INSURING THE SECURITY AND AVAILABILITY OF HOSPITAL WIRELESS LAN SYSTEMS

Eisuke Hanada#, Takato Kudou*, Shusaku Tsumoto#

#Division of Medical Informatics, Shimane University Hospital
*Faculty of Engineering, Oita University
Wireless Technologies in Modern Hospitals

• Rapidly introduced as part of the data communication infrastructure
  • The demand is remarkably high
• Sometimes planned without consideration of the construction materials
  • Metal plates in wall and floors obviously reflect electromagnetic signals, but metal is often used without proper planning
• Sometimes lack security
  • In addition to the cyphering of data, connection restrictions and user authentication are also necessary
EMC Between Wireless LAN and Medical Devices

“It is very rare that wireless LAN communication interferes with medical devices” (Japanese guidelines for wireless use)

- This has been shown by the results of irradiation experiments by the Ministry of Internal Affairs and Communications
- The maximum output of wireless LAN apparatus is set at 150mW by Japanese law
- Our studies have shown little EMI with medical devices by wireless LAN
Purpose and Target

- Located in Izumo in western Japan
- 2 buildings for inpatients
- 600 beds
- 21 wards with 30-40 beds each
- Each ward has 8-10 daytime and 2-5 night nurses

Procedures introduced at Shimane University Hospital (SUH)
The SUH Patient Information System

• SUH currently has:
  • Computerized patient records (from Sept., 2006)
  • Computerized nursing records (from Sept., 2006)
  • Filmless PACS (from April, 2008)
  • Order entry system for almost all physician instructions (from Nov., 2006)
  • Support system for making medical certification forms (from Nov., 2006)
  • Electronic “Introduction Letter” system (from 2001)
• The instantaneous sharing of patient information and doctor’s instructions has been enabled
System at SUH

computers were connected to the wireless LAN

• In addition, about 8 desktop PCs were available
Early Stage WLAN Security Settings

- Connectable Media Access Control (MAC) addresses were registered for each access point
  - Only registered PCs could connect to the hospital LAN
- The SSID value was different on each floor
  - An “Any” setting of the SSID was refused
  - The different values allow connection refusal to prevent unauthorized connection
- OCB AES (128 bits) was adopted as the cipher system
- HIS user authentication with ID/passwords
- Communication logs were stored for a year
Connection Problems
Example: Problems Involving Signal Reachability

• Connection problems arose
  ① In the common space for patients
    – Where nurses record the information of newly hospitalized patients
  ② In the consultation room of the ward
    – The door of the room must be closed during consultations

• We have placed additional APs to make connection available in these spaces
Reconstruction of SUH

- Reconstruction started in 2010 and finished in 2103
  - The main building was finished in June, 2011
- Wireless LAN use was to be available at the opening of this building
- We decided to reconstruct the whole WLAN system at this time
  - To correct the above mentioned problems
  - To adopt new technologies
Wireless LAN in the New Building

- Wireless LAN has been introduced into all floors, except the 4th floor, which is used for administrative functions, such as a server room.

< floor plan of 2nd floor

↓ floor plan of 7th floor
(staff station is at the center)
Electromagnetic Field Simulation in the New Building

- In the basic planning stage the designer proposed “6 APs to cover each floor”
  **We could not believe it!**

- We decide to do an electromagnetic field simulation with commonly used materials
  - Between patient rooms: Chalk walls
  - Door of the pipe space for every room: Metal

- Purpose of the simulation
  - To secure 10 Mbps transmission speed at each bedside, in hallways, and in the staff station
Simulation Result

Example: 7th floor

Notes:
- The ICU and HCU on the 2nd floor have few walls
- Hallways are divided by doors on the 8th and 9th floors (to insure cleanliness)
However, in Reality:

- Construction often progresses without adequate coordination with the builders
  
  -> Wiring work is often finished at different times and locations before the start of AP location

- We did a second simulation to verify differences in the range of access (11a and 11g)

- Compared with 11a, a smaller number is required for coverage in 11g

![Simulated throughput (11a)](image1)

![Simulated throughput (11g)](image2)
Current Security Policy

• The cipher system was changed to WAP2-PKI
  • Other systems (MAC address filtering, SSID settings, and communication log management) are done as before
• The input of an ID and password is unnecessary at the time of connection to the WLAN
  • Authentication with an ID and password is necessary at the time of login to a destination system
New WLAN Settings: Multi-Standard Use

• Both IEEE802.11a and 11g are used in the new WLAN system
  • 11a is assigned mainly to HIS terminals
  • 11g is assigned to other uses
    Ex.) Portable radiological imaging device
    PC other than HIS terminal

• Purpose
  • We must keep the influence of other systems on the HIS to a minimum
  • Many physicians cannot tolerate delays in obtaining their desired information
New WLAN Settings: Dynamic VLAN

• "Medical teams,” such as Infection Control
Employment of WLAN Terminals in SUH

physician rounds

transfusion of the blood lot at the time of

confirmation of the drug and dose used in an
injection
SUH WLAN: Present and Future

• We now have almost 200 WLAN terminal PCs.

• The SUH wireless LAN has been successfully incorporated into the routine of hospital staff. SUH has realized an "ubiquitous environment" in which access to and the sharing of information are possible "anytime, anywhere."

Our future plans:
• Shifting to the use of IEEE802.11ac.
• Introduction of a system that uses RFID.
Conclusion

The continuous availability of WLAN and adequate security countermeasures are indispensable when introducing wireless patient information