Taste of Research
Gough Yumu LUI
Engineer's Log Book

Week 1

- Monday 15th November 2010

Taste of research started at 2pm for me as I had an exam in the morning. Had a meeting with the Head of School, Professor Chris Rizos and got a quick induction and explanation of what was required. We were then shown to the computer lab where we can work and tried to arrange ID card access. I sat with Binghao to get some ideas as to what direction the research should proceed – in the end, we concluded that it would be productive for me to quantify the differences between 2.4Ghz and 5Ghz propagation, especially in the case of MIMO based wireless N systems. It would also be productive if I could quantify the difference in signal strength reports from devices with different chipsets. The need for proper wireless N based equipment such as access points and client cards was discussed, with potential purchases to come later. Additional factors such as data rate for a given signal strength was discussed and decided as a promising lead. I also met Thomas Gallagher for a bit of a discussion about positioning algorithms and prior work – he e-mailed me some papers. Suggested to Binghao that we will need to discuss more about finding out information about the present Uniwide deployment – such as model of AP, locations, how the dual band configuration is done (is N in Greenfield mode or mixed mode?) and whether dynamic power control is enabled. Also suggested that I should probably look around and see what sort of candidate models of access points we could purchase for further research.

- Tuesday 16th November 2010

Took a formal look through all the induction material posted online. Realized there were forms for next of kin and OH&S checklist which has to be completed and returned by the end of the week. Filled in the next of kin form, arranged by e-mail with Binghao to meet the next day to get the OH&S checklist done and signed. Read two publications that were referred to me from Thomas – Wireless LAN Location-Sensing for Security Applications (TAO, Ping, et.al.) and Practical Robust Localization over Large-Scale 802.11 Wireless Networks (HAEBERLEN, Andreas, et.al.).

Practical Robust Localization over Large-Scale 802.11 Wireless Networks main points:

- Gaussian distribution used for signal strength fingerprinting – Gaussian more reliable than histogram method due to probability of seeing weak signal AP's drop in and out. Reduces storage requirements.
- Robustness distribution map shows a lack of robustness sometimes despite low distance from AP – why? Ambiguity perhaps?
- Time varying signal phenomena due to people more during the day – less during the night.
- Calibration curves for Prism and Atheros compared to the ACX100 card show an offset and a gain factor – based on signal intensity 8 bit value from driver – driver dependence? Also, already has been proven – so should probably expect offset and gain factor in testing.
- Fingerprinting method for location based on visible AP's and power. Auto and manual calibration available by scaling (?) observed values.

Wireless LAN Location-Sensing for Security Applications main points:

- Observed signal strength distributions are NOT Gaussian – strict contradiction. Bimodal distribution and unimodal depending on time. Average value is the most important.
- Signal strength proportional to transmitter power linearly (not so sure! – if there's a gain and offset error – it may not be proportional!)
- Histogram and Difference location method. Histogram uses Bayesian inference (?) scheme – conditional probability. Average difference between observed AP's used in difference mode as observation that "differences" are more robust in face of daily variations.
- Using different card produces comparable accuracy trained or histogram – doesn't this suggest either both cards are very similar in reporting signal strength or that the differences are not necessarily linear (i.e. diminishing accuracy for the difference case).
- Histogram method less robust but more accurate for situations where variances are small.

- Wednesday 17th November 2010

Made a trip into uni to get OH&S forms done and submitted to Chloe Fong in the Administrative unit. Took a look through the SSIS website under all publications for any and or all papers which mention wireless and wifi. Downloaded 22 publications in total (with more that were of interest but not directly related to the project). Took a quick search of the library's catalogue for general terms such as wifi, mimo to try and get some more information. Not much information available on mimo – mainly it's about chipsets and cards getting released.

Read some papers that were downloaded:

Uniwide Wifi Based Positioning System (Ching, W, et.al.):

- WiFi capable of room level accuracy. Time of Arrival, TDOA, Angle of arrival possible but difficult for WiFi – errors from NLOS. Not suitable for fine positioning.
- Triangulation – requires directional antennas and suffers from NLOS effects.
- Trilateration/multilateration – distance measurement difficult. Signal strength model not ideal.
- Fingerprint matching – problems with changes to environment, requires area to be surveyed.
- Netstumbler graph showing orientation causing signal strength changes – human effects? Device effects? Which orientation to test in? Fingerprints taken on several directions.
- Deterministic approach relies on least "distance" from a fingerprint, probabilistic approach calculates probability to the signal strength distribution. More sampling required.
- Android handsets used – server architecture used to provide positioning from an SQL database of fingerprints.

Design of an adaptive positioning system based on WiFi radio signals (Chiou YS. et.al.):

- Propagation modeling less computationally intensive, but less accurate that fingerprinting.
- Report focuses on filtering and tracking as solutions to variations in SS data.
- SNR is used instead of RSS. Radio propagation modeling.
- FSPL formulae not suitable for indoors due to multipath, scattering, attenuation dominance. A model is used which counts the number of walls and proposes a wall attenuation factor.
- SNR method shows better performance of Kalman Filter over Fingerprinting for number of AP's > 1.

Errors in Deterministic Wireless Fingerprinting Systems for Localization (Dempster A.G., et.al):

- Confirms RSSI changes are due to body – same graph as Ching, W, et.al.
- Inferred distance from RSSI doesn't have as strong of a correlation as desired.

Short Baseline Propagation Characteristics of Deterministic Wireless Fingerprinting Systems for Localisation (Dempster, A.G., et. Al.):

- Short range fingerprints exhibit fading dominated effects which cause problems for modeling.
- (?) Manhattan distance, Euclidean distance, L1, L2 norms?
- Weighted average neighbours better than nearest neighbour.
- RSSI variance more a function of distance than of time.
- Kismet used – probably try getting this and playing with it. Passive scanning. Netstumbler/Ministumber also mentioned.
- Was collection stopped when moving between points?
- Fig 4 – I don't see a bimodal relationship?
- Fig 5 – suggests a lot of variance compared to the slope?

- Thursday 18th November 2010

Received e-mail from Yong Li about access cards – have printed out the e-mail with me, but will not get card activated for access until I make my next trip to uni. Am enjoying the freedom of not needing to trip into uni as it saves me a lot of time. The flexibility is in stark contrast to working in the Government as I had done previously. Downloaded Backtrack 4 Live Linux Distribution – apparently this is used a lot for wireless network auditing and would be possibly quite useful for surveying wireless networks and recording signal strengths. Have booted it up but haven't had much progress besides scanning for networks.

Also have tried Netstumbler (doesn't work on Windows 7), and inSSIDer but haven't tried the logging features. Will have to find a software solution that works and possibly code up my own log processing program. Wonders whether promiscuous sniffing as I plan to do is comparable to active probe request – in theory it's coming from the same AP – but what about MIMO – will it beamform based on the incoming probe request and throw the probe response back stronger in that direction? What about different AP's with different degrees of beamforming ability – or no beamforming ability at all. Too many variables! http://www.kjhole.com/Standards/WiFi/WiFi-PDF/WLAN4alt.pdf seems to suggest "Passive scanning is mandatory, while active scanning is optional" – I'm not too sure about this. Also says "TPC and DFS were standardized as 802.11h in 2003."
http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/vowlan/41dg/vowlan_ch5.html seems to suggest Active Scanning is preferred as it's faster to solicit a response from AP's in range – but there's a potential problem – not all AP's respond to broadcast probe request frames.

Read more papers, many of which don't seem relevant to my line of work. Many related to Kridging as a method of correcting for NLOS phenomena or are not related to WLAN. Many were duplicate papers – same paper republished in different journals.

Indoor Positioning Techniques Based on Wireless LAN (Li, B., et.al.):
- SS to distance model found to be worse than fingerprinting with medium training.

Direction Based Wireless LAN Positioning (Li, B., et.al.):
- Estimate MU orientation as well.
- Fig 5a/b – why is the correlation reduced so much when human traffic is around? Expect relative strength ordering to remain consistent unless more people in one direction than another?

WIFE: Wireless Indoor Positioning Based on Fingerprint Evaluation (Papapostolou, A, Chaouchi, H.):
- Aliasing – points physically distant are close in signal space – use location history to eliminate aliasing.
- Random LOS creates zero readings which, when averaged, causes strong distortion in estimation process – data filtering removes zero valued samples.

802.11 Positioning in the Home (Salter, J, et.al.):
- Also used Kismet, passive scanning beacon frame signal strengths for fingerprints.
- Single AP fingerprint location is very sensitive – two AP's reduces sensitivity markedly.

Outdoor Localization of a WiFi source with unknown transmission power (Thompson, R.J.R., et.al):
- Test used AP on a survey trolley and VB Script to read RSSI from NDIS. Mode, rate fixed for fixed power.
- Log10 distance : RSSI straight line relationship.

Unsupervised Learning for Solving RSS Hardware Variance Problem in WiFi Localization (Tsui, A.W., et.al.):
- Experiments conducted by the authors and others show that RSS mapping from a tracking device to a training devise exhibits a linear relationship.
- Gain and offset can be estimated through easy to guess locations.
- Best adjustment is manual, however, difficult for large number of chipsets.
- Four chipsets shown – cross correlation produces straight lines (!!).
- Wonder if different channels will produce different results – would possibly make sense due to antenna/transmitter tolerances – is this a significant thing to follow?

An indoors wireless positioning system based on wireless local area network infrastructure (Wang, Y., et.al.):
- Figure 5 – SS vs time graph shows quite a lot of disturbance.
- External environmental elements always weaken the SS – is this true?
- Figure 7 seems to show a good SS decrease for distance correlation exponentially.
- Wall effect factor of about 15.9dBm.

Two New Algorithms for Indoor Wireless Positioning System (Wang Y., et.al.):

- Zero baseline test – laptop and desktop as close as possible facing the same AP – Fig 9 shows almost identical result whereas at a short baseline, the difference is significantly noticeable. Medium baseline shows a big difference with curve correlation beginning to suffer. At 15m, the differential system has totally failed. Does this suggest non-linearity in signal strength reports for different wireless cards? I think maybe!

GPS/WiFi Real-Time Positioning Device: An Initial Outcome (Wayn, C.J., et.al.):

- Passive Scanning, averaging of RSSI – Figure 5, a,b,c seem to show stepping in b and loss of signal between 40-55s which suggest strange AGC related events possibly?

Application of WiFi-based indoor positioning system for labor tracking at construction sites: A case study in Guangzhou MTR (Woo, S., et.al.):

- Wi-Fi Tags, Kalman Filter, Fingerprint Mapping with Interpolation.

It is of note that I haven't really found any other paper other than the one recommended by Thomas and the one found above which has much to do with different chipsets and signal strength data. I think this is probably the most important area of research to do, along with varying behaviour of wireless N nodes as there has been no papers I have found about that.

- Friday 19th November 2010

Had a thought about test design – what software is presently being used? How many samples are required for a point to average out instantaneous signal variations? Testing polarization? Multipath variables being controlled and human influence being controlled? At the moment, I haven't got much on the software, but I was thinking – if we take a scan every second, and we take 100 scans for every point – we have 20 seconds to reposition for a new spot surveyed every 2 minutes. If clocks on computer/device and me are synchronized, we can automate a program to process this data. Scanning was detailed as taking about 40 seconds in one paper – in my experience this is not true as if we do the scanning passively by observing beacon frames – i.e. airodump-ng style, we can get many samples per second provided the channel is locked.

Searching for access points are not necessarily fruitful. At the moment, I think the access points we would want to buy should have the following features:

- External power (not PoE – else we will need PoE adaptors as well)
- Wireless N with Dual Band
- Web Configuration (or console configuration, provided a manual is available – hopefully nothing too hard to setup)
- Power Control (dynamic power control preferable)
- Air Spectrum Analyser (would be nice).

One of the issues is – should we buy the ones that ITS are using – would that be better for our results? What about influences of external antennas. They're expensive – is there any consumer grade options which have similar features and could be used?

Models which I found online and notes about them:

- Linksys by Cisco – WAP610N Wireless N Dual Band – internal antennas have 1.58dbi gain for 2.4ghz and 1.45dbi for 5ghz – may not be desireable – from my understanding, <2.1dbi = less than a dipole. Consumer grade.
- D-Link DAP-2690 Airpremier Wireless N Dual Band with PoE – External antennas could be replaceable which may be good. Has web management interface. Supposedly enterprise grade.
- D-Link DAP-1522 Xtreme N Duo Wireless Bridge/AP – internal antenna, browser config – consumer grade.

- Netgear Prosafe Dual Band Wireless-N Access Point WNDAP350 – PoE power with internal antennas. External antennas catered for with external ports. Power adaptor is available. Web config supported. Supposedly enterprise grade.
- **Ruckus Wireless Zoneflex 7962 dual band with dynamic beamforming – "automatic interference mitigation" – 8 db signal gain, -15db interference rejection with 4000 pattern smart antenna array. 16SSID support, load balancing.**
- **Ruckus Wireless Zoneflex 7363 "mid grade" with dynamic beamforming – 4db signal gain - 10db rejection, 300 patterns and 8 ssids, load balancing.**
- Apple Airport Extreme – consumer grade, integrated antenna. Airport utility required to configure, external adaptor.
- Buffalo Tech – all AP's are not explicitly dual band according to the website. Not enough information available.
- Netgear Rangemax Dual Band Wireless N Router WNDR3700 – Consumer grade, not much info.
- ZyXEL NWA3166 Dual Band Wireless N access point – corporate grade – managed or independent AP with 3 internal antennas. PoE.
- Sonicwall SonicPoint N Dual Band Wireless AP – corporate/kiosk grade dual band. Not much info available.
- Trendnet TEW-670AP 300Mbps Concurrent Dual Band wireless N access point – 4 SSID's supported, external antennas – 2x3dBi with 2x4dBi internal antennas.
- **Aruba Networks AP-105 Access Point – 2x2 MIMO radios with internal omni antennas. Adaptive Radio Management and Spectrum Analysis Capabilities (!!). PoE or standalone PSU. Transmit power configurable in steps of 0.5dBm (!!).**
- HP V-M200 – Web interface, three external antennas, PoE or standalone PSU. Four SSID support, 3x3 MIMO.
- HP A-802.11n Access Point – Auto Channel Selection/DFS. Sparse information.
- Cisco Aironet 1140 Series – M-Drive Technology, Dynamic Frequency Selection, PoE, integrated antenna. Requires IOS/UWN Software for configuration. Discrete power level settings in certain steps – 10/17/14/11/8/5/2/-1 dBm only. Omni antennas with 4.0dBi on 2.4Ghz and 3dBi on 5Ghz. Clientlink technology produces beamforming according to their white paper – beamforming has potential to skew signal strengths.
- Cisco AP 541N Wireless Access Point – dual band N clustering AP for small businesses – 2T3R design with 3 antenna ports. Information sparse.
- Cisco Aironet 1040 Series – dual band to be released Q4CY10 – 2x2 MIMO with MRC and DFS, CSD support. Integrated panel antenna. Transmit power settings in steps only. Requires software to configure.
- Cisco Aironet 1250 Series – dual band – similar to 1040 but with external antennas and dual radios. Stepped power options as well.
- Cisco Aironet 1260 Series – 2x3 MIMO similar to 1250 with external antennas. Stepped power.
- **Cisco Aironet 3500 Series – clean air technology for self healing, self optimizing wireless network. RF interference detection. 2x3 MIMO, MRC, beamforming, DFS, CSD. Stepped transmit power. PoE, software to configure. Unsure if it can be deployed without an accompanying wireless AP controller unit. Read CleanAir Deployment Guide – Radio Resource Management system. Difficult setup.**