Detecting, Locating, and Tracking Hacker Activities within a WLAN Network

Kevin C. Shum, and Joseph K. Ng
Department of Computer Science, Hong Kong Baptist University, Kowloon Tong, Hong Kong
{cyshum,jng}@comp.hkbu.edu.hk

Abstract

When it comes to positioning technology, people usually think about the Global Positioning System (GPS). However, GPS, although mature enough to be used for navigation and tracking of goods, it is not effective in indoor environment. On the other hand, with the advance in WLAN technology and the popular adoption of wireless equipments and in particular, the IEEE 802.11 family, almost everyone in the community has a Wi-Fi enabled device integrated into their everyday life. With a good location estimation integrated into a Wi-Fi surveillance system, system administrator can closely monitor the network traffic as well as the behavior of the mobile users. Hence, there is a growing demand to have a quick and efficient way to indentify a specific group of people, or devices or asset within a controlled wireless network. In our proposed system, all the Wi-Fi traffic or information especially the MAC addresses and RSSI from the mobile clients (i.e. Wi-Fi devices) can be sniffed by an open-source Wi-Fi router or access point with custom-made embedded software program without pre-loading any client program on the mobile user devices. These sniffed information is then analyzed and stored in a database which will help network administrator to monitor the wireless network for surveillance purpose and security concerns. In summary, this paper proposes a wireless LAN system that can detect, locate and track down wireless communication within the system by modifying the embedded software in off-the-shelf WLAN routers or access points. Experiment results have shown that abnormal wireless activities can be detected and by our signal strength based localization algorithm, positions of these wireless mobile devices can be identified and be tracked within meters inside our WLAN system.

1. Introduction

Under the Government's Digital 21 Strategy [1] to build Hong Kong into a wireless city, the HKSAR government had put forward a Wi-Fi Programme (GovWiFi) [2] as an initiative to create a wireless infrastructure to facilitate Internet access by citizens and businesses for enhancing quality of living and business operations. Other than the intended value-added services on the Internet, this programme also raises serious concern about hacking activities within the WLAN networks. In view of the heavy usage and progressively growing coverage of WLAN within the indoor environment, and the relatively few research studies on effective ways to do WLAN positioning and tracking, there is a need to investigate the feasibility of using the WLAN to locate a mobile user as well as tracking hacking activities in an indoor environment.

Wi-Fi becomes a much more valuable asset within a computer network; every mobile user can be granted a permission to use those Wi-Fi accesses within a permitted area. Consequently, mobile hackers and unauthorized access are possible within a mobile network, and no good tools are available to monitor the wireless network easily. In this paper, we proposed a back-end network surveillance system making use of a popular off-the-shelf wireless router by Linksys – (Model: WRT54G).[3]

It is important for us to consider a network which is capable of monitoring the access of the valuable wireless assets, and can be able to locate key personnel as well as mobile users. Every mobile device has a unique Media Access Control (MAC) address, and almost all the smart phones developed are equipped with a Wi-Fi chipset. When a mobile user turn-on the Wi-Fi access in his smart phone and entered into WLAN covered area, the message and packet exchanges with its corresponding signal strength become the fingerprint or the identifier for the mobile user within the network. Hence, there is a need to conduct a research to build an efficient and effective surveillance network to improve the system administrator's sensitivity to detect, locate, and to track hackers within a Wi-Fi network.

Besides, the estimation of the location of the hackers, or harmful devices can be useful for system administrator, as well as policeman to determine the location of those users, as to minimize the time for them to stop the un-authorized access to the network. As wireless networks are installed everywhere, the maintenance and fine tuning of the network become very complicated especially when hacker's activities are involved.

We very much relying on the existing intrusion detecting algorithm for detecting hackers' presence in a WLAN, but for detecting the hacker's location, there are some constraints when constructing our location estimation algorithms. First of all, we cannot assume that we can plant a client program in the hacker's device for data acquisition, that is for collecting the signal strength information at the mobile device for location estimation. Furthermore, we cannot assume that the hacker devices will behave like an ordinary mobile device, because they can change their SSID at will, tune up and tune down the antenna power for bigger fluctuation of signal strength in order to avoid being detected and located [4]. Hence, our approach is to enhance and rewrite embedded software at the Access Point (AP) side to "listen" to "conversations" among all the APs and wireless devices within the coverage of the WLAN network. In more technical terms, we will write software and re-program the AP and wireless Routers such that our software can collect signal strength readings when wireless devices, especially those hacker devices, that are communicating with any of the surrounding APs. [5] With these signal strength readings collected in real-time and stored in the data store at our data centre, together with the known positions of the APs, we can reuse our previous algorithms [6-12] to find out the whereabouts of the hacker devices.

Besides tracking hacker's activities within the WLAN, while some of the Wi-Fi devices are attached to the network all day, some of the Wi-Fi devices are only attached to the network in the daytime, but not at night. Thus, the ability to monitor the health and status of major components and key devices, such that we can receive prompt notification when changes appear, also serve an important role for network maintenance.

Finally, there are a number of ways to locate a mobile user based on RSSI. Some of the fundamental position techniques

are Location fingerprinting (LF), Propagation Loss Model (RF), Tri-lateration, Tri-angulations and Radio Maps with pattern recognition approaches. [13-17]. As yet another location estimation algorithms is not our main focus in this paper, for easier deployment of our system, and with the limited computation power of our system servers, a center of gravity (CG) method for location estimation is adopted in our system just for demonstrating the effectiveness for network surveillance purpose. [18]

2. Related work

In previous years, our research group had done quite a number of work on mobile phone positioning and results are astounding [19-30]. Although theoretically we can use the same or similar location estimation algorithms for the mobile phone network to be applied to the WLAN, there is relatively few researches on WLAN positioning [31-34] in the literature. The problems are mainly due to the differences in penetration power, signal fading, signal attenuation, the layout of access points (regularity vs. randomness), and the more serious body effect within the WLAN as compare to the mobile phone network. Although many researchers have proposed methods in providing location services using the mobile phone networks, few projects have actually been implemented. The RADAR system [32] was one of the early WLAN-based location estimation systems. Based on the FreeBSD distribution and WaveLAN WLAN network, the RADAR system can locate a user who carries a notebook with an accuracy of 5 meters. Y. Wang et al [31] did have a study on the feasibility for making use of the WLAN to locate a mobile device. They had done an empirical study inside their department building and labs and reported their findings and simulation results. However, there is no systematic way to generalize these approaches and in fine tuning the necessary environment parameters. Furthermore, the target environment is critical to the quality of positioning. Radio characteristics in an open environment are never static and there is no single methodology that can fine tune data from time-to-time to adapt with the changing environment. It is only recently that they starts to have studies on post-deployment adaptation issues. These include installing special hardware which monitors radio characteristics at different position and rebuild the propagation model from time-to-time [33, 34]. Among the commercial products that are available for WLAN positioning, ekahau is the company that is taking a leading position in in-door positioning. Their positioning system relies on building an accurate radio map according to the layout of the access points as well as the model and specific characteristics of these access points. Regardless that it is a costly system, it also subject to environmental changes and post-deployment adaptation problems.

3. Proposed System and Technologies Involved

Electronics, computers and wireless devices are becoming more in-expensive, low-power usage and multifunctional. And recent open-source wireless router has fast data processor that can handle real-time data acquisition for wireless network surveillance as well as location estimation for wireless devices.

In our experiments, a programmable router - Linksys WRT54G, which is burned with an open-source custom-made firmware can act as a wireless sensor to obtain information from data packets within the wireless environment. Service Set Identifier (SSID), Extended Service Set Identifier (ESSID), Received Signal Strength (RSSI), Noise Level, Traffic rate and Traffic Frequency… etc can be collected by a custom-made wireless data acquisition application written for the Linksys WRT54G WLAN router. In particular, the data acquisition application is a cross-compiled program for the 32-bit MIPS architecture processors manufactured by Broadcom, and this embedded piece of software plays an important role to achieve our goals in locating the hacker devices.

In short, we proposed a surveillance system to let the network administrator to monitor and analysis the network traffic and behavior. By making use of multiple wireless routers (Linksys WRT54G) burned with our custom-made cross-compiled program. Useful information is extracted, communications among all wireless devices are sniffed and being stored into our database server at the data centre [35]. With this information, locations of the mobile users can be estimated and suspected hacker's activities can be detected, identified, located and tracked with our WLAN environment.

Since we have to re-program the wireless router for packet sniffering, we have done lots of compatibility test on different open-source wireless routers and test out the feasibility. We found out that most wireless routers are using chipset from two major chipset manufacturers – Atheros and Broadcom.

We found out that for those who had chipset from Atheros, we can make use of the public open-source system call to switch the router into the monitor-mode as well as to the deep-monitor mode which can sniff all Wi-Fi traffic from the air.

On the other hand, for those routers who adopted the chipset from Broadcom, like the Linksys WRT54G, we cannot obtain the correct monitor mode to obtain necessary information for location estimation by using the usual system calls from iwlib.lib, wl.lib, or iwlist.lib… etc. So we have to rewrite the code from the pcap library, the prism library and code from wlioctl [36-38] to extract the Wi-Fi packet one by one in order to obtain the necessary information for location estimation.

Our custom-made program for Linksys WRT54G (AP) thus turned this wireless router into a wireless capture device which requires no authentication or access privileges in order to help us to do security auditing and to estimate the location of the hacker. And thus, we have made the AP to support monitor mode, such that we can disclose and decode the 802.11 frame information.

Wireless measurement can be done at both AP and mobile device level. For mobile device like a notebook, a D-Link PCMCIA Wi-Fi card with Atheros chipset can do the best job in extracting Wi-Fi frame information. Besides, we use the Nokia N96 mobile phone which is running Symbian 3.2 OS, to be programmed to extract the WLAN information. When the mobile device is associated to AP, both sides can obtain the RSSI data from each other, so that the upstream and downstream RSSI value can be obtained simultaneously.

In our system, all the APs sniffed data packets over the channels and each of these packets is being analyzed and stored in our data store. When a mobile user entered our monitoring areas (i.e. the WLAN), the MAC address, Received Signal Strength (RSSI) and relevance information were sniffed by the modified APs. Any data packet in the air will be captured not only by one AP, but also be captured by any APs that can detect and decode these packets.

The value of RSSI and the inter-distance between the mobile device and the AP varies with the inverse square law and is

somehow affected by interference, noise…etc. Indoor positioning technology or the technique for locating a mobile user is the base technology for indoor location-aware computing. In general, there are a large variety of location-based applications and services that rely on an accurate and stable location estimation system such as warehouse management, point-of-interest, infotainment and customer/consumer flow analysis within an enclosed area like a shopping mall or exhibition centre. Such location-based services play a crucial part in enabling e-commerce, and m-commerce, and eventually a critical part to bring the community to the era of ubiquitous/pervasive computing. [39]

Furthermore, at the mobile device, we had tried to formulate a RF signal propagation Loss Model based on the free space loss equation Lp(db)=20*LOG(f)+20*LOG(d)-function(fx) [40], where d is the inter-device distance in meters, f being the carrier frequency in MHz (i.e. at about 2400MHz according to the 802.11 standard due to difference channel), and function(fx) being the signal loss function due to obstacles like office furniture, book shelves and file cabinets. Calibration for function(fx) is needed especially for Multi-path fading and interference.

Thus, in summary, each AP in the WLAN is running a custom-made program to sniff data packet in the open air within the coverage of the WLAN network. Useful information is extracted from these data packets, including MAC address of the mobile device and the signal strength received by the APs are transferred to a control server, and then stored into a database together with the current timestamp for logging purpose. Later on, these data is analyzed by the control server and locations of the mobile users are estimated in real-time by our location estimation algorithm. In this paper, we used the center of gravity algorithm to estimate the mobile location within our test-site.

For better visualization, a program is written such that it will show all the mobile users at their estimated locations within the detectable area of our WLAN network. On the loading of our system, according to the database, less than 300 mobile users and Access Points can be detected and monitored within an hour during the daytime working hours.

4. Experiments and Results

4.1 Experiment 1

Figure 1 shows the layout of APs for Experiment 1 with obscured objects like tables, chairs, bookshelves and benches in a lab of the Research Centre for Ubiquitous Computing (RCUC) at HKBU. During the experiment, our system can detect the presence of about 25 APs. Within the coverage area and we looked into the inter-device distance and the corresponding RSSI under signal attenuation, multipath, reflection, refraction, and signal interferences. Within the WLAN, we obtain signal (data) mainly from three APs, which is BUAP7, BUAP9 and BUMAIN, others APs are just treated as wireless devices. The number in the middle is the distance unit between the AP and the wireless device. For example, distance from BUAP7 to BUAP1 is 3.28m. In this experiment, about 50000 samples were taken for each wireless device. The inter-device distance, that is, the distance between the sender and the receiver, and the received RSSI value is plotted out for investigation.

From Figure 1, BUMAIN and BUSTAFF1 were placed at same location, but only BUMAIN is used to grab packets from the others APs. On the other hand, BUAP7 and BUAP9 were also placed at same location, and both of them were used to grab packets from the other APs. This setup used to demonstrate intra-device error, the error reading on RSSI when the same equipment with the same distance to others APs is used.

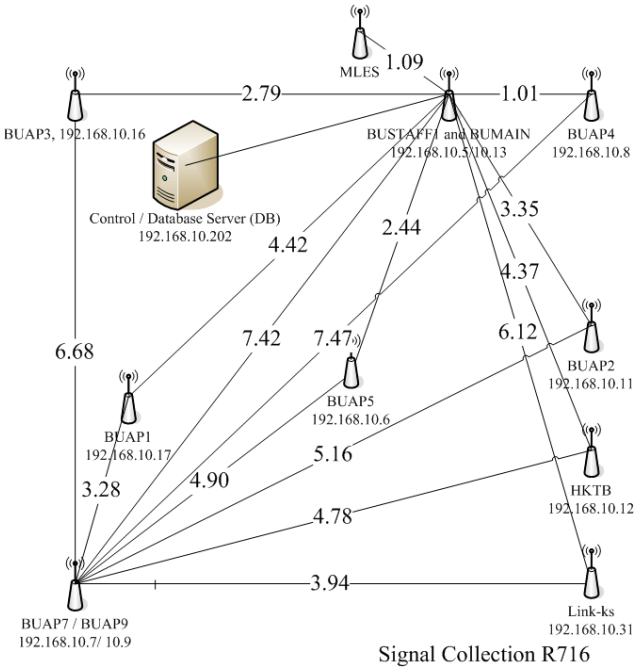

Figure 1. The Setup for Experiment 1 at a Lab in RCUC.

4.2 Experiment 1 Result and Analysis

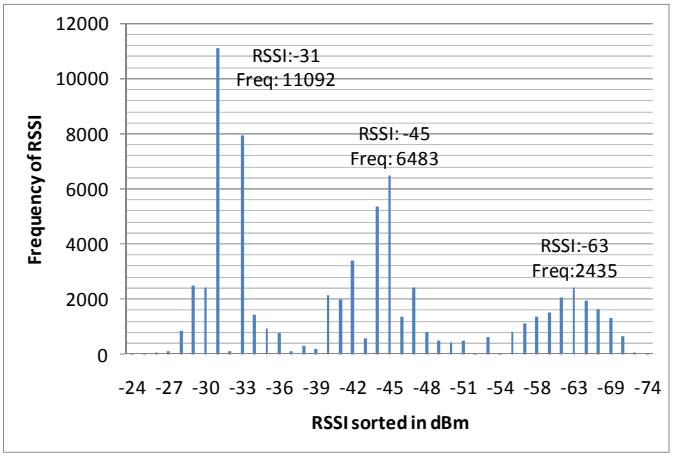

Figure 2. Experiment 1

Figure 2 shows the RSSI received at BUAP1 from BUAP7. The distance between the two routers is fixed at 3.28m. From Figure 2, there is a good indication that three peaks occurred at different RSSI readings, that is, at-32dbm, -45dbm, and -63dbm. This clearly shows that signal transmissions are influenced by multi-path, reflection, refraction, absorption, constructive as well as destructive interferences within this test-site. This raises an important question on how we should relate RSSI readings with the inter-device distance. And thus, we look into the average, the mode and the average of the top 10% readings of the RSSI.

Marker ID	Distance (meter)	Avg. RSSI (dbm)	Mode. RSSI (dbm)	Top 10% (dbm)
BUAP4	1.01	-36.36	-41	-28.08
BUAP5	2.44	-37.94	-37	-31.55
BUAP3	2.79	-42.89	-43	-33.74
BUAP2	3.35	-45.05	-41	-36.49
BUAP1	4.42	-45.53	-43	-37.71
link-ks	6.12	-49.23	-50	-45.4
BUAP7	7.42	-47.31	-43	-41.24
BUAP9	7.42	-49.77	-50	-42.98

Table 1, Sniffer AP at BUMAIN and RSSI Measurements.

Table 1 and Figure 3 show the signal strength data (RSSI) and a plot of RSSI against different inter-device distance. From Figure 3, all three curves show some fluctuations of signals across the range of inter-device distances. The curve on the "Mode of RSSI" fluctuates the most, followed by the curve with the "Average RSSI", and the Top 10% RSSI curve shown to be most stable, except the point at 6.12m where all three measurements do not follow its own trend. We highly suspected that there are strong destructive interference of signals at this marker. Anyhow, we find out that the Top 10% RSSI readings is a good indicator for the RSSI readings against the inter-device distances between the sender and receiver.

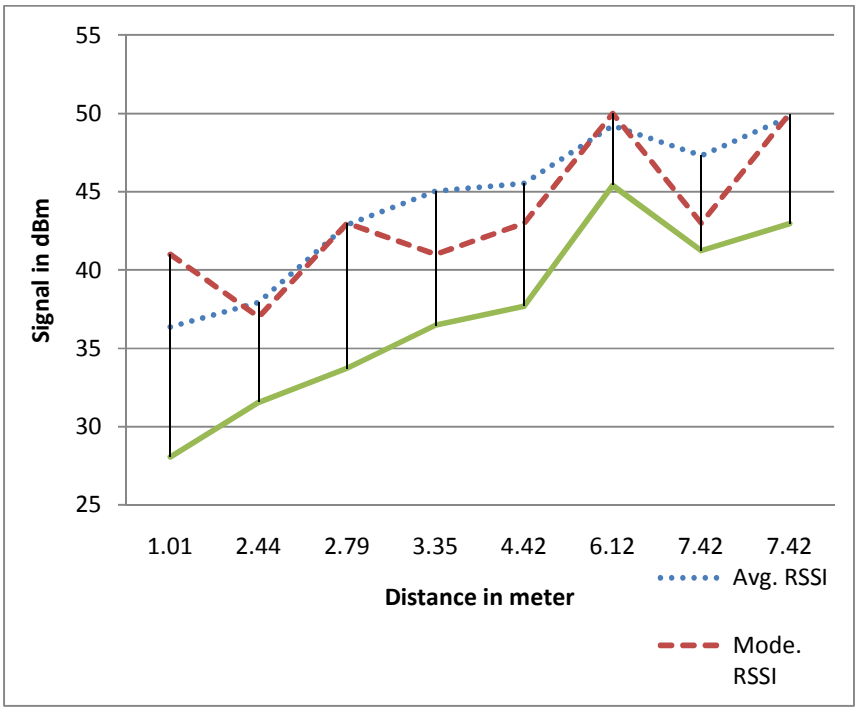

Figure 3. Sniffer AP at BUMAIN, RSSI Measurements vs. Inter-device Distances.

Marker ID	Distance	Avg. RSSI			Mode. RSSI			Top 10%		
		BUAP7	BUAP9	%Diff	BUAP7	BUAP9	%Diff	BUAP7	BUAP9	%Diff
BUAP9	0	-24.37	-21.00	16%	-18	-25.42	29%	-12.28	-11.80	-4%
BUAP1	3.28	-43.13	-40.23	7%	-31	-31	0%	-29.43	-28.20	-4%
link-ks	3.94	-47.86	-50.92	-6%	-38	-39	3%	-34.78	-37.72	8%
BUAP5	4.90	-41.84	-39.10	7%	-34	-34	0%	-32.25	-28.71	-12%
BUAP2	5.16	-47.71	-42.78	12%	-42	-34	-24%	-38.96	-31.84	-22%
BUAP3	6.68	-44.80	-50.61	-11%	-50	-45	-11%	-35.47	-42.50	17%
BUMAIN	7.42	-49.78	-48.65	2%	-53	-45	-18%	-41.57	-42.88	3%
BUSTAFF1	7.42	-50.67	-47.92	6%	-51	-45	-13%	-44.62	-40.67	-10%
BUAP4	7.47	-47.42	-46.20	3%	-42	-43	2%	-38.22	-36.97	-3%
			Average	4.00%		Average	-3.56%		Average	-3.00%

Table 2. Sniffer AP at BUAP7/BUAP9, RSSI Measurements vs. Inter-device Distances.

Table 2 shows the intra-device discrepancy on receiving signals. Signals are collected by both BUAP7 and BUAP9 where they are located at the same position during the experiment. Table 2 shows that of the three methods in measuring the RSSI readings, the top 10% RSSI reading produces the smallest differences with an average difference at -3.00%. And thus, Experiment 1 has shown that multi-path and interferences do exist and affect the signal readings and that we should use the "Top 10% RSSI" readings for estimating the inter-device distance between sender and receiver and the average differences in RSSI readings between two wireless routers varies between -3.56% to 4%

4.3 Experiment 2

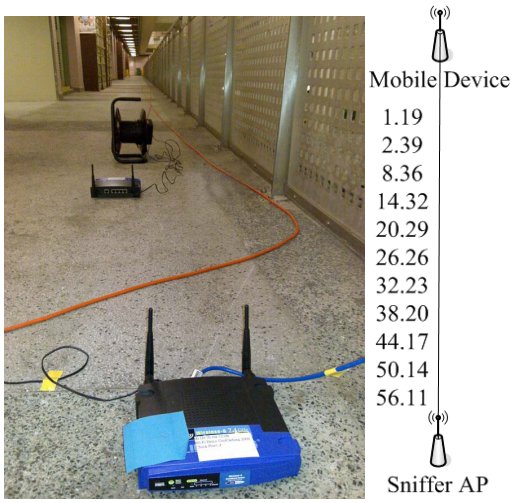

Figure 4. Signal Attenuation along a corridor.

Figure 4 shows the setup for Experiment 2 - the investigation on signal attenuation and distance between mobile devices in a semi-outdoor environment (outside corridor). Only 4 APs are used and we marked down 11 markers along a straight line. At each marker position, that is at positions shown below (1.19, 2.39, 8.36, 14.32, 20.29, 26.26, 32.23, 38.20, 44.17, 50.14, 56.11). 100 Samples are collected for our later analysis.

4.4 Experiment 2 Result and Analysis

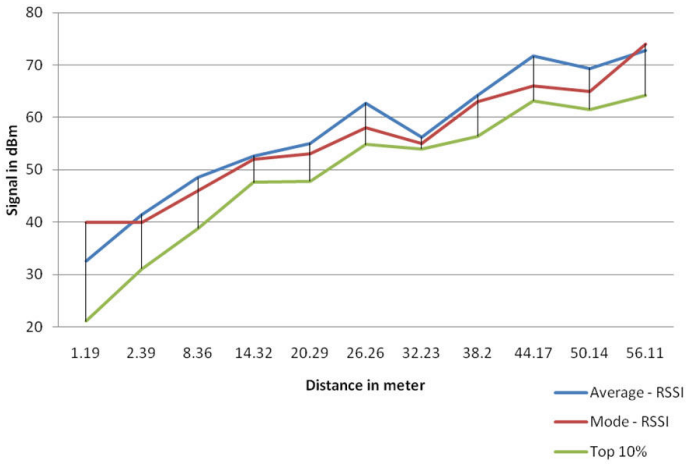

Figure 5. RSSI vs. Inter-device Distances in Experiment 2.

Unlike Experiment 1 which is conducted in an enclosed area, Experiment 2 is an investigation on the signal readings in a semi-open area – an open corridor outside our lab. When comparing Figure 3 and Figure 5, signals from Figure 5 (i.e. Experiment 2) are less fluctuating and more stable. There is a nice correlation between signal strength and inter-device distance indicating that a strong signal relates to a shorter inter-device distance and a weak signal correlates to a longer inter-device distance. Furthermore, there is no good indication of multi-path and interferences of signals throughout the range of distances in the experiment which varies from 1.1m to 56.11m. This range of distance is much wider than that in our Experiment 1.

Distance in meter	Average - RSSI	Mode - RSSI	Top 10%
1.19	-32.59	-40	-21.1
2.39	-41.49	-40	-31.1
8.36	-48.50	-46	-38.8
14.32	-52.66	-52	-47.6
20.29	-55.07	-53	-47.8
26.26	-62.72	-58	-54.8
32.23	-56.23	-55	-54.0
38.2	-64.28	-63	-56.4
44.17	-71.73	-66	-63.2
50.14	-69.38	-65	-61.5
56.11	-72.82	-74	-64.2

Table 3. RSSI Measurements and Inter-device Distances in a semi-outdoor environment.

Table 3 shows the three proposed methods in measuring the RSSI, and similar to what is observed in Experiment 1 (Table 1), the Top 10% RSSI reading is the best among the three indicators for estimating the inter-device distance between the sender and receiver based on RSSI in this experiment.

4.5 Experiment 3

Figure 6 shows a similar experiment setup as in Experiment 1. It is used to demonstrate the accuracy of a location estimation method called Center of Gravity (CG). In this experiment, the distance between AP1 and AP3 is 6.68m, and the distance between AP1 and AP2 is 3.94m. Under the CG algorithm, the (x,y) co-ordinates are calculated as follows:

$$x = \frac{x_1 s_1^{-b} + x_2 s_2^{-b} + x_3 s_3^{-b} + \ldots + x_n s_n^{-b}}{s_1^{-b} + s_2^{-b} + s_3^{-b} + \ldots s_n^{-b}}$$

$$y = \frac{y_1 s_1^{-b} + y_2 s_2^{-b} + y_3 s_3^{-b} + \ldots + y_n s_n^{-b}}{s_1^{-b} + s_2^{-b} + s_3^{-b} + \ldots s_n^{-b}}$$

where (x,y) is the estimated location of the mobile user, (x_1,y_1), $(x_2,y_2),\ldots,(x_n,y_n)$ are the locations of n receiving APs, and $s_1,s_2,s_3\ldots,s_n$ are the corresponding RSSI from each AP. The CG

algorithm has proven to be very effective and can provide outstanding performance in metropolitan area during our mobile location estimation experiments using the mobile phone network. However, the down side is that it can only estimate a mobile device inside the convex hull as defined by the APs involved.

4.6 Experiment 3 Result and Analysis

For Experiment 3, we assume a mobile user is carrying a wireless device and is performing some hacker's activities. Nine marker positions are defined and the mobile user will visit each marker in turn and signal information from the handheld device will be collected through the four access points - AP1, AP2, AP3, and AP4 as indicating in Figure 6.

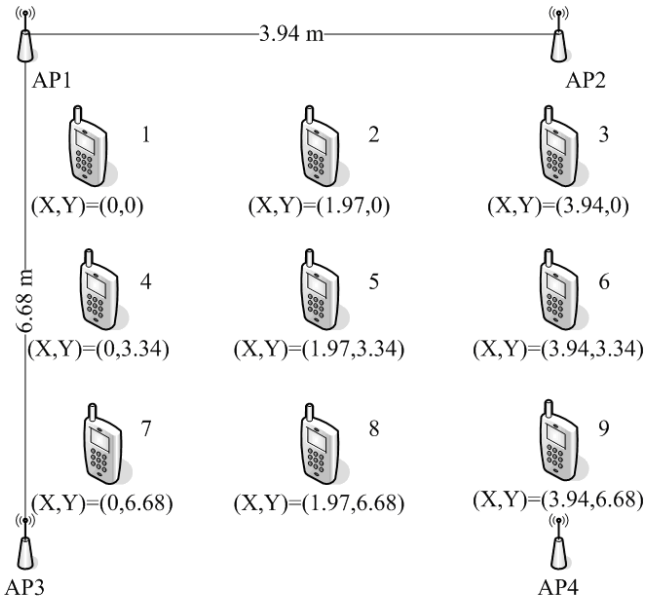

Figure 6. Localization of mobile devices within a lab in RCUC.

Marker ID	Actual Position (X,Y)		Estimated Position (X,Y)		Error in meter
	x	y	x	y	
1	0.00	0.00	0.45	0.70	0.83
2	1.97	0.00	1.70	3.27	3.28
3	3.94	0.00	2.94	1.25	1.60
4	0.00	3.34	2.04	2.66	2.15
5	1.97	3.34	2.09	3.29	0.13
6	3.94	3.34	1.78	2.47	2.33
7	0.00	6.68	0.86	5.21	1.71
8	1.97	6.68	2.34	3.91	2.80
9	3.94	6.68	2.57	4.44	2.63

Table 4. Accuracy of the CG localization algorithm.

Knowing the physical location and coordinates of the four APs, and together with the signal information collected through these four APs, we will use the "Center of Gravity" location method to estimate the mobile user's location. Table 4 shows the actual positions of the nine markers as well as the estimated location of the mobile user at the corresponding marker. With the actual position and the estimated position of the mobile user, the relative error is calculated and listed in Table 4.

One can observe that the error in meter ranged from 0.13m at Marker 5 to 3.28m at Marker 2. The system can estimate the hacker's position when it is near the centroid of the WLAN network, and the accuracy deteriorates towards the rim of the convex hull as defined by the four access points.

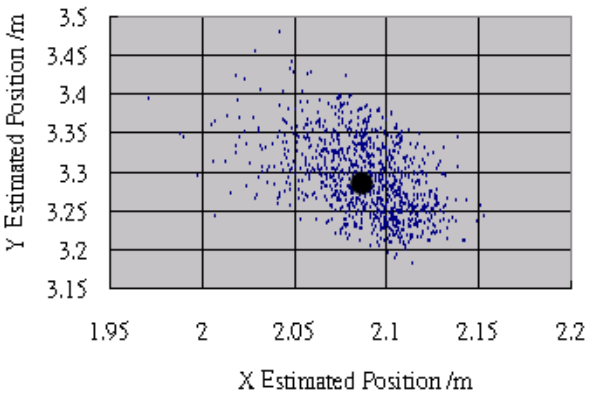

Figure 7, Marker #5 at (1.97,3.34)

Figure 7 shows the plot of the estimated position at various time instances at Marker 5 (1.97, 3.34). The plot itself shows the accuracy as well as the distribution of the estimated positions by the "Center of Gravity" algorithm with respect to the actual position of the mobile user at Marker 5. And the overall average error for the CG algorithm is 0.13m as shown in Table 4.

5. Conclusion and Future Work

The goal of the proposed project is to investigate the feasibility of using the WLAN to locate a mobile user as well as locating and tracking hacking activities in an indoor environment to enhance information security and to enable location-aware computing.

In the future, we are going to enhance the existing signal strength based location estimation methods for indoor location estimation base on the method we have done on our previous research paper, such as integrates two or more location estimation methods, and make use of RSSI collected from mobile terminals and/or from base-stations (WLAN access points) for a more stable location estimation. By the way, in order to use the Multi-fingerprinting method to nullify the body effect, we need to investigate how signals are collected, organized & stored, recognized & retrieved from location server and to reduce the cost of data acquisition and the cost of maintaining the signal data in the database up to date. Furthermore, we have to study and provide practical solutions for locating and tracking hackers' activities within the wireless network, and to investigate the feasibility and practicality of integrating our methods into the GovWiFi project so as to provide location based services and extra security services for better location-aware computing in Hong Kong. With such a development platform, application builders can develop numerous location based services and applications ranging from warehouse and resource management, indoor workers deployments, infotainment, and personal safety

Finally, we are entering a new era of computing – the era of ubiquitous/pervasive computing where we can retrieve any data

from any device using any network at anytime and any place, and this is the technology that will bring us a step closer to a more secure and more convenient ubiquitous computing society!

6. References

[1] "Hong Kong Government's Digital 21 Strategy" at http://www.info.gov.hk/digital21/eng/index.htm

[2] "Government Wi-Fi Programme (GovWiFi)" at http://www.gov.hk/en/theme/wifi/program/index.htm

[3] "Linksys WRT54G series" at http://en.wikipedia.org/wiki/Linksys

[4] T. King, S. Kopf, T. Haenselmann, C. Lubberger, and W. Effelsberg, COMPASS: A Probabilistic Indoor Positioning System Based on 802.11 and Digital Compasses, in Proc. The First International Workshop on Wireless Network Testbeds, Experimental Evaluation & Characterization(WiNTECH 06) , pp. 34-40, Sep. 2006.

[5] "Open Source Fireware for Access Point" at http://www.opertwrt.org

[6] William H. Wong, Joseph K. Ng, and Wilson M. Yeung, "Wireless LAN Positioning with Mobile Devices in a Library Environment", Proceedings of ICDCS-MDC 2005 Workshop, pp. 633-636, June 6-10, 2005, Columbus, Ohio, USA.

[7] Zhili Wu, Chun-hung Li, Joseph K. Ng, "Improvements to RADAR Location Classification", in Proceedings of the 2008 International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM 2008)

[8] Joseph K. Ng, Junyang Zhou, Kenneth M. Chu, and Karl R.P.H Leung, "A Train-Once Approach for Location Estimation using the Directional Propagation Model (DPM)", IEEE Transactions on Vehicular Technology, 57(4), pp. 2242-2256, July 2008.

[9] Junyang Zhou, Wilson M. Yeung and Joseph K. Ng, "Enhancing Indoor Positioning Accuracy by utilizing signals from both the mobile phone network and the Wireless Local Area Network", in Proceedings of the IEEE 22nd International Conference on Advanced Information Networking and Applications (AINA 2008), pp 138-145, March 25-28, 2008, GinoWan, Okinawa, Japan. IEEE Computer Society Press.

[10] Wilson M. Yeung, Junyang Zhou and Joseph K. Ng, "Enhanced Fingerprint-based Location Estimation System in Wireless LAN Environment", in Proceedings of the 1st International Workshop on System and Software for Wireless SoC (WSOC 2007), pp 273-284, December 17-20, 2007, Taipei, Taiwan, Springer.

[11] Wilson M. Yeung and Joseph K. Ng, "Wireless LAN Positioning based on Received Signal Strength from Mobile device and Access Points", in Proceedings of the 13th International Conference on Embedded and Real- Time Computing Systems and Applications (RTCSA 2007), pp. 131-137, August 21-23, 2007, Daegu, Korea 2007, IEEE Computer Society Press.

[12] Wilson M. Yeung, and Joseph K. Ng, "An Enhanced Wireless LAN Positioning Algorithm based on the Fingerprint Approach", Proceedings of IEEE TENCON 2006, IEEE CS Press, 14-17 November 2006, Hong Kong, China.

[13] Kenneth M. Chu, Karl R. Leung, Joseph K. Ng, Chun Hung Li, "A Directional Propagation Model for Locating Mobile Stations within a Mobile Phone Network", International Journal of Wireless and Mobile Computing (IJWMC): Special Issue on Applications, Services and Infrastructure for Wireless and Mobile Computing, 3(1/2) pp. 12-21, August 2008, Inderscience.

[14] William H. Wong, Joseph K. Ng, and Karl R.P.H. Leung, "Large-Scale Location Estimation over GSM networks: the GEAR Approach", Proceedings of the 24th IEEE International Conference on Distributed Computing Systems Workshops (ICDCS-MDC 2004), pp. 574 --- 579, March 23-26, 2004, Hachioji, Tokyo, Japan.

[15] William H. Wong, Joseph K. Ng, and Karl R.P.H. Leung, "Large-Scale Location Estimation over GSM networks: the Gear Approach", to appear in International Journal of Wireless and Mobile Computing.

[16] Zhi-li Wu, Chun-hung Li, Joseph K. Ng, and Karl R.P.H. Leung, "Location Estimation via Support Vector Kernel Regression", IEEE Transactions on Mobile Computing, Vol. 6, No. 3, pp. 311-321, March 2007.

[17] P. Bahl and V.N. Padmanabhan, “RADAR: An in-building RF-based user location and tracking system”, in Proceedings of INFOCOM 2000, (2): 775-784. Available online at citeseer.ist.psu.edu/bahl00radar.html

[18] Junyang Zhou, Enhanced Signal Propagation Models and Algorithm Selector for Providing Location Estimation Services within Cellular Radio Networks, Hong Kong Baptist University 2007

[19] Melvyn Wong and Joseph K. Ng, "Fleet Management System", Innovation and Technology Fund (UIM), Innovation and Technology Comission, HKSAR Government.

[20] Duncan Lau, Joseph Ng, Karl Leung, Lawrence Cheung, "Develop an accurate low-cost Mobile Location Estimation System (MLES) for fleet management applications using existing mobile phone infrastructure ", Innovation and Technology Fund (ITSP), Innovation and Technology Comission, HKSAR Government.

[21] Stephen K. Chan, Kenny K. Kan, and Joseph K. Ng, "A Dual-Channel System for Providing Location Estimation in Mobile Computing", Journal of Interconnection Networks (JOIN), Volume 4, Number 3, pp. 271 --- 290, September 2003, World Scientific Publishing Company.

[22] Kenny K.H. Kan, Stephen K.C. Chan, and Joseph K. Ng, "A Dual-Channel Location Estimation System for providing Location Services based on the GPS and GSM Networks", Proceedings of The 17th International Conference on Advanced Information Networking and Applications (AINA 2003), pp. 7 - 12, March 27-29, 2003, Xi'an, China.

[23] Joseph K. Ng, Stephen K. Chan, and Kenny K. Kan, "Location Estimation Algorithms for Providing Location Services within a Metropolitan Area based on a Mobile Phone Network", Proceedings of the 5th International Workshop on Mobility Databases and Distributed Systems (MDDS 2002), pp. 710 --- 715, Aix-en-Provence, France, September 2-6, 2002

[24] Karl R.P.H. Leung, Joseph K. Ng, Tim K. Chan, Kenneth M. Chu, and Chung Hung Li, "Network Based Mobile Station Positioning in Metropolitan Area", Proceedings of the International Conference on Parallel and Distributed Computing (Euro-Par 2003), pp. 1017 --- 1026, Springer-Verlag, August 26-29, 2003, Klagenfurt, Austria.

[25] Ka Ho Kan, "Location Estimation System Based on the GSM Network", M.Phil. Thesis, Hong Kong Baptist University 2004.

[26] Kenneth M. Chu, Karl R.P.H. Leung, Joseph K. Ng, and Chun H. Li, "Locating Mobile Stations with Statistical

Directional Propagation Model", Proceedings of the 18th International Conference on Advanced Information Networking and Applications (AINA 2004), pp. 230 --- 235, March 29-31, 2004, Fukuoka, Japan.
[27] Kenneth M. Chu, Karl R. Leung, Joseph K. Ng, Chun Hung Li, "A Directional Propagation Model for Locating Mobile Stations within a Mobile Phone Network", International Journal of Wireless and Mobile Computing (IJWMC): Special Issue on Applications, Services and Infrastructure for Wireless and Mobile Computing, 3(1/2) pp. 12-21, August 2008, Inderscience.
[28] William H. Wong, Joseph K. Ng, and Karl R.P.H. Leung, "Large-Scale Location Estimation over GSM networks: the GEAR Approach", Proceedings of the 24th IEEE International Conference on Distributed Computing Systems Workshops (ICDCS-MDC 2004), pp. 574 --- 579, March 23-26, 2004, Hachioji, Tokyo, Japan.
[29] William H. Wong, Joseph K. Ng, and Karl R.P.H. Leung, "Large-Scale Location Estimation over GSM networks: the Gear Approach", to appear in International Journal of Wireless and Mobile Computing.
[30] Zhi-li Wu, Chun-hung Li, Joseph K. Ng, and Karl R.P.H. Leung, "Location Estimation via Support Vector Kernel Regression", IEEE Transactions on Mobile Computing, Vol. 6, No. 3, pp. 311-321, March 2007.
[31] Y. Wang, X. Jia, H.K. Lee, and G.Y. Li, "An indoor wireless positioning system based on wireless local area network infrastructure", Proceedings of the 6th International Symposium on Satellite Navigation Technology Including Mobile Positioning & Location Services (SatNav 2003), Melbourne, Australia, 22-25 July 2003.
[32] P. Bahl and V.N. Padmanabhan, “RADAR: An in-building RF-based user location and tracking system”, in Proceedings of INFOCOM 2000, (2): 775-784. Available online at citeseer.ist.psu.edu/bahl00radar.html
[33] P. Krishnan, A.S. Krishnakumar, W.-H. Ju, C. Mallows, and S. Ganu, “A system for LEASE: Location estimation assisted by stationary emitters for indoor RF wireless networks”, in Proceedings of INFOCOM 2004, 2004.
[34] S. Ganu, A.S. Krishnakumar, and P. Krishnan, “Infrastructure-based location estimation in WLAN networks”, in Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC 2004), 2004.
[35] Wilson M. Yeung, Wireless LAN Positioning in Indoor Environment, Hong Kong Baptist University 2007
[36] "Broadcom 802.11abg Networking Device Driver" at https://dev.openwrt.org/browser/trunk/openwrt/package/openwrt/include/wlioctl.h?rev=375,
[37] "pcapsource from Kismet" at http://www.google.com.hk/codesearch/p?hl=zh-TW#ACmMdBt9LZs/Firmware_Alchemy-pre5.4a.src.by.TheIndividual.tar.bz2|g0iVX931-Yk/Firmware_Alchemy-pre5_4/src/router/kismet/pcapsource.cc&q=WLC_GET_MONITOR
[38] "Partial driver for WAVELAN" at http://www.google.com.hk/codesearch/p?hl=zh-TW#p-OcbD5DbwM/packages/1.2/kernel/patches/49-3rdparty/MC16_vt_ar5k-20030509.tar|xlsugco9EAs/3rdparty/vt_ar5k/include/vt_wlan.h&q=prism_hdr_t
[39] Junyang Zhou, Kenneth M. Chu, and Joseph K. Ng, "An Improved Ellipse Propagation Model for Location Estimation in facilitating Ubiquitous Computing", Proceedings of the 11th International Conference on Embedded and Real-Time Computing Systems and Applications (RTCSA 2005), pp. 463-466, August 17-19, 2005, Hong Kong.
[40] Junyang Zhou, Enhanced Signal Propagation Models and Algorithm Selector for Providing Location Estimation Services within Cellular Radio Networks, Hong Kong Baptist University 2007