Experience of wireless local area network in a radiation oncology department

ABSTRACT

The aim of this work is to develop a wireless local area network (LAN) between different types of users (Radiation Oncologists, Radiological Physicists, Radiation Technologists, etc) for efficient patient data management and to made easy the availability of information (chair side) to improve the quality of patient care in Radiation Oncology department. We have used mobile workstations (Laptops) and stationary workstations, all equipped with wireless-fidelity (Wi-Fi) access. Wireless standard 802.11g (as recommended by Institute of Electrical and Electronic Engineers (IEEE, Piscataway, NJ) has been used. The wireless networking was configured with the Service Set Identifier (SSID), Media Access Control (MAC) address filtering, and Wired Equivalent Privacy (WEP) network securities. We are successfully using this wireless network in sharing the indigenously developed patient information management software. The proper selection of the hardware and the software combined with a secure wireless LAN setup will lead to a more efficient and productive radiation oncology department.

KEY WORDS: Local area network, mobile workstation, network security, wireless networking

Abhijit Mandal, Anupam Kumar Asthana, Lalit Mohan Aggarwal

Department of Radiotherapy and Radiation Medicine, Institute of Medical Sciences, Banaras Hindu University, Varanasi-221 005, U. P., India

For correspondence:
Abhijit Mandal,
Department of Radiotherapy & Radiation Medicine, Institute of Medical Sciences,
Banaras Hindu University,
Varanasi - 221 005,
Uttar Pradesh, India.
E-mail: amandal751@yahoo.co.in

DOI: 10.4103/0973-1482.65236

INTRODUCTION

Efficient management and availability of accurate information improves the quality of patient care in radiation oncology department. There are many challenges involved in organizing and communicating information in radiation oncology. Complex planning and treatment delivery systems increase the amount of available data, which require a comprehensive information management system.[1-4] Organizational management of information in support of patient care, medical education and medical research is an area of interest in Medical Informatics, which includes acquisition, storage, retrieval and optimal use of medical information for problem solving and decision-making. The radiation oncology department is one of the most important sub-systems of the medical informatics world. The information system (IS) provides the backbone for communication, documentation and quality control and integrates all necessary data/images in a seamless, reliable and efficient manner.[1] As Radiotherapy technology and techniques have advanced, the IS have become electronic. This creates an additional level of complexity revolving around the electronic environment. Specifically, modern electronic IS are built on networks of computers connected in complex arrays, running sophisticated software, to provide transparent and seamless information availability to the users. Computers act as servers, controllers and interfaces. The network provides a data communication system between groups of interconnected computers. The computers on the network share information, application software and peripheral devices such as scanners, printers etc.[3-5] The network may be a local area network (LAN), limited to a single division or small group in one geographical location, or a wide area network (WAN) brings a larger geographical area into a single network.

With constant use of digital records, treatment planning and patient management software, there is a need for access to patient records, from both inside and outside the office, has become tremendous. In the last few years, several new technologies have emerged that made the use of mobile computers in Medicine more practical and useful. The utmost requirement is the development of fast, secure, and reliable wireless networking. Nearly instantaneous data access has been possible in the department via a wired local area network (LAN). However, because the computer is physically connected wired to the network, data access is restricted to particular sites in the department. A wireless connection to the LAN with a computer configured for it would provide data throughout the office, especially chair-side, as well as in the other areas of the department.[2] This would also permit easier simultaneous access to patient data, saving time in a busy radiation oncology department. With appropriate password protection, data can be safely accessed, modified, and saved. Therefore, we have made an attempt to use the prototype wireless local area networking in radiation oncology department.

MATERIALS AND METHODS

Three components are required to implement a wireless LAN: hardware, software, and network connection. Three mobile workstations (HP Pavilion Notebook dv2000 (HDD-80GB, RAM-1GB, dual core processor), one desktop (with a LAN card compatible to 802.11g wireless standard), all having built-in wireless-fidelity (wi-fi) access were used. In this prototype wireless network, we have used one laptop as a server as well as mobile workstations. Wireless Standard 802.11 and its sub standards are recommended by the Institute of Electrical and Electronic Engineers (IEEE, Piscataway, NJ). Because of its easy and fast deployment and installation, the 802.11 wireless networks has become one of the most useful networks. The commonly used wireless standards are 802.11a, 802.11b, and 802.11g [Table 1]. We have used 802.11g wireless standard, because of its adequate speed, range, compatibility and easy availability [Table 1]. In this study, we have used 54 Mbps wireless Router (NETGEAR, Model- WGR614v6). Security was the most important issue while establishing the wireless network, so that, patient data cannot be intercepted and accessed illegally (hacked) by someone other than the authorized user. An 802.11 wireless network can be secured by specific security protocols such as Wired Equivalent Privacy (WEP)-128 bit strength WEP encryption key, WPA and 802.11i, and mechanisms such as Service Set Identifier (SSID) and Media Access Control (MAC) address filtering, so that it remains compliant with Health Insurance Portability and Accountability Act (HIPAA).

The IEEE 802.11 is a family of standards, each one defining and specifying parts of the standard. The 802.11i standard defines the 802.11wireless network security protocols. The 802.11e standard defines the Quality of Service in 802.11 wireless networks.

The infrastructure and ad-hoc are the two basic modes of operation in 802.11 wireless networks.

In the infrastructure operation mode, there is no direct connection between others wireless clients; each wireless client connects directly to a central device called Access Point. The function of an Access Point is similar to a wireless hub that connects the wired network. The clients' authorization, authentication, access control and enabling data traffic encryption are the main responsibilities of Access Point. Ad-hoc operation mode each wireless client connects directly with each other. There is no central device. The security is a tough issue in this type of network because there is no central device that could authenticate and authorize the wireless clients. In this work, we have used the infrastructure operation mode.

The wireless networks generate a beacon signal periodically to detect the wireless clients for the presence of near surrounding wireless networks. The Access Point generates this signal; a beacon is a small broadcast data packet that reports the characteristics of the wireless network, with information such as supported data rate (max data rate), capabilities (encryption on or off), Access Point MAC address, SSID (wireless network name), etc.

We have developed a Radiation Oncology patient information management system, constructed by open source software. Features of this system are to browse the patient information with web browser.[6,7] This software has been shared with the wireless network between different users (Radiation Oncologists, Physicists, Radiation Technologists, etc) in our department for the data management of cancer patients attending the department. This system accepts simulator images from indigenously developed digital image management system (which was used to convert the analog images of simulator to digital images).[8]

RESULTS

Proper selection of hardware, software, and network standards will yield a useful, functional, and secure wireless network in

Table 1: Merits of various wireless security standards introduced by Institute of Electrical and Electronic Engineers (IEEE)

	Wireless standard			
Feature	**802.11b**	**802.11a**	**802.11g**	**802.16a (Wi-Max)**
Popularity	Widely adapted readily available everywhere	New technology	New technology with rapid growth expected	Newer technology that will surpass all other standards
Speed	11 Mbps	Up to 54 Mbps	Up to 54 Mbps	Up to 75 Mbps
Frequency	2.4 GHz. Conflicts may occur with other 2.4 GHz devices	5 GHz. Can co-exist with 2.4 GHz bandwidths	2.4 GHz. Conflicts may occur with other 2.4 GHz devices	2.11 GHz. Compatible with 802.11 b or g
Range	100-150 feet indoor	25-75 feet indoor	100-150 feet indoor	Up to 30 miles with a cell radius of 4-6 miles
Public access	Accessible via public hotspots	None	Accessible via public hotspots using 802.11b/802.11g	Accessible via public hotspots that use 802.11b/802.11g
Compatibility	Widely adopted	Incompatible with 802.11b or 802.11g	Interoperates with 802.11b networks (at 11 Mbps). Incompatible with 802.11a	Interoperates with 802.11wireless LANs

a radiation oncology department. We are successfully using this wireless network in sharing the indigenously developed patient information management software. Patient data will be compromised if security is not treated as a vital issue when implementing a network system. Among the current standards of wireless networking and in terms of security, speed of transmission, bandwidth, etc, 802.11g appear useful for a radiation oncology department. Newer standards in wireless bandwidths are being introduced (802.11n, 802.16) that still need to be tested for suitability for clinical application.

DISCUSSION

The security is the most important issue in wireless transmissions. It is very difficult to control, which computers or devices are receiving the wireless network signal, as the wireless network based on RF signal. Therefore, the wireless must be protected from network attacks by software link-level protection, specifically implementing cryptography. The original 802.11 standard only offers WEP to secure the wireless network.

Simple protocols like simple mail transfer protocol and simple network management protocol were used in the past. These protocols were very simple and widely used but they were not necessarily efficient. Network communications have expanded dramatically into the wireless and mobile data communications arena.

SSID protection

The SSID is the most common and the default configuration in network settings for broadcasting. The SSID serves to identify a particular wireless network. The router is configured when it is initially installed on the network. A client that wants to join a wireless network must set the same SSID as the one in that particular Router (Access Point). Without it, the wireless client will not be able to select and join a wireless network. Network access control can be executed by using an SSID associated with an access point or a group of access points. The SSID acts as a simple password and provides a measure of security by hiding the SSID from the beacon. However, when the access point is configured to "broadcast" its SSID, this security is compromised. Hiding the SSID cannot be considered as a security measure, because most wireless network analyzers are capable of obtaining the hidden SSID by passively sniffing it from any probe signal containing the SSID. Even if you turn off the SSID broadcasting, the beacon signal cannot be turned off. A proper wireless network analyzer tool can make it visible even if the SSID hidden beacon generated by the Router.

MAC address control protection

An access point or a group of access points can be identified by an SSID and a client computer can be identified by the unique MAC address of its 802.11 network card. Each access point can be programmed with a list of MAC addresses that records the client computers, which increases the security of an 802.11 network. Any client computer cannot associate with the access point if the client's MAC address is not included in this list. In small departmental networks, MAC address filtering can provide good security [Figure 1].

The MAC address control only offers access control of the access point. The wireless network traffic confidentiality or integrity cannot be protected by this measure. Therefore, any wireless network protected with only this mechanism is very vulnerable and open to any network attack. As it is easy to change the MAC address (Windows and UNIX/Linux OS) on any wireless network interface temporarily, this security mechanism is vulnerable. Anyone can obtain by its own a list of registered MAC addresses using wireless analyzers utilities. One can passively monitor or sniff wireless network traffic, gathering important information about the wireless network.

WEP protection

WEP (Wired Equivalent Privacy) is a link-level security option in the 802.11 standard networks which provide the protection of the confidentiality and integrity of the wireless network traffic. WEP provides encrypted communication by using an encryption key between the client and an access point. All users and access points on a wireless network use the same static key to encrypt and decrypt data.[9] In this work, WEP uses the RC4 stream cipher with 128 bits key to provide data packet encryption. As part of the WEP key is transmitted in clear text along with the data packet, the effective key becomes smaller. The WEP key has two parts: a dynamic value called initialization vector (IV) and the static part of the key called the shared secret key. The IV is a dynamic 24-bit value chosen randomly by the transmitter wireless network interface giving more than 16 millions possible keys and each message can be encrypted with a different key. The length of the shared secret key is 104 bits long (13 ASCII character) key for a 128 bit key. First, the wireless network interface randomly chooses an IV value and the shared secret key to form the WEP Key (IV + secret key). The IV value was chosen as per the manufacturer

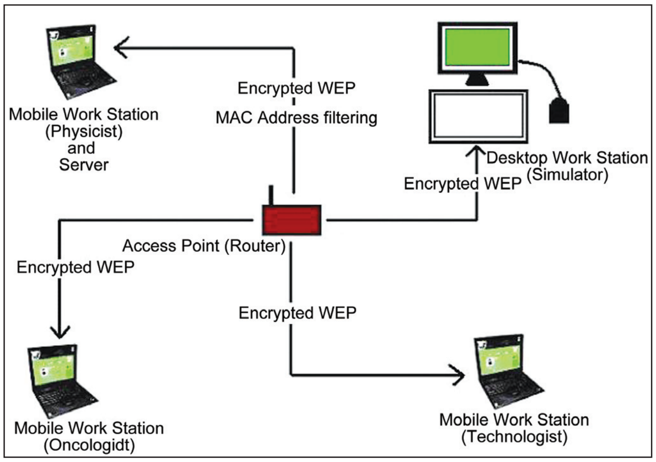

Figure 1: Schematic diagram of wireless local area network secured by encrypted WEP, MAC address filtering and SSID

specification. The RC4 stream cipher produces a pseudo-random string with the data packet length from this WEP key. The WEP-protected data packet, the link-level headers, IV value and the encrypted data packet are then packed together and then transmitted to the recipient. The recipient decrypts a WEP-protected data packet; it first reads the IV value and then follows the same steps of the encryption process.

Even the wireless connection according to 802.11 protocol shows a great advancement, it has limits in terms of speed, range, security, power, and imaging capabilities [Table 1]. Even though the data transfer rate with a wireless device is about a tenth as fast as it is with a wired network, that rate was fast enough for almost all computer tasks in any radiation oncology department, with the exception of full motion streaming video. Advanced wireless specifications that would come in the due course of time will increase the data transfer speed. Wireless networks have a limited range; walls, positioning of the access points can degrade wireless connections and electrical activity in the area also degrades the signal. Another limitation is the power source for the hardware. Mobile devices run on batteries, which have limited life, so mobile devices will deliver at the most 3 to 4 hours of service. The time could vary depending on how the device is used.

CONCLUSION

From our experience with wireless networking and patient information management system, we can conclude that with the easy availability of hardware and software, it is very simple and cost effective to setup a secure wireless LAN for radiation oncology department. The wireless networking in combination with well designed patient IS will lead to a more efficient and productive radiation oncology department in spite of limitations on range, speed, power, and bandwidth. Some important limitations of wired network (i.e. messy wire connections and chair side users restriction) can be completely avoided. Authentic users can access the patient information from any where of the department.

REFERENCES

1. Palta JR, Frouhar VA, Dempsey JF. Web-based submission, archive, and review of radiotherapy data for clinical quality assurance: A new paradigm. Int J Radiat Oncol Biol Phys 2003;57:1427-36.
2. Yokohama N, Kagiya G. Development of a radiation therapy information system and linked medical image server using techniques of WWW-DB. Nippon Hoshasen Gijutsu Gakkai Zasshi 2004;60:835-41.
3. Nagata Y, Okajima K, Murata R, Mitsumori M, Mizowaki T, Yamamoto M, *et al*. Development of an integrated radiotherapy network system. Int J Radiat Oncol Biol Phys 1996;34:1105-11.
4. Kalet IJ, Jacky JP, Risler R, Rohlin S, Wootton P. Integration of radiotherapy planning systems and radiotherapy treatment equipment: 11 years experience. Int J Radiat Oncol Biol Phys 1997;38:213-21.
5. Smith CL, Chu WK, Enke C. A review of digital image networking technologies for radiation oncology treatment planning. Med Dosim 1998;**23**:271-7.
6. Perriss RW, Graham RN, Scarsbrook AF. Understanding the internet, website design and intranet development: A primer for radiologists. Clin Radiol 2006;61:377-89.
7. Mandal A, Asthana AK, Aggarwal LM. Development of an electronic radiation oncology patient information management system. J Cancer Res Ther 2008;4:178-85.
8. Mandal A, Asthana AK, Aggarwal LM. Inexpensive digital image management system for conventional radiotherapy simulator. J Med Physics 2005;30:29-31.
9. Duntemann J. Making connections by cutting cables. Wi-Fi guide. Phoenix: Paraglyph Press; 2003. p. 65-85.

Source of Support: Nil, **Conflict of Interest:** None declared.