications Industry Association (TIA) TR 8 Encryption Committee to ensure that TIA standards meet Government requirements. ITS also participates in other TIA TR 8 Committees and Project 25 task groups as necessary to ensure that the total suite of Project 25 LMR interoperability standards meets Federal requirements, and to continually assess Project 25's impact on Federal agencies. An ITS engineer represents NCS on the Project 25 Steering Committee. To date ITS has contributed to the development of standards for the encryption of voice and data sent over the Project 25 Common Air Interface, a standardized key fill interface for Project 25 equipment, and for the over-the-air-rekeying of Project 25 radios.

NIJ's AGILE Program Support

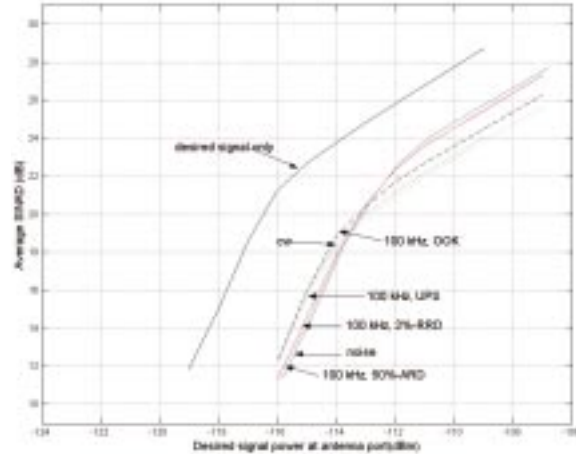
As the Department of Justice's science and technology arm for assisting State and local agencies, NIJ addresses wireless telecommunications and IT interoperability issues. In particular, NIJ's AGILE program has facilitated the efforts of the practitioners in the justice/public safety/homeland security community to coordinate and share information. The long-term thrust involves assistance toward standardization of interoperability approaches. The AGILE program continues to provide specialized technical support to help users define their requirements, and then assists the practitioners to address and satisfy those functional needs. This is done by recommending standards that most aptly specify the context of a nationwide information sharing framework. The

second thrust of the AGILE Program provides technical investigation and laboratory evaluation of interim interoperability products, services, and techniques to allow agencies to work better now while longer term standardization efforts are developed. ITS performs the AGILE standardization and evaluation activities under the auspices of NIST's Office of Law Enforcement Standards (OLES), one of NIJ's technology centers.

During FY 2002, considerable progress was made in the AGILE Program regarding standardization of IT applications by teaming with the Global Justice Information Network Advisory Committee (Global). Global, as the Group of Groups, represents all practitioners in the Justice community (e.g., law enforcement, courts, corrections, prosecutors, defense, etc.; see <http://it.ojp.gov/global/index.html>). ITS worked with Global's Infrastructure/Standards Working Group to develop a standard approach for XML (eXtensible Markup Language) implementation, along with a data element dictionary that can provide common "words" for a common "language" to be used by the justice/public safety/homeland security community. In addition, ITS helped design and develop a web-based Justice Standards Registry for Information Sharing to allow practitioners to list and discuss their interoperability standards, standards projects, and concepts that may benefit others (see <http://it.ojp.gov/jsr/public/index.jsp>). An Interoperability Research Laboratory (p. 69) was established at ITS to accommodate testing and evaluation of interim interoperability products and proposed ideas.

Public Safety Wireless Network (PSWN) Support

ITS provides technical support to the TIA TR8 (Project 25) Committee to develop Project 25 Standard documents. Specifically, ITS has had the responsibility for developing procedures to test the interoperability of radio systems engaged in conventional voice, over-the-air re-keying of encryption, trunking, and data applications. The procedures are TIA Telecommunications Systems Bulletins (TSB) and guide TSB users on the set-up and conduct of functional tests to assure that two Project 25 devices are interoperable. In addition, through AGILE and PSWN, ITS provides support to the ISSI Task Group of TR8 in the development of the Inter-RF Sub-System Interface (ISSI) standard for Project 25. This standard is needed to link the radio networks of cooperating jurisdictions and to link local radio systems to a nationwide network, such as proposed by the Treasury/Justice Integrated Wireless Network.



Susceptibility of an analog land mobile radio to various ultrawideband devices.

ITS developed and conducted tests to measure the performance of Public Safety radio receivers with ultrawideband interference. The information resulting from the tests is important as practitioners are expected to use land mobile radios in their vehicles or carry handheld radios while they also make use of ultra wide band equipment in support of their missions. Thus, the levels that cause interference to the radios are important to the community. The graph above shows the susceptibility of an analog land mobile radio to various, typical ultrawideband devices. The desired signal is an analog FM signal at the antenna port of the radio. The interference signals are the signals that cause the desired signal reception to degrade by 3 dB.

Recent Publications

TIA/EIA TSB-102.CABB Project 25 Interoperability Test Procedures: Over-The-Air-Rekeying (OTAR), Feb. 14, 2002.

Draft version TIA/EIA TSB-102.CABx Project 25 Interoperability Test Procedures Voice Operation in Trunked Systems, Sep. 2, 2002.

Presentation to Congressional, Federal, and State/local representatives: Invited paper on Emerging Technology Solutions at the NTIA/PSWN Public Safety Communications Interoperability Summit.

For more information, contact:
 Val J. Pietrasiewicz
 (303) 497-5132
 e-mail valp@its.bldrdoc.gov

Railroad Telecommunication Planning

Outputs

- Demonstration of advanced radio technology and infrastructure along the Midwest passenger rail corridor, in support of the Federal Railroad Administration's high-speed rail pilot program.

The incremental train control system (ITCS) is a radio-based signaling system designed by G.E. Transportation Systems whose purpose is to facilitate high-speed passenger rail transportation along the Midwest rail corridor between Chicago and Detroit. The current ITCS demonstration system "overlays" on an existing legacy track signaling system of approximately 70 miles in length. It provides enforcement of signal indications and civil speed limits, as well as advanced start of highway crossing gates, in a high-speed rail environment. The overlay design supplies system redundancy, so that in the event of data communication failure between ITCS components, passenger safety is not compromised, as train control will revert to the legacy signaling infrastructure.

At higher track speeds, the status of highway crossings and signal lights must be made known to the locomotive at further distances from the crossing and signals, as compared to traditional track speeds, and highway crossing gates must be activated when the locomotive is further distant from each crossing. Monitoring and notification over these greater distances is accomplished by radio frequency (RF) data links.

ITCS monitors the status of "wayside" devices (signal lights, highway crossing gates, etc.) via an RF data link, and relays these statuses to the locomotive via a second RF data link. A computer onboard the locomotive evaluates the status information from these devices in conjunction with local sensory information (speed, GPS location, etc.) and other



Amtrak station at Niles, Michigan (image courtesy of G.E. Transportation Systems).

pertinent data (track profile, computed braking distances based on track profile, and so forth), and then determines permissible locomotive actions, so as to facilitate efficient high-speed rail travel.

During the course of this pilot program, operational system anomalies, believed attributable to radio propagation, have been experienced on a

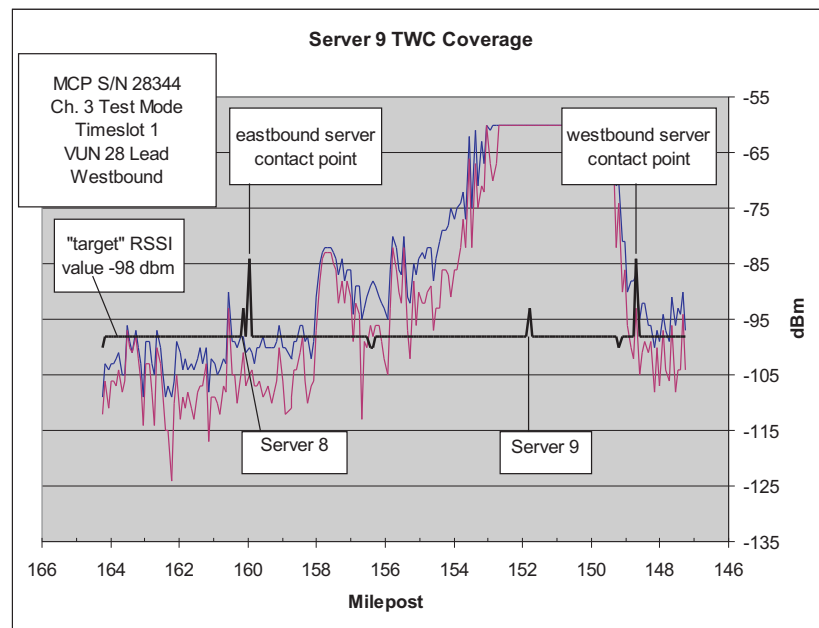


Figure 1. Measured signal strength – Server 9; Amtrak locomotive at track speeds.

number of occasions. While these anomalies have always resulted in restrictive “fail-safe” modes of operation, with ITCS functioning exactly as it should under these degraded conditions, these anomalies have resulted in sub-optimum transit time performance of passenger trains traversing the territory. Consequently, the Federal Railroad Administration (FRA) asked the Institute to provide technical representation to the ITCS program on their behalf.

Empirical evidence collected thus far suggests that log-normal shadowing phenomena is deleteriously affecting the propagation of the 900-MHz RF data link signals. Figure 1 shows typical receiver response curves (average and minimum received power levels) as measured by G.E. Transportation Systems.

What this plot shows is that on eastbound moves (although this measurement was actually taken traveling westbound), the signal strength would not have been sufficient to allow the locomotive’s ITCS equipment to have acquired the signal from wayside server 9 by the time milepost marker MP 160 had been reached. Even though MP 160 is still in server 8 territory, having acquired server 9 by this time ensures that an RF data link is established and that advance gate crossing activations and other critical actions can be triggered just as soon as the locomotive would enter server 9 territory at MP 156.

Further investigations by the Institute determined representative areas of successful data communication. Figure 2 shows the locations of successfully received ITCS packets over a portion of the same track territory, indicated by the turquoise-colored dots on the (magenta-colored) tracks. It is to be noted that this data was collected in a single pass while driving along trackside in an ITCS-equipped Hy-Rail vehicle, at speeds of about 5 mph, as opposed to a number of data sets collected at typical (faster) locomotive speeds, as was done in Figure 1.

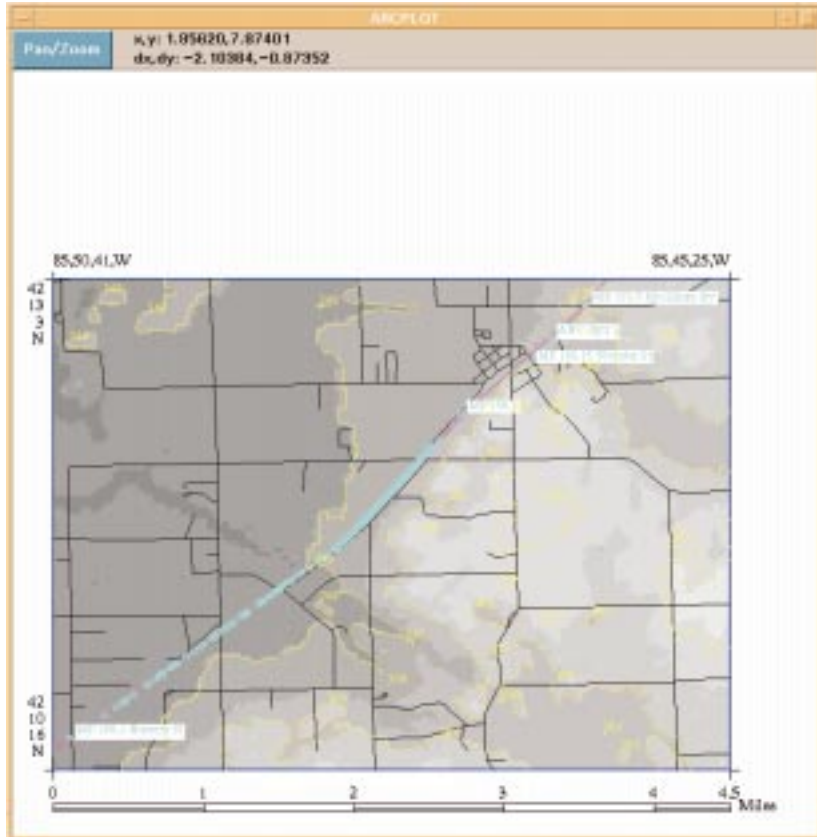


Figure 2. Successfully received ITCS data packets; Hy-Rail vehicle at 5 mph.

What is apparent is that near MP 160 (lower-left corner) and west, successful packet reception in this fringe area appears to be less reliable than further east, a region more centrally located to the track section. During this data collection activity, the Institute noted that the tree line was on the same order of height as the 900-MHz antennas, a very likely cause of the shadowing phenomena being experienced. The Institute is currently exploring whether apposite solutions could be as simple as raising the heights of wayside antennas, or whether an entirely new approach to system design and/or deployment of the underlying infrastructure may be more appropriate.

For more information, contact:
John M. Vanderau
(303) 497-3506
e-mail jv@its.bldrdoc.gov

Voice over IP

Outputs

- Report to IEEE conference regarding VoIP degradation over 802.11 networks under Bluetooth interference.
- Standards contributions (ITU, TR-41.1) detailing the behavior of Government Emergency Telecommunications System (GETS) calls over VoIP based systems.

Advances in quality of service (QOS) and greater market availability have resulted in increased utilization of Voice over IP (VoIP) on enterprise networks. VoIP technology offers substantial benefits including efficient resource utilization, a homogeneous network offering both voice and data, potential for other multimedia transmission (e.g. video), and lower data bandwidth requirements than traditional telephony.

As wireless local area networks (LANs) based upon IEEE 802.11b (Wi-Fi) technologies become more ubiquitous, attempts are being made to utilize VoIP over radio channels as well as the fixed location wired networks more traditionally associated with VoIP systems. However, interference problems within the wireless channel can substantially degrade the QOS of a VoIP system. This effect is of particular concern in Wi-Fi systems, which share the same spectral allocation as Bluetooth (IEEE 802.15) devices.

In order to evaluate some of the effects of radio interference on VoIP transmission over wireless channels, ITS has investigated the degradation of estimated mean opinion scores (MOS) in VoIP transmissions over Wi-Fi channels with nearby Bluetooth interferers. This experiment simulated the effects of multiple active Bluetooth piconets (small networks of devices connected in an ad hoc fashion using Bluetooth technology) operating in close proximity to VoIP-encoded Wi-Fi transmissions at various signal to noise ratios (SNR).

In this experiment, standardized Harvard phonetically balanced sentences were transmitted using an H.323-based VoIP system. The packet telephony devices used the G.723.1 codec at a bit rate of 5.3 Kbps. The information was carried over a Wi-Fi channel at 11 Mbps, where the transmitter and receiver were in close proximity to as many as four independent Bluetooth piconets that were sending large files using FTP. Forty sentences were transmitted during each experimental iteration, and the audio signal transmitted was compared with the audio signal received. Estimates of MOS were derived using the perceptual evaluation of speech quality (PESQ) algorithm (ITU-P.862) and packet loss was measured using a software-based protocol analyzer.

The experimental results were analyzed over multiple planes. The percentage of packets dropped versus the number of Bluetooth piconet interferers was investigated, as well as the estimated MOS compared to number of piconets. Both of these comparisons were made for three different SNR values. A third comparison, shown in Figure 1, indicates the degradation of MOS with increasing packet loss percentages. The target MOS for toll quality telephony (and VoIP systems) is 4, so these results indicate that

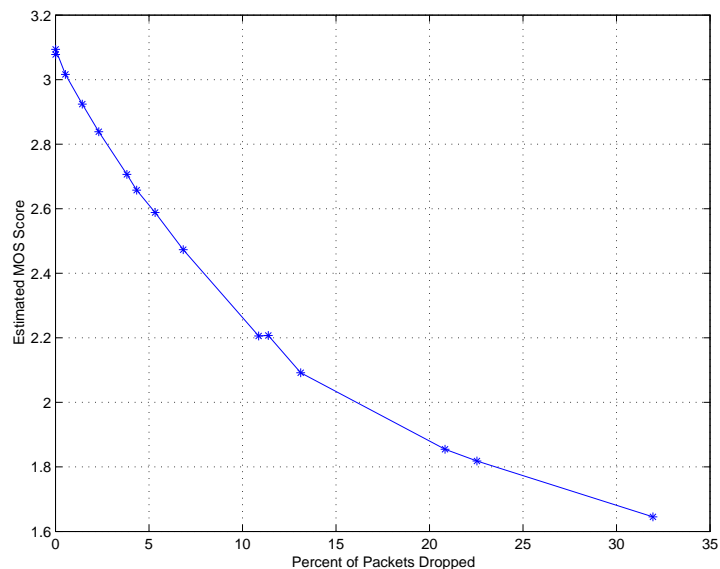


Figure 1. Mean opinion score (MOS) versus dropped packets in Wi-Fi transported VoIP.

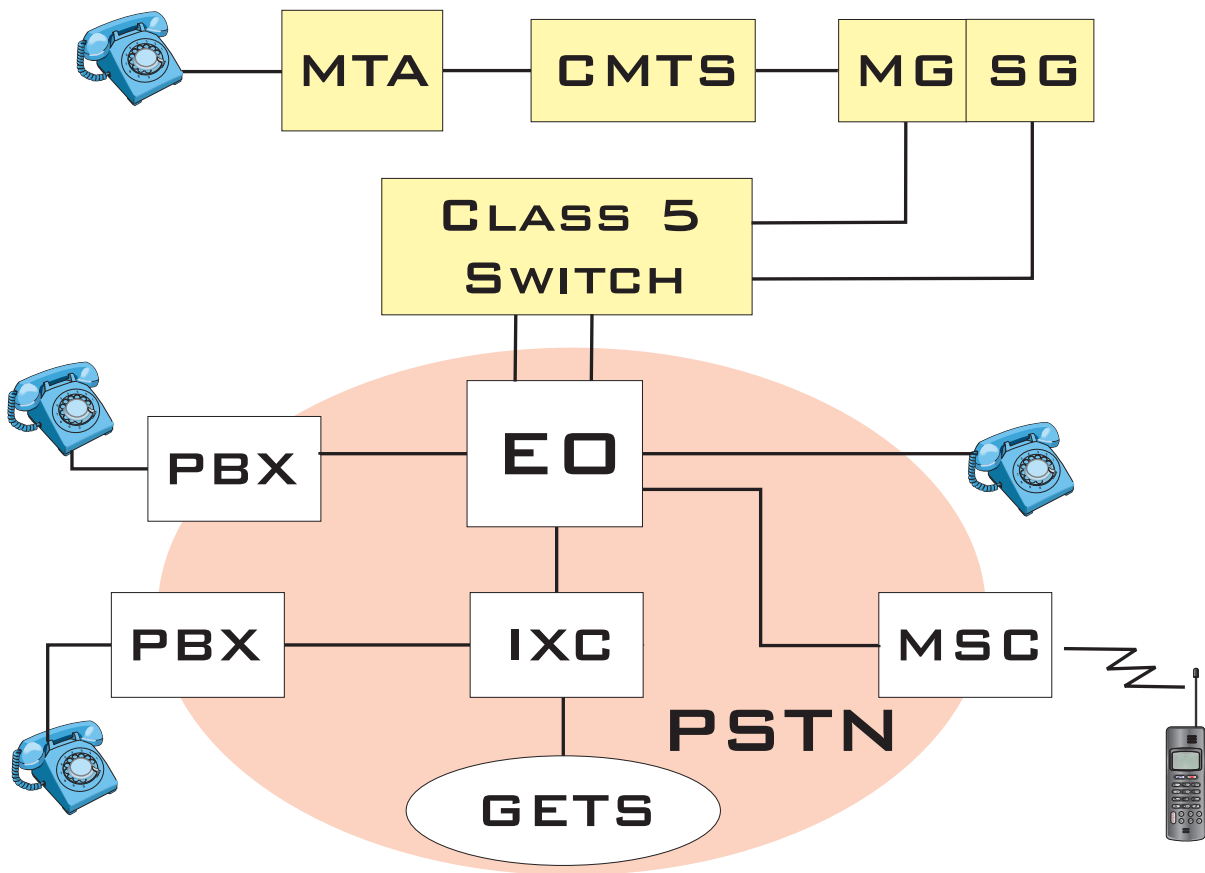


Figure 2. Test setup for GETS calling over VoIP-based media.

low percentages of packet loss due to radio interference can severely degrade the intelligibility of these systems.

Recognizing the growing availability of VoIP-based packet telephony, as well as a heightened awareness of government emergency communications, ITS has also embarked on a series of investigations regarding the capabilities of current VoIP signaling implementations for this process. During emergencies, the public switched telephone network (PSTN) may encounter congestion, precluding emergency calls from getting through. Even government emergency telecommunications service (GETS) calls, which enjoy enhanced priority, may be impossible to place using normal telephone connections. However, VoIP-based enterprise networks might be used to route calls around the congested area, through gateways into non-congested portions of the PSTN. In order to test the viability of using alternative VoIP-based media to make such calls, experimental

GETS call placements over existing alternative systems like the one diagrammed in Figure 2 are being made. Here, the enterprise network includes a cable modem system with a media terminal adaptor (MTA) and a cable modem termination system (CMTS) as well as media and signaling gateways (MG and SG). The calls may be terminated through a variety of equipment including local phone and private branch exchange (PBX) equipment as well as cellular telephones and long-distance PBX (e.g., through an interexchange carrier or IXC). This is an ongoing effort, in connection with other ITS projects studying the emergency telecommunications service (ETS).

For more information, contact:
 Dr. Robert B. Stafford
 (303) 497-7835
 e-mail stafford@its.bldrdoc.gov