Proceedings of the Second Joint EMBS/BMES Conference
Houston, TX, USA • October 23-26, 2002

Operational Parameters of a Medical Wireless LAN: Security, Range and Interference issues

Konstantinos A. Banitsas[1], Sapal Tachakra[2], Robert S. H. Istepanian[1]
[1]e-Med Systems and Health Engineering Group, Department of Electronic & Computer Engineering, Brunel University, Uxbridge, UB8 3PH, UK www.brunel.ac.uk/departments/ee/Research_Programme/e_med/pages/index.htm
[bany@hol.gr], www.bany.gr [robert.istepanian@brunel.ac.uk]
[2]A&E Department, North West London Hospitals NHS Trust, Central Middlesex Hospital, Acton Lane, London NW10 7NS. [sapal.tachakra@tinyworld.co.uk]

Abstract - **This paper provides an overview of the operational parameters of Wireless Local Area Networks (WLANs) in hospital and clinical ward environments and presents the concept of MedLAN system, dedicated to these environments. It then deals with the issues of security, range and interference with an emphasis on the first one.**

***Keywords* - wireless network, security, interference, range**

I. INTRODUCTION

Nowadays wireless LAN systems have gained an important position in the telemedical field. However, before hospitals will adopt such systems there is much concern about the security issues and the possible interference that these could cause to medical equipment. Privacy and security seems to be at risk as, installing a wireless LAN (WLAN) is considered to be as unsafe as putting network plugs everywhere, including areas in the immediate surroundings of the hospital.

II. THE MedLAN SYSTEM

Mobile telemedicine is a new and evolving area of telemedicine that exploits the recent developments in mobile networks for telemedical applications in general. Presently, a project named "MedLAN" is developed to accommodate these medical needs [1].

MedLAN consists of two main parts: A mobile trolley that exists in the open plan Accident & Emergencies majors area (A&E) and a consultation point, within the hospital.

The mobile trolley consists of a high-end laptop computer that is equipped with a WLAN PCMCIA card using the IEEE 802.11b protocol that permits total mobility within the A&E room and beyond. An access point (AP) within the A&E department acts as a wireless bridge for the network data to be transmitted to and received from the rest of the network. A high quality digital camcorder is connected to the laptop and high quality video and audio and still pictures can be transmitted. Additional medical instruments like otoscopes, dermascopes can also be connected to the system.

In the consultation point (either within the same hospital or in another NHS hospital) the consulting physician can have a choice of teleconferencing either from a fixed computer within the existing hospital network, or from a mobile computer, sharing the same mobility advantages as the former laptop. It can even transmit video to a PDA.

III. SECURITY

The IEEE 802.11b protocol includes two standards for ensuring security and privacy [2]:

- WEP: Wired Equivalent Protocol defines a mechanism for securing a WLAN. It uses RC4 algorithm to encrypt the wireless data stream offering access control and privacy services. To implement RC4, either a 40-bit or a 128-bit key is set both to the AP and to the client devices. If any of the client devices do not possess the correct key, the device will not be permitted to access the AP.
- SSID: A Service Set Identifier is a name for the wireless devices within the range of a WLAN. SSID is set by the AP and is transmitted in every of its beacons, therefore sole use of SSID is considered an unsafe.

Even with the use of the above encryption, there are still a number of security threats:

- Theft of hardware: After setting the correct key to the client card, that key is stored permanently within the card's memory. If a PCMCIA card gets lost or stolen anyone using it can access the WLAN. In that case, the network administrator can simply change the WEP keys both to the APs and to the client cards.
- Rogue APs: A possible attack to the system could be made by placing a dummy AP close to the existing WLAN. As clients will always try to associate with the AP that offers the best signal to noise ratio, they will connect to the dummy AP losing contact with the valid network. However, a simple site survey reveals the "hidden" APs.
- Disloyal personnel: Staff can be bribed to reveal the secret keys to a possible attacker. Nevertheless, in most of the systems, keys are revealed only to the persons setting them and not to the staff that operates the system.
- Hacker attacks: Much concern is given lately to the efficiency of the RC4 algorithm and its weaknesses [3]. By monitoring the data sent by the AP, a hacker could obtain information such as the client and AP's MAC addresses, MAC addresses of internal hosts, time periods that the system is used, etc. Doing a long-term analysis the attacker can extract some information out of the system.

In summary, to address the security issues raised above, a WLAN system should:

- Support mutual authentication between a client and an authentication server
- Base WLAN security on device-independent items such as usernames and passwords
- Support session-based WEP keys
- Make a right choice of encryption key to eliminate the RC4 weaknesses [3]
- Encapsulate WEP with other security protocols like IP Secure (IPSec)

To implement the above it is advised that a written security policy, establishing both the aims and the goals of the system, is set by the hospital management.

0-7803-7612-9/02/$17.00 © 2002 IEEE

IV. Range and Scalability

The range of the WLAN system is directly related to the security of the system: the designer of the system should know what is the area that needs "protection".

A site survey tool is usually included with most client card software. It allows the user to carry a mobile computer and examine the limitations of the WLAN.

Both the designer of such a system and the management of the hospital should keep in mind that:

- The nominal range that the manufacturer suggests is much higher than the actual range of the WLAN.
- Although the PCMCIA card's transceiver will only work in the effective range, by the use of special antennas this range can be widely extended.
- It is only with a site survey tool and with the use of practical means that the developer can estimate the effective range of the WLAN. Simulation and modeling tools fail to take into account small details (walls, furniture, metallic surfaces) that greatly affect WLANs
- When the signal quality of the WLAN is reduced, IEEE 802.11b falls-back in a lower speed to preserve the signal integrity. The fall-back speeds from 11 Mbps are 5.5, 2 and 1 Mbps
- IEEE 802.11b defines 11 channels in US and 13 channels in Europe; three of them being independent. By carefully placing the APs in order not to interfere with each other, the designer can extend the range of the WLAN all over the hospital space allowing for the mobile computers to roam from one AP to another without loosing connection.

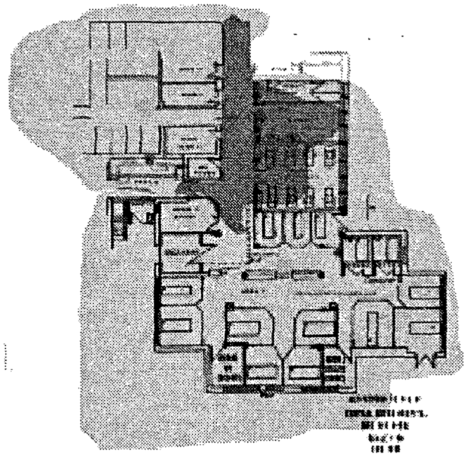

Fig. 1. Using two APs the whole area of the A&E room in CMH Hospital, is covered (green points indicate the AP's position)

V. Interference

Designing a system that uses radio signals within an A&E environment, one has to be extra careful for the possible interference that these signals might cause to the existing medical equipment. [4] The only way to determine that is by practically testing both the PCMCIA client and the Access Point in various scenarios inside the A&E ward.

Such a test was done in the Central Middlesex Hospital A&E ward, under the following conditions:

- Each of the devices usually found in an A&E or Resuscitation ward, was tested with emphasis on oscilloscopes.
- Both the client card and the AP were placed in a number of different positions near or on the device in question
- To ensure realistic conditions, all the above devices were connected to one or more patients and possible changes in their vital signs were examined both by doctors and by technicians.

Below is a table that summarizes some of the most frequently used equipment that can be found within an A&E room along with the possible interference that the MedLAN system could cause in such equipment.

No visible interference was noticed in all the medical equipment tested in Central Middlesex Hospital.

TABLE I

Medical equipment	Power	Effect
HP 78353 BU	30 mW	No visible interference
VDU monitors	30 mW	No visible interference
HP Page Writer Xli	30 mW	No visible interference
LIFEPAK 8 cardiac monitor	30 mW	No visible interference
Agilent Page Writer 300pi	30 mW	No visible interference
Nova SI and Profig Nutra	30 mW	No visible interference
Passport XG Datascope	30 mW	No visible interference
Propaq encore	30 mW	No visible interference

Fig. 2. Interference of IEEE 802.11b WLAN with existing medical devices

Usually it is devices that operate by amplifying a weak signal (ECG, EEG, etc) that are most vulnerable in radio interference. In contrast with Time Division or Frequency Division Multiple Access, that most of the mobile phones use, IEEE 802.11b uses Spread Spectrum techniques that minimize the amount of interference to such devices: instead of occupying a narrow band, SS spreads the energy of the signal over a wide frequency band.

V. Conclusions

Wireless LANs are a valuable tool in today's health care delivery. As they become increasingly popular, hospital management should consider using them in a wider scale, both for teleconsultation and for every day use.

Concern about the WLAN's security and safety is mostly based on reluctance to adopt new technologies, rather than the lack of security in itself: by following simple design rules, WLANs are proven to be as secure as (or even more secure) than their wired equivalents.

References

[1] K. A. Banitsas, R. Istepanian, S. Tachakra, "*Applications of Wireless LAN systems (MedLAN)*", IJMM, vol. 2, No. 2, pp. 136-142, January 2002

[2] Cisco, "*Wireless LAN Security*", white paper, 2002

[3] A. Stubblefield, J. Ioannidis, A. Rubin, "*Using the Fluhrer, Mantin, and Shamir Attack to Break WEP*", rev. 2, AT&T Labs Technical Report TD-4ZCPZZ, August 2001

[4] J. S. Lombardo, M. McCarty, R. A. Wojcik, "*An evaluation of mobile computing for information access at the point of care*", Biomedical instrumentation & technology, pp. 465-475, September / October 1997