MEDINFO 2013
C.U. Lehmann et al. (Eds.)

doi:10.3233/978-1-61499-289-9-166

Ensuring the Security and Availability of a Hospital Wireless LAN System

Eisuke Hanada[a], Takato Kudou[b], Shusaku Tsumoto[a]

[a] *Division of Medical Informatics, Shimane University Hospital, Izumo, Japan*
[b] *Department of Electrical and Electronic Engineering, Faculty of Engineering, Oita University, Oita, Japan*

Abstract

Wireless technologies as part of the data communication infrastructure of modern hospitals are being rapidly introduced. Even though there are concerns about problems associated with wireless communication security, the demand is remarkably large. Herein we discuss security countermeasures that must be taken and issues concerning availability that must be considered to ensure safe hospital/business use of wireless LAN systems, referring to the procedures introduced at a university hospital. Security countermeasures differ according to their purpose, such as preventing illegal use or ensuring availability, both of which are discussed. The main focus of the availability discussion is on signal reach, electromagnetic noise elimination, and maintaining power supply to the network apparatus. It is our hope that this information will assist others in their efforts to ensure safe implementation of wireless LAN systems, especially in hospitals where they have the potential to greatly improve information sharing and patient safety.

Keywords:

Wireless LAN, Hospital information system, Data security.

Introduction

Wireless technologies as part of the data communication infrastructure of modern hospitals are being rapidly introduced [1, 2]. In wireless communication systems, data is transmitted by electromagnetic signals that travel freely through space, which makes them difficult to control and presents various security problems that must be addressed. Even though it is obvious that a wall made of metal reflects electromagnetic signals, wireless communication systems are sometimes planned without considering the construction materials, which can result in areas in which wireless communication was intended but that are not completely covered. The demand for wireless communications is remarkably high, which has resulted in some hospitals having too quickly introduced them without sufficient consideration of security and availability.

Herein we discuss security countermeasures and measures to ensure availability that must be taken to safeguard hospital/business use of wireless LAN systems, referring to the procedures introduced at a Japanese university hospital (hereafter, target hospital). The target hospital introduced a wireless LAN system that covers all its wards in 2003. Even though the hospital adopted a system with readily available technology and commonly used procedures, the system has been employed for over nine years with only minor problems that were easily addressed.

Wireless communication system of the target hospital

The target hospital and its hospital information system

The target hospital is a university hospital located in western Japan. It has 600 beds in 21 wards and has approximately 1,700 staff members, including about 380 physicians and 480 nurses in 30 clinical divisions. The older of the two buildings has eight floors, all 110 meters in length and oriented east to west, with the third to the eighth floors housing patient wards. Each floor has a staff station in the center of the building that includes a nursing care/management unit that is divided into sections that serve the east and west wards. Each ward houses from 30 to 40 inpatients.

A new building opened in June 2011. It has nine floors that are 51 meters east to west and 31 meters (the lower four floors are 51 meters) north to south. The fifth to ninth floors are wards, and there is a staff station in the center of each floor. The ICU and other special sections are located on the second floor of the new building. Next to these buildings sits a three-story building that houses the outpatient clinics and special examination sections. The locations of these building are shown in Figure 1. The floor plan of the new building is shown in Figure 2.

Figure 1 - Location of the target hospital buildings (11: Old building, 33: New building, 10: Building for outpatient clinics, 12, 20: Examination sections,21: Warehouse for patient records)

The hospital information system (HIS) of the target hospital includes a computerized patient record system (September 2006), computerized nursing records (September 2006), and a filmless PACS (April 2008). The integration of these systems means that we have not only completely systematized and computerized our medical records, but that we have enabled the instant sharing of patient information and our physicians' instructions on patient care.

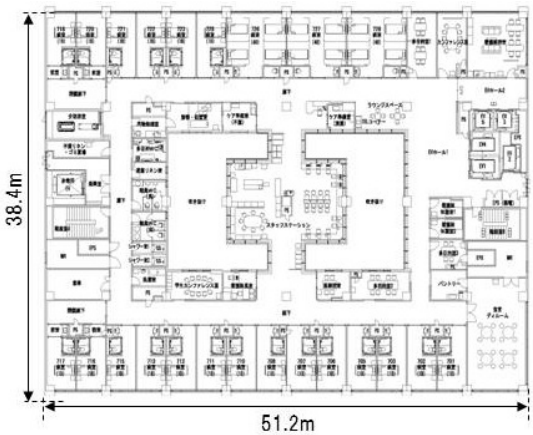

Figure 2 - Floor plan of the new building (7F)

Wireless LAN system installation in the target hospital

Wireless LAN communication infrastructure was introduced throughout the older building, marked 11 in Figure 1, in October 2003 [1], with IEEE 802.11a the adopted specification. A new wireless LAN system was introduced at the time of the opening of the new building, 33 in Figure 1. In the new building, 87 sets of access points (APs) were installed. The number and locations of the APs installed in the new building were determined based on the results of electromagnetic propagation simulation. The simulation results are shown later in this paper.

After the new building was completed, remodeling of the older building and the outpatient clinic building began. The old APs had be removed and refigured because the walls and ceilings of the older building were changed during reconstruction. Although the older system was working well, technological change had outdated many features, so we decided to remodel the system by replacing the APs and updating the wireless LAN communication infrastructure to the same, modern design as that of the new building. The number of APs in the older building has been increased by about 1.5 times, and the number of wireless HIS terminals will eventually be increased to approximately 180.

Security policy of the target hospital wireless LAN

Initially, the wireless LAN communication infrastructure of the target hospital was for staff use only. As requested by the staff, the wireless LAN network is connected to the Internet through proxy and a firewall. The firewall blocks access from outside the system, but it possible to read e-mails at terminals connected to the wireless LAN. Anti-virus software has been installed to scan the e-mails from the e-mail server, and it is constantly updated. MAC Address filtering was used in the APs to prevent unauthorized connection. Also, the setup of the Service Set Identifier (SSID) refuses connection with the values "Any" or blank, and the value is different for each floor to prevent unauthorized connection and to prevent terminals from being moved from their assigned floor. WPA2-PKI data encryption is used to prevent the interception of information. In addition, communication logs are stored for a year and managed by the network administrators. Although the input of an ID and password is unnecessary at the time of connection to the network, authentication with an ID and password is necessary at the time of login to a destination system.

Both IEEE802.11a and IEEE802.11g specifications are used in the new system. Communication with HIS terminals is mainly done with 11a, and other uses are assigned 11g. The purpose of this separation is to keep the influence of other systems on the HIS at a minimum, for example by portable radiological equipment that transmits a massive amount of data. Patient charts in the past contained mostly text data and in many cases small pictures; thus the quantity of individual information was just several bytes to hundreds of kilobytes. Portable radiological imaging equipment, which is now in widespread use, demands the transmission of tens of megabytes of data between a server and remote terminals. When using a wire-based communication system, the bandwidth can be secured using Quality of Service (QoS). However, with present wireless communication technologies, it is impossible to assign a bandwidth to an individual session. Thus, a mass data transmission using wireless communication can affect other sessions. For many physicians, such as surgeons and emergency room doctors, instant access to information is imperative, and delays of even a few seconds cannot be tolerated. It is important that they be able to refer to information, determine a course of action, and input information related to patient care in as short a time as possible.

To prevent their loss by movement to other areas of the hospital, PCs, which are used as HIS terminals, are forbidden from being moved to any area other than that to which they were assigned by the system administrator. However, a medical model has come to be used in which medical teams are a blend of staff from the traditional clinical divisions. This means that staff members may work in multiple wards. To solve the challenges created by this movement, we adopted Dynamic Virtual LAN (VLAN) technology that enables selection of a connection destination by setting up an SSID for use in a single floor unit or for the whole building. This was realized by using APs and switches that can set up with two or more VLANs. The setting-up of SSID terminals is restricted to the system administrators, and changes by the users are not permitted.

Ensuring availability of the target hospital wireless LAN

To ensure the availability of wireless communications, the target hospital took preventive measures for each network apparatus, such as signal reach management, a noise invasion check, and power supply management.

To confirm the reachable area, an electromagnetic propagation simulation was done before starting installation. An example of the simulation result is shown in Figure 3.

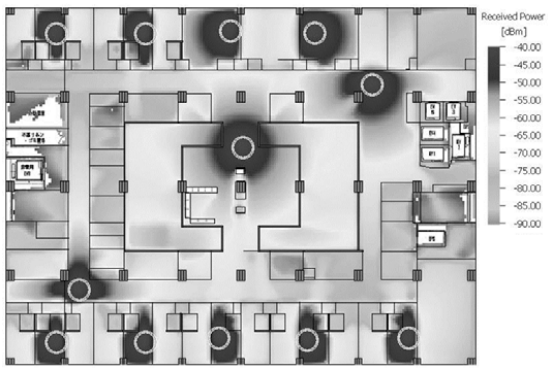

Figure 3- Simulation results (7F in the new building, circle is the recommended position of an AP)

In this simulation, specifications of the materials of the walls, doors, and other construction materials were gathered. Electromagnetic field propagation simulation was done using the ray-tracing method with Dominant Path Model [3, 4]. The necessary number of APs to be installed in the new building was determined based on the results of the simulation. For the signal invasion check, we walked around the areas in which the use wireless LAN was planned while checking the SSID of the signals using AirMagnet Surveyor. When we found a signal coming from outside, the intensity was measured. Both IEEE802.11a and 11g were measured. If the invasion was from outside or inside the hospital was confirmed by the received SSID. Measurement was performed after the building was completed, but before it began to be used. No APs other than those we planned existed in this building at the time of measurement. Some signals invading from the outside were found on all floors. No 11a signals were detected, and the three 11g signals detected were at intensities that were so weak that they would not affect wireless LAN communication in the target hospital.

The power supply to all APs is Power over Ethernet (PoE), and backup power is available to all networking apparatus, such as switches, to keep the whole wireless LAN appratus alive. Backup power is also available to HIS servers. Uninterrupted power supply (UPS) systems are used for each apparatus and the servers to prevent stoppage by sudden/short power failures. Terminals of the HIS connected to the wireless LAN can be driven by battery.

Uses of wireless LAN in the target hospital

Our wireless LAN is connected to HIS terminals that are equipped with barcode readers. Patients can easily be identified by reading their wristband. Patient information, such as vital signs, can be referred to and input at bedside. Also, recording the start and end of infusion has been enabled as has reference to the results of clinical laboratory tests and reference to radiological images. Drugs for infusion can be confirmed by reading a barcode on the seal attached to the bottle, which enables identification of who the drugs should be given to and when. If an infusion is canceled or changed, staff can obtain the necessary information by accessing the HIS server from the bedside.

Figure 4 – A nurse in an inpatient room using a wireless HIS terminal

In addition, since the new building of the target hospital opened the wireless LAN is being used not only by HIS terminals but also by portable examination devices and surgical instruments that have had RFID tags attached [5].

Results

Only minor problems with communication using the above setup were reported. Before renovation, there were a few reports of premature disconnection because the signals from the APs did not reach terminals in some areas. This occurred because of an insufficient number and poor location at the time of installation, problems that were rectified at the time of remodeling.

Because there are too few workers to staff each room, a wireless LAN communication infrastructure has been added to reduce the burden on the staff. We have not as yet started our research on the effectiveness of the wireless LAN in the outpatient building.

Discussion

Because much sensitive personal information is dealt with in hospitals there has been some resistance to the use of wireless LAN. Labor shortages are being experienced by large Japanese hospitals, making labor efficiency of the utmost importance. The benefits of wireless LAN for quickly and accurately transmitting the physician's instructions regarding patient care have resulted in the widespread introduction of wireless LAN systems. However, the high costs related to the necessity to ensure a high level of security are problematic for hospitals. Because of the above conditions, continued improvement of the security of wireless LAN technology will be necessary to ensure its continued safe use in Japanese hospitals.

We recommend doing the following before the introduction of a wireless LAN system that deals with patient information

1. Taking measures against unauthorized access: A plan for preventing connection to the wireless LAN system without the permission of the administrator
2. Taking measures against illegal interception of data: A plan for preventing the interception of wireless LAN signals and data tapping
3. Taking measures against unauthorized users

4. Management of communication logs to verify the appropriateness of the use of data

As a concrete measure against unauthorized access, MAC address filtering etc. should be considered. Encryption is a common measure against illegal interception, and user authentication a good example of a measure that has proven useful for controlling unauthorized access. In addition, authentication using Remote Authentication Dial In User Service (RADIUS), a one-time password system, computer virus quarantine, and digital certificates, etc. can be useful security measures. Security policy can be divided into measures that protect the wireless LAN system and those that protect the destination server. The planners of the wireless LAN should contact the server managers to confer about the measures to be taken before LAN installation. Overly complex procedures create a huge burden on the users, so procedures must be carefully crafted for the LAN and for each system.

In addition to the above security measures, we recommend that the following be examined to ensure availability.

5. The accessible environment: Ensuring the necessary range of signal access, measures against jamming by electromagnetic noise, and measures against signal invasion
6. Ensuring proper operation: Measures to ensure constant power supply, measures against equipment failure

It is necessary to ensure an adequate range of signal access; thus it is important to have as much information as possible about the structure of the building, the building components, and the arrangement of medical devices and metal fixtures. Because the remodeling of hospital buildings is difficult and costly, we think it important that the administrators of systems that involve radio communication be involved in the process of building design. Electromagnetic propagation simulation at the time of planning for the location of APs is imperative. Ensuring the proper wiring route from switches to APs is an example of an important matter that should be taken into consideration before building construction, but that is often overlooked.

When the installed wireless communication system uses an ISM band, such as IEEE802.11g, microwave ovens and microwave therapy equipment are potential electromagnetic noise sources [6]. Some heaters may also emit or leak an electromagnetic field. Because they are managed by staff members, the interference from these devices can be minimized by careful location or by shielding. Electromagnetic noise or signals from APs installed in an adjoining building may affect the wireless communications of a hospital. In hospitals in which information is computerized, a communication blackout would result in the inability to access patient information.

As a result, there could be serious danger to the lives of the patients. We recommend that the electromagnetic environment be investigated before, and periodically after, AP installation. It has been shown in Japanese studies that little electromagnetic interference that would affect medical devices is generated by wireless LAN [7]. This is shown by the following; The maximum output of wireless LAN technologies is about 150 milliwatt by Japanese law. If the Japanese guidelines are followed, no interference with medical devices will occur, as shown by the results of irradiation experiments by the Ministry of Internal Affairs and Communications [8] and by our experiment [7].

To secure the power supply against unforeseen events, measures including the use of PoE and the preparation of UPS and an emergency electric power source should be considered. Because priority must be given to ensuring continuous power to medical devices, the design process for the emergency electric power source should include scope-of-supply decision-making and must be carefully done. Having more than one backup generator should also be considered as a measure against an equipment failure.

Other important security countermeasures against the leakage of data include measures against unauthorized visual access to portable terminal screens and the prevention of inaccurate screen hard copy. Most matters of this nature can be done as part of the setup of terminals or as a component of user education. When patient information is stored in terminal devices, such as desktop or laptop computers or PDAs, there is the potential for theft of or misuse of the information stored on them; thus strict information security measures are required. To ensure security, the computers can be locked to their desks or carts. Periodic inventory of each device and recording the ID of each user are measures that can help eliminate theft. A system for managing terminal devices needs to be constructed.

Japanese hospitals cannot account for the cost of a data communication network directly as a health care cost. With few exceptions, such as for the use of a private room or for special equipment, billing for other than direct medical costs is not permitted. In addition, introducing wireless LAN is currently expensive, and sometimes not considered cost-effective. Although the concern of Japanese hospitals for patient information protection has increased, it has not yet resulted in universal introduction of completely safe systems, and many hospitals have not introduced wireless LAN at all. The target hospital had conditions that encouraged the early computerization of patient information and the introduction of a wireless LAN infrastructure, such as a greater labor shortage than other hospitals. It is now being widely recognized that the introduction of information and communications technology (ICT) in clinical settings is effective in raising patient safety. Large hospitals that house patients with severe diseases are becoming highly cognizant of the benefits of the introduction of wireless communication infrastructure. A greater sense of security should lead to increased introduction of such systems in the future.

Conclusion

The target hospital has realized an environment in which access to and the sharing of information are possible ”anytime, anywhere", i.e., a "ubiquitous environment." The setup of the wireless LAN communication infrastructure we installed is only one example of the systems possible at the present time. Considering that security countermeasures are indispensable when introducing wireless communications to a clinical setting, the above security countermeasures and availability must be considered.

Acknowledgments

This work was partially supported by the Japan Society for the Promotion of Science (Basic research (B) No.24390129).

References

[1] Hanada E, Tsumoto S, Kobayashi S. A "ubiquitous environment" through wireless voice/data communication and a fully computerized hospital information system in a university hospital. WCC2010 E-Health 2010, IFIP AICT 335, Springer, 2010; pp.160-168.

[2] Heslop L, Weeding S, Dawson L, Fisher J, and Howard A. Implementation issues for mobile-wireless infrastructure and mobile health care computing devices for a hospital ward setting. J. Med. Syst. 2010; 34(4): 509-518.

[3] Ji Z., Li BH. Wang HX., et al.: Efficient ray-tracing methods for propagation prediction for indoor wireless communications. IEEE A P MAGAZINE 2001: 43(2): 41-49.

[4] Hoppe R., Wertz P., Landstorfer F. M., et al.: Advanced ray-optical wave propagation modeling for urban and indoor scenarios including wideband properties. European Trans. on Telecom. 2003: 14(1): 61-69.

[5] E. Hanada. Medical device management system using an RF-ID active tag with a unique sensor. Proc. IADIS International Conference e-Society2012, 367-374, Berlin, 2012.

[6] Hanada E, Hoshino Y, Takano T, Kudou T. A pilot study on electromagnetic interference between radio waves used in wireless LAN communication and medical electronic equipment. J. Inf. Tech. in Health. 2004: 2(4): 281-291.

[7] Hanada E, Hoshino Y, Kudou T. Safe introduction of in-hospital wireless LAN. Stud Health Technol Inform. 2004;107(Pt 2):1426-9.Ministry of Internal Affair and Communication (Japan) Guidelines for wireless communication tools to prevent affect to the implanted medical devices (in Japanese), 2010.

[8] Ministry of Internal Affair and Communication (Japan) Guidelines for Wireless communication tools to prevent affect to the implanted medical devices (in Japanese), 2010

Address for correspondence

Eisuke Hanada
Division of Medical Informatics, Shimane University Hospital,
Izumo, 693-8501, Japan
E-mail: e-hanada@med.shimane-u.ac.jp