Design of a WLAN experiment: a case study

Philip Tsang†, Paul Kwok† & Sandy Y-M. Tse‡

Open University of Hong Kong, Hong Kong, China†
Hong Kong Web Symposium Consortium, Hong Kong, China‡

ABSTRACT: WLAN research and experiments can take on a positivist or post-positivist paradigm, depending upon the set aims and objectives. In WLAN experiments, one paradigm can take the form of site-surveying radio frequency modelling. This entails a physical site survey of empirical measurements or the utilisation of software tools (such as *OPNET* or *NEC2*), with a built-in or user definable signal propagation model. In this research paper, the authors describe a longitudinal WLAN study of the largest WLAN experiments in the Hong Kong Special Administrative Region (SAR) of China, and the implications for engineering education are also discussed.

INTRODUCTION

The BSc/BSc(Hons) in Communications Technology programme at the Open University of Hong Kong (OUHK), Hong Kong, China, has been running in a distance learning mode for over eight years. Enrolments in the distance-learning programme have gone through a period of growth and a period of decline. Over the last two semesters, a climb in enrolments has been observed, coinciding with the restructuring of OUHK courses and the recovery of the local telecommunications industry. This recovery is fuelled by the development of WLAN, 3G mobile communication and associated services [1]. The demand for communication engineers is expected to increase and sustain itself in the next few years. Educators of future communications engineers need to be in line with, what the trend is, the needs of industry, as well as those of students. Equally important is the need to motivate students in their studies. In this paper, the authors report on their experiences in designing WLAN experiments that have been popular among project students since 2002.

EXPERIMENTAL DESIGNS

The whole project process involves the following key phases:

1. Students select a relevant area of study of WLAN either proposed by staff or initiated by students;
2. Literature and theoretical review of the focused area of WLAN;
3. Project plan of the experiment;
4. Carrying out pilot experiments;
5. Refining project objectives and techniques;
6. Undertaking the full-scale experiment;
7. Preparation and analysis of results;
8. Presentation of results to a large group audience;
9. Writing a report that incorporates feedback from audience.

It must be stressed that the research process is not linear and often includes feedback to previous phases.

SELECTION OF THE PROJECT

All communications technology project students must have completed all the technical courses, which provide them with sufficient background to conduct an investigative research project. Over the past three years, many students have focused on the theoretical background and the application of WLANs. Typical projects include the following:

- WLAN security and mathematical algorithms;
- WLAN geographic information system (GIS) mapping;
- WLAN surveillance system;
- WLAN traffic monitoring system;
- WLAN design and simulation;
- WLAN AP site survey and 802.11 antenna design.

In this paper, the authors focus on security, the quality of service (QoS) and DIY Antenna of WLAN. The study also forms part of a longitudinal study of WLAN deployment in Hong Kong. The aims of the experiment are twofold: to gain experience in the design of 802.11 antennas and to survey the current security status of WLAN in Hong Kong.

THEORETICAL REVIEW

WLAN Standards

The current rapid growth of WLAN has its roots in the ratification of the IEEE 802.11 standards during the 1990s. WLANs are of importance for providing ubiquitous access to a network. Students were guided to go over the 802.11 standards, from the common ones such as 802.11a, 802.11b and 802.11g, to the latest 802.11i, etc [3].

Students need to know more than just the speed of the standard. They also need to know the coding schemes, security characteristics, limitations and QoS of the standard. For example, they need to know that 802.11b, known as Wi-Fi, uses Direct Sequence Spread Spectrum (DSSS) at 2.4 GHz band and whether there are any overlap channels.

QoS and SNR Measurement of 802.11

The ITU-T defines QoS as *The collective effect of service performance, which determines the degree of satisfaction of a user of the service* [2]. While a number of parameters (delay, throughput, jitter, bandwidth, echo and packet loss) are associated with QoS, for this study's purpose, the QoS refers to the SNR strength of access point (AP), which enables a WLAN client to connect to the relevant APs.

Design of an 802.11 WLAN Antenna

In 2004, project students were asked to focus on two types of 2.4GHz antenna based on the collinear and waveguide concepts. For this purpose, students needed to review the theoretical models and construct their own. Figure 1 shows the theoretical construct of a collinear antenna.

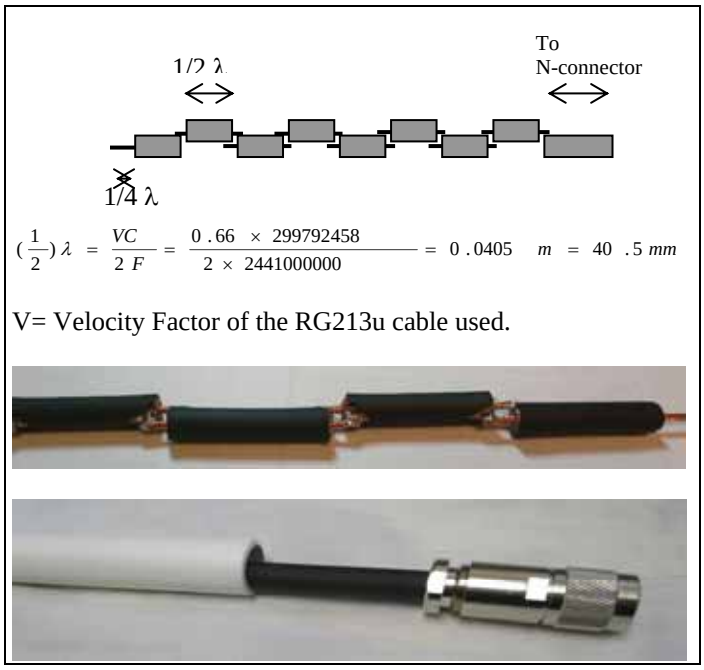

Figure 1: Design of collinear antenna from concept to construction.

Waveguide WLAN Antenna

Figure 2 shows the theoretical blueprint, while Figure 3 shows the final waveguide antenna designed and deployed in the WLAN site surveying experiment, and the actual implementation of the two antennas designed.

PROJECT PLAN OF THE EXPERIMENT

As all the OUHK project students engaged in this study are employed full-time and many have family commitments, good planning is of paramount importance for the success of any of project course. Microsoft *Project* and *Excel* are the two software packages that help students with their projects. The planning of a project was also supported through many face-to-face Sunday meetings. In addition to face-to-face meetings in the project laboratory, students and staff are in constant contact, either via mobile phone or via an online support system.

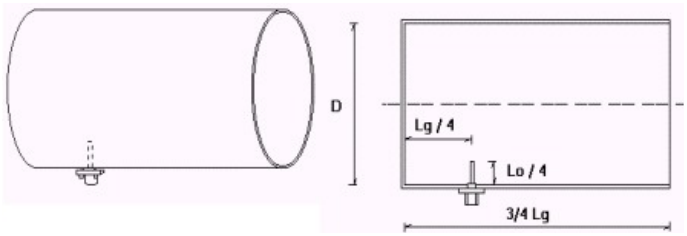

Figure 2: Theoretical construct of waveguide antenna.

Figure 3: The two antennas mounted on a site-surveying mobile-testing van. The circular one is the waveguide antenna and the tube-like one is the collinear antenna built by students. The vehicle used is the same van used in testing Hong Kong's 3G mobile station, which was commissioned by Hutchison Global Communications.

PILOT EXPERIMENT

A pilot experiment is an important part of any experiment as it can reduce/avoid potential mistakes (some may be inevitable) in the full-scale experiment. For example, the pilot experiment conducted three months before the real WLAN survey carried out in January 2005, a number of important issues and questions were identified. These included the following:

- The notebook PC battery ran down very fast;
- The input of the GIS interface was incompatible with the notebook interface ports;
- In one case, the higher gain antenna detected a smaller number of WLAN APs when compared to a notebook without an external antenna;
- The van hired for WLAN AP detection lacked a proper place to put the notebooks and the *bumping* of the van provided a nuisance to the experimenters and a hazard to the notebooks and built-in CD drive.

REDEFINING PROJECT OBJECTIVES AND TECHNIQUES

After the pilot experiment, it was decided to make it a worthwhile project; the experiments needed to be expanded in

scope to cover an additional subject area: that is, to have a site-survey of the design of WLAN in a particular shopping mall and compare it with designs using software such as *OPNET* or *NEC2*.

CARRYING OUT THE FULL-SCALE EXPERIMENT

For the 2004 project, only two types of a site survey were conducted, namely: *site-walking* and *site-driving*. Similar to earlier site surveys undertaken by Communication Technology project students, the 2004 experiment included:

- An industrial grade mobile signal testing van;
- Global positioning system (GPS) enabled interface;
- Onboard 220V/50Hz AC support for the notebook computers, and an industrial strength notebook holder with absorption cushion;
- Five notebook computers running Windows XP;
- 802.11 access point (AP) detection software was utilised.

Furthermore, the two DIY 802.11 antennas outlined earlier were added to the 2004 survey. The site-riding approach used in early 2004 was dropped as experience indicated that the site-driving approach produced better AP detection and was more cost effective when compared to the site-riding approach used previously (see Figure 4).

Figure 4: Snapshots of the WLAN field survey; the lower right hand corner shows a student riding a tram, while the upper right hand corner shows the screen capture of GIS and WLAN data.

Site Surveying

The survey consisted of two parts, namely: the site-driving of commercial, industrial and residential areas; and the site-walking of a shopping centre (Hollywood Plaza).

Selection of the Site-Driving Survey Path

Like the first large scale 802.11 site survey conducted in 2002, the routing consisted of two paths, described as follows.

- Route 1 is marked by the dark line on the northern side of the Victoria harbour (Kowloon) shown in Figure 5. It started from the OUHK campus in Homantin, Kowloon, through the business and tourist districts of Kowloon (Mong Kok, Tsim Sha Tsiu), plus various residential and industrial areas (Kwun Tong) of Kowloon, then across the East Harbour Tunnel to Hong Kong Island (where Route 2 starts);
- Route 2 is the Hong Kong Island path as marked by the dark line on the south side of Victoria Harbour. The path includes residential areas, business centres and ends in Kennedy Town, which has a mix of office and residential complexes.

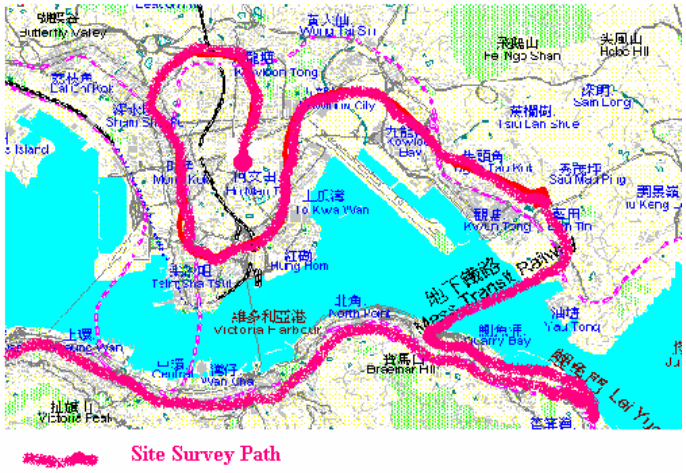

Figure 5: Site-survey path of the Hong Kong largest WLAN experiment.

The survey paths were repeated in reverse order once the final destination of route 2 (Kennedy town, lower left hand corner of the map) was reached.

Site-Walking of Hollywood Plaza

Hollywood Plaza consists of three main shopping floors. Students carried out a site-walking survey on each floor and mapped out the Signal to Noise Ratio (SNR) in the locations marked with arrows.

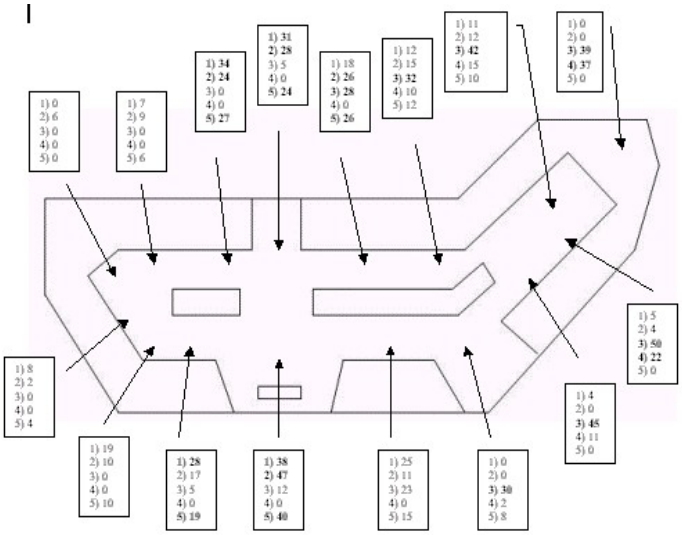

Figure 6: The QoS of the five APs detected and their distribution in a typical floor of Hollywood Plaza.

RESULTS OF THE SURVEY

The 2005 site-driving survey revealed a fivefold increase in WLAN APs. Among other results (such as a general increase in the use of 802.11g), there was a also change of percentage of

WLAN APs not enabling even the basic security (WEP) option of WLAN. For example, the figure was 71% in 2003, 79% in 2004, and 65% in 2005. The authors were more interested in encouraging project students to analyse and propose reasons for such a pattern change.

Another important finding in the 2005 experiment was the discovery of *WLAN stop packet*, which disabled all of the notebook PCs when entering a coverage area of a certain AP or AP clusters (see Figure 7).

Figure 7: All of the notebook PCs were frozen due to a *WLAN stop-packet* being received; this shows a typical 005 screen error.

Given prior experience gained with *WLAN kill packets*, which crashed two of the notebooks in 2003-2004, the finding has wide implications, be it for business or the military. For the site-walking survey, it was found that there were five WLAN access points (APs) on each floor. Better signals were received in the central areas, while poorer signals were received on the left side of the mall (see Figure 6). Students were also asked to ascertain where the APs were located and provide an AP location scheme. They were further asked to compare this scheme with simulation results using *OPNET*'s wireless module tools.

PRESENTING AND SUBMITTING FINAL REPORTS

Part of the Communication Technology series required project students to present their findings in an Emerging Technology Forum, which is held each year before the final examination. At the Forum, students put their experimental results and presentation skills to a final test. Students' performance at the Forum is factored into 10% of the course marks. Students had another four weeks to revise their final reports after the presentation.

CONCLUSIONS

While a wide range of hardware- and software-based projects are offered to project students, some topics are more popular than others. In this paper, the authors shared their experiences in coaching project students who chose to carry out a more in-depth study of WLANs via action research. While the WLAN projects have been made part of the longitudinal WLAN site-survey study, which began in 2002, new perspectives are constantly added to new WLAN projects each year. For example, QoS of WLAN and GIS AP mapping have been added along the two sides of Victoria Harbour, AP distribution scheme mapping in a large shopping mall, the simulation of WLAN APs allocation using tools like *OPENET*, and the design and simulation of 8021.11 antennas [4]. The authors consider it more important for students to appreciate the process of research – to communicate and analyse the findings rather than just record the data. A number of *firsts* have been achieved through this longitudinal study since 2002, namely:

- The first most comprehensive coverage of a WLAN site survey in Hong Kong SAR (2002-2003).
- The first and most comprehensive coverage of WLAN via site-driving (2002-2005).
- The first and most comprehensive coverage of WLAN via site-walking (2002-2005).
- The first and most comprehensive coverage of WLAN with GPS (2002-2005).
- The first and most comprehensive coverage of WLAN with self-made 802.11 antenna (2003-2005).
- The first WLAN site survey to capture the *stop packet* in Hong Kong (2004-2005).
- The first WLAN site survey to capture the *kill packet*, which crashed the XP system (2004).

A number of common misconceptions of WLAN were also demystified, such as detecting WLAN AP implies accessibility and that no WEP implies no security.

The following new perspectives will be added to the WLAN site-survey study in 2005-2006: more in-depth coverage of 802.11 antenna design and testing with the aim of students designing a low-cost high-gain 802.11 antenna that is patentable. Examining the best practices of adopting WLAN solutions, students will also make full use of the RF signal testing chamber for assessing 802.11 antennas (Figure 8) [4]. A new site-survey approach (such as site-flying, site-sailing, site cycling) and better use of simulation tools will also be added.

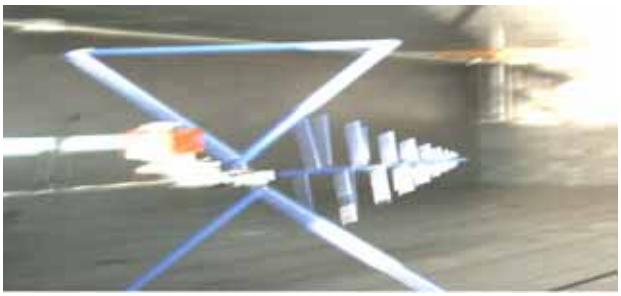

Figure 8: RF signal testing chamber (2 to 50 GHz).

ACKNOWLEDGEMENTS

The authors wish to thank the project tutor (Mr William Lai) and all the 2002-2005 WLAN project students for inspiring the writing of this paper. The authors also want to record their appreciation for the editorial assistance of Dr Rex Sharman, of the Education, Technology and Publishing Unit (ETPU) at the OUHK.

REFERENCES

1. Kwok, P., Tsang, P., Chu, W. and Lau, G., An overview of public LAN services in Hong Kong. *Proc. IMB2005*, 211-216 (2005).
2. Ohrtman, R.L., *Wi-Fi Handbook: Building 802.11b Wireless Networks*. New York: McGraw-Hill (2003).
3. Tsang, P., WLAN security: the next step. *Online Proc. APEC Telecom and IT Working Group Meeting*, Singapore (2004).
4. Tsang, P., Kwok, P., Lau, G. and Chu, W., A survey of success cases and best practices in adopting wireless enterprise solutions. *Proc. IMB2005*, 252-256 (2005).