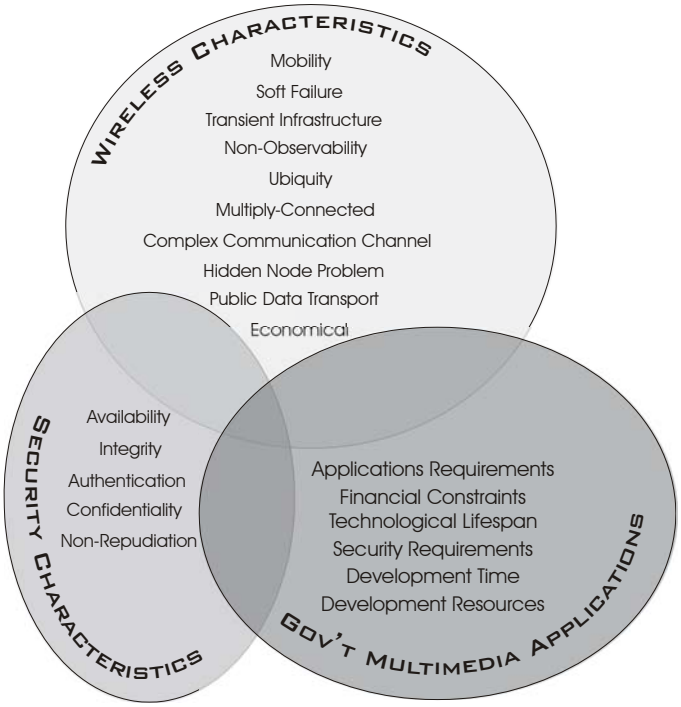
Wireless Networking Analysis and Forecasting

Institute for Telecommunication Sciences (ITS)

- **Forecasting of Future Wireless Technologies**
- **Usage Studies of Commercial Wireless Networks**
- **Secure Wireless Network analysis**

ITS produces analytical services that aid in the fielding of Federal communications products that rely on public wireless infrastructure. The studies that ITS has conducted are used to advise and inform Federal wireless users and designers. The work of the Institute can assist Federal wireless communications meeting financial and technical criteria. In addition, ITS has done extensive research for a variety of agencies including the maintenance and operation of secure Government communications. Often as part of a comprehensive report ITS includes reasoned opinions of the future of wireless technologies.



Intersection of Security, Wireless and Government Multimedia Requirements in Public Networks.

The Institute is actively investigating the kinds of wireless networks and services Federal users will be seeing in the future. These networks are being examined for suitability to interface to mobile government security services. In particular, common interfaces are being closely examined since they may aid in the rapid adoption of emerging wireless technology. ITS is attempting to identify the interfaces, both software and hardware, that will allow a broad range of government wireless communications services to be developed and deployed. Future wireless networks, such as IEEE 802.15 and 802.16 (WiMAX), which are on the verge of being fielded promise to make broadband services widely available. IEEE 802.15 will support data rates of up to 54 Mbps with a range of tens of meters. This technology will provide the capability to send real-time video over piconets in the unlicensed 2.4 GHz band.Piconets are also identified as wireless personal area networks (WPAN). IEEE 802.16 is designed for data rates of up to 155 Mbps in a point-to-multipoint metropolitan area network (MAN). A MAN facilitates the connection of multiple wireless LANs over a range of 50 km.

Wireless communication links are used to extend the wired networks to solve the first mile/last mile connectivity problem. The advantages of economy and flexibility are making wireless data links more attractive relative to fixed infrastructure. The inherent limitations of a fixed infrastructure restricts user mobility and is more expensive to upgrade. IEEE 802.11 (Wi-Fi) networks essentially extend the range of wired networks rather than operating as autonomous and/or independent networks. Wired networks are extended via wireless access points, where multiple wireless communications links connect to a central point. The nodes that make up a Wi-Fi network communicate through a wireless access point, rather than peer-to-peer. This topological similarity with wired networks does not exploit the advantages of wireless links, which possess the unique features of mobility and self association. Peer to peer communications, such as defined in the 802.11 standard and Bluetooth, take only partial advantage of the self association characteristic of wireless communications. Self associating wireless networks are known as ad hoc wireless networks. ITS is examining the use of ad hoc

wireless networks for use in Federal communications architectures. Research at the Institute is focusing on how to make these ad hoc wireless networks suitable and secure for Federal wireless users.

Other application requirements, such as mobility, affect the type of data service that can be provided to Federal users. If no mobility is required, optical or point-to-point radio frequency (RF) technology may be satisfactory. If a high degree of mobility is required, cellular technology may be the only solution. Security requirements may also dictate particular choices. As always financial considerations often are the predominate motivator for the Government to use public wireless networks. An additional financial motivator is the potential long-term stability of a technology. Finally, service development time and resources availability may color the type of wireless communication service that can be used.

Government communications services share common features with public services. Successful Government communications applications require levels of performance and quality of service that are no different from most private sector services. Some Federal requirements can fall outside the capabilities of the commercial market. Government data services can be elevated to the level necessary to preserve national security. For these crucial services, the requirements demanded from wireless service providers may be difficult to achieve using public networks. Secure application requirements may be so stringent that a proprietary network is necessary. The intersection of security and wireless characteristics shown in the Figure, represents commercial implementations of wireless security. This intersection is overlapped by Government multimedia applications requirements. Future wireless services will require that Federal users are familiar with the interplay between the intersections in the Figure to effectively meet the communications needs of the future. ITS provides the analysis necessary to understand all three areas.

While the constraints that wired infrastructure impose on wired network design are well known, wireless data transport constraints are less understood. Network centric designers often overlook unique characteristics of wireless that can lead to network functionality that is unavailable on wired infrastructure. On the other hand, the wireless communications environment has numerous constraints that call for very sophisticated and complex network designs. The difficulty in designing applications for wireless environments is the requirement that the designer be well versed in both networking and wireless disciplines. The strengths of wireless can bring a new dimension to the way applications and Federal users relate to data. Yet, the weakness of wireless, foremost being public data transport, can have catastrophic consequences - especially in networks where security is of importance. ITS draws on its' expertise in RF propagation and knowledge of networking to provide a comprehensive view.

Contact: Christopher Redding
303-497-3104
credding@its.bldrdoc.gov

Institute for Telecommunication Sciences
325 Broadway, Boulder, Colorado 80305
http://www.its.bldrdoc.gov, **303-497-5216**

The Institute for Telecommunication Sciences (ITS), located in Boulder, Colorado, is the research and engineering arm of the National Telecommunications and Information Administration (NTIA) of the U.S. Department of Commerce. ITS receives direct support from the Department of Commerce and is sponsored by other government agencies and U.S. industry. ITS performs telecommunications research and provides technical engineering support on a reimbursable basis. ITS also has cooperative research agreements with private companies.

(2006)