Report on

Wireless LAN War Driving Survey 2004-05

Hong Kong

Version 1.0

Apr-2005

Organizers

Professional Information Security Association

(PISA)

專業資訊保安協會

Hong Kong Wireless Technology Industry Association

(WTIA)

香港無線科技商會

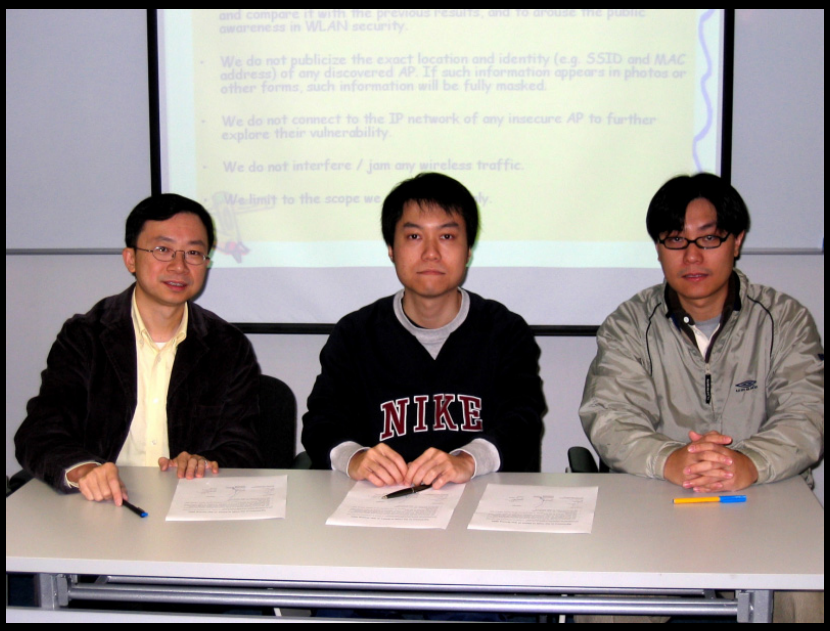
Copyright

Disclaimer

This report is to provide information on WLAN security status and risks in Hong Kong. It should not be used for malicious intent. Unauthorized Access to computer system is an offense. The author takes no liability to any act of the user or damage caused in making use of this report.

The points made here are kept concise for the purpose of presentation. If you require details of test and implementation please refer to other technical references.

Photos



Signing of the Code of Ethics (C.O.E back projected)

[From left]: Ken Fong (WTIA), Jeff Chung (e-Zone), Alan Tam (PISA)

War Tramway Team before start of survey

[Back row from left]: Dennis Kwong (WTIA), SC Leung (PISA), Jeffrey Wong (WITA), Eric Leung (WTIA)

[Middle row from left]: Ken Fong (WTIA), Alan Ho (PISA), Jim Shek (PISA), Marco Ho (PISA)

[Front row from left]: Kelvin Lee (WITA), Alan Tam (PISA)

Photos

War Driving is possible with simple equipment like a notebook computer or even a PDA (an iPAQ shown running Kismet on linux)**.**

War Tramming with antenna

[From left]: Ken (WTIA) with +12dB antenna and Jim (PISA) with +5dB antenna

Photos

The War Sailing Team with gears at the Cruise Pier (Tsimshatsui)
[back row from left]: Alan Ho, Johnway Ip. Clayton Check, S.C. Leung
[front row from left]: Ken Fong, Sang Young, Kelvin Lee, Jim Shek, Alan Tam, Eric Leung

Looking at a similar passenger ferry from TST Cruise Ferry Pier
(The background was the International Financial Centre II of Hong Kong Island at sunset.)

Photos

Setting up the equipments at the front deck of the Cruise Ferry
(Cruise Ferry was modified from a passenger ferry with ceilings at front deck and stern removed)

War Sailing in the scenic Victoria Harbour on a sunny day
(Clayton was holding a +12dB planar antenna. The background was West Kowloon.)

Terms used

WLAN	Wireless Local Area Network. There are three popular standards now: • 802.11a: using 5GHz, 54Mbps • 802.11b: using 2.4GHz, 11Mbps (most popular) • 802.11g: using 2.4GHz, 54Mbps
War Driving	Collecting wireless LAN information including network name, signal strength, location by using a device capable of WLAN signal receiver and moving from one place to another.
GPS	GPS stands for Global Positioning System. It is a "constellation" of 24 well-spaced satellites that orbit the Earth and make it possible for people with ground receivers to pinpoint their geographic location. The GPS is owned and operated by the U.S. Department of Defense but is available for general use around the world.

AP	Access Point. A device that serves as a communications "hub" for wireless clients
MAC	Media Access Control address. The physical address of a Wireless LAN card
SNR	Signal-to-Noise Ratio. A measurement of signal strength versus noise.
SSID	Service Set Identifier. The identifier name of each wireless LAN network
WEP	Wired Equivalent Privacy. An encryption protocol in using WLAN
WPA	Wireless Protected Access. An improved encryption protocol over WEP in using WLAN

Executive Summary

In Dec 2004, the two associations **PISA** and **WTIA** jointly conducted the "War Driving 2004" field survey along the classic tramway of Hong Kong Island and around the scenic Victoria Harbour. The objective of the survey was to conduct a non-intrusive study on the status of Hong Kong WLAN security and arouse the public awareness in securing the use of WLAN.

The field survey was very successful. The results were benchmarked against that of two previous studies conducted by PISA in 2002, and by PISA & WTIA in 2003 to plot the profile of Hong Kong WLAN security development. The survey indicated that the number of WLAN implementation had skyrocketed in the past two years, and yet there was some improvement in the adoption of security strategies. The number of discovered APs had notably **increased by** 120**%** while the percentage of improved security on the whole was only a few percents.

The result of the survey also proved that it was feasible to war drive from distances in the order of kilometres. With a high gain antenna, over 1000 APs was discovered along the Victoria Harbour. We were able to connect to an authorized access point up in a tall building in Admiralty from a distant point in the sea. The possibility of war driving at such distance and height was out of the imagination of many people.

GPS has been used to conduct this survey this year. It can let us know how many APs and its security characterizes by granular location.

The study was carried out in a non-intrusive and responsible way. The information of individual vulnerable AP was not disclosed.

PISA and **WTIA** share a common vision in promoting the use of wireless network in a productive and secure manner. They call for the public awareness of the problem. They would follow up the findings with educational programs to promote the adoption of WLAN security strategies.

Introduction

In 2002, a team of **PISA** investigators performed the city's 1st "War Driving" study on the Wireless LAN Security Flaws in Hong Kong. It had aroused the public and corporations awareness to tighten their WLAN security loopholes. In Oct 2003, **PISA** and **WTIA** jointly conducted the 2nd "War Driving". The scope of test was extended to

- the whole tram way, covering the business corridor of the HK Island
- lookouts at the Victoria Peak, covering far-away signal of the HK Island north and the Kowloon Peninsula, at an bird-eye view

In Nov 2004, **PISA** and **WTIA** conducted the 3rd "War Driving" again to benchmark the improvement for the WLAN Security in Hong Kong. Some new ideas of the 2004 war driving include:

- touring on boat in the Victoria Harbour, covering the both side of HK Island and Kowloon at the sea level
- making a real-life connection to an authorized access point in the middle of Victoria Harbour
- using GPS in locating position and mapping of path

Objectives of Study

1. To study the current WLAN security status of Hong Kong and to benchmark the result with that of the previous year
2. To study the feasibility of long distance war driving and its impact to WLAN security
3. To conduct a non-intrusive* information security study with responsible disclosure of information
4. To arouse the public awareness in WLAN security and follow up with education program

** The study involved neither sniffing of data nor jamming of network traffic. The tool used was mainly for discovery of wireless network broadcasted signals. No association with access point, no network connection was attempted during the war driving study. Please see Code of Ethics below.*

Code of Ethics

The organizers and the reporter agreed on the following points to the study to take care of the security and privacy issues.

- Our objective of the War Driving is to study the WLAN security status and compare it with the previous results, and to arouse the public awareness in WLAN security.
- We do not publicize the exact location and identity (e.g. SSID and MAC address) of any discovered AP. If such information appears in photos or other forms, such information will be fully masked.
- We do not connect to the IP network of any insecure AP to further explore their vulnerability.
- We do not interfere / jam any wireless traffic.
- We limit to the scope we state above only.

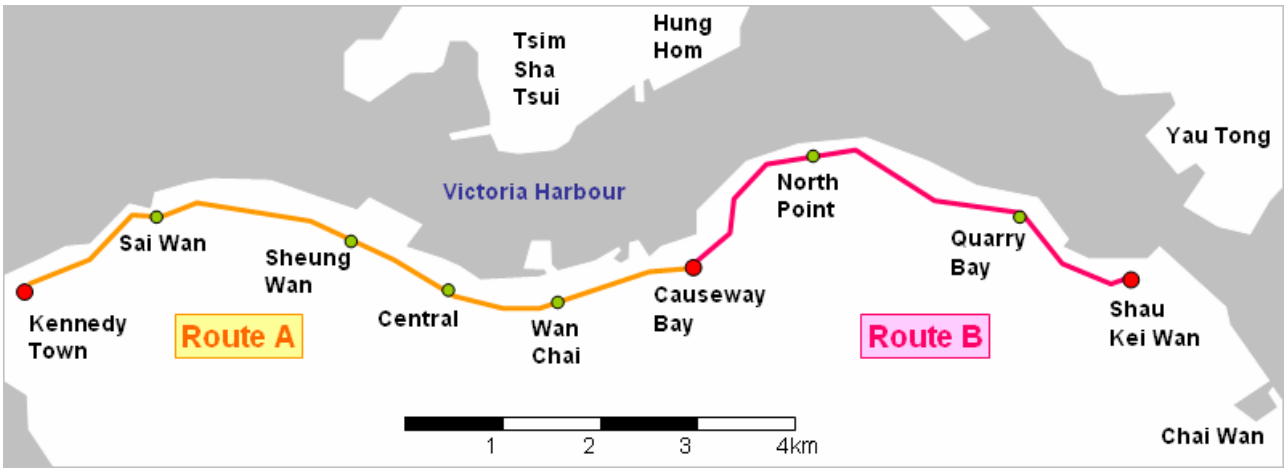
Methodology and Equipment

The War Driving was divided into 2 parts: ***War Tramming*** and ***War Sailing***.

Part I: War Tramming (War Driving along Tramway)

- Tram is only available in a handful of cities around the world and tram riding is a popular activity of tourists in Hong Kong.
- War Driving on a tram had been proved to be a very effective way because trams run at a moderate speed (30-50km/h) in the middle of the road, allowing very good coverage of signals from the both sides of the road.
- By War Driving on a tram, we targeted to benchmark the results with that of the war driving study of year 2002 and 2003 along the tramway from Kennedy Town to Causeway Bay (Route A).
- We also benchmarked the results with that of the war driving study of year 2003 along the tramway from Kennedy Town to Shau Kei Wan. This route was equivalent to the whole business corridor of Hong Kong Island. (Route B).

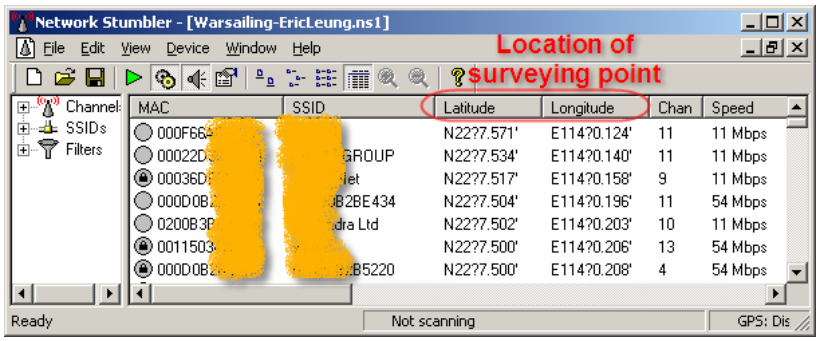
Date:	28-Nov-2004 (Sunday)
Time:	11 am -3 pm
Equipment:	*Hardware:* Notebook computers, WLAN cards and various +5dB omni-directional antennae *Software:* Netstumbler
Route:	• Route A: ○ Taking tram from Queensway, Admiralty westwards to Kennedy Town terminus, then return tram from Kennedy Town terminus to Sogo Department Store, Causeway Bay (this was the same route as in War Driving 2002 and 2003) • Route B: ○ Taking another tram from Causeway Bay to Shau Kei Wan terminus (this was the same route as in War Driving 2003)



Part II: War Sailing (War Driving in Victoria Harbour)

- In 2003, the War Driving Team did a war driving from the Victoria Peak at an altitude of 554m, overseeing the Hong Kong Island north coast and the whole Kowloon Peninsula. This year, we changed to a more “down-to-earth” path – touring on a tourist cruise ferry around the scenic Victoria Harbour which is again a popular tourist attraction.
- War Sailing allowed a survey at sea-level of access point which faced the harbour. Since the clearance at the middle of the harbour to the business buildings along the sea-side is excellent, and the distance between the WLAN Access Points (APs) and the WLAN client was smaller than that from the Victoria Peak, it presented a good opportunity to conduct a real life **Connection Test**. We had arranged an AP in an office building in the Admiralty for such test. Some of our team members were authorized to connect to that specific AP. We did not attempt any other connection other than the authorized AP because unauthorized connection is neither ethical nor legal.
- The team also tried to use Global Positioning System (GPS) to plot the path of war sailing. Mapping was very popular in field surveying and well integrated into war driving studies around the world. Sailing in the harbour provided an excellent opportunity for the GPS to locate 3 satellites to calibrate the positions. Several points were taken as triangular reference points for calibrating the map and to locate the ferry route. With the mapping software for war driving, we can track the concentration of and strength of WLAN signals along the coast of the harbour.

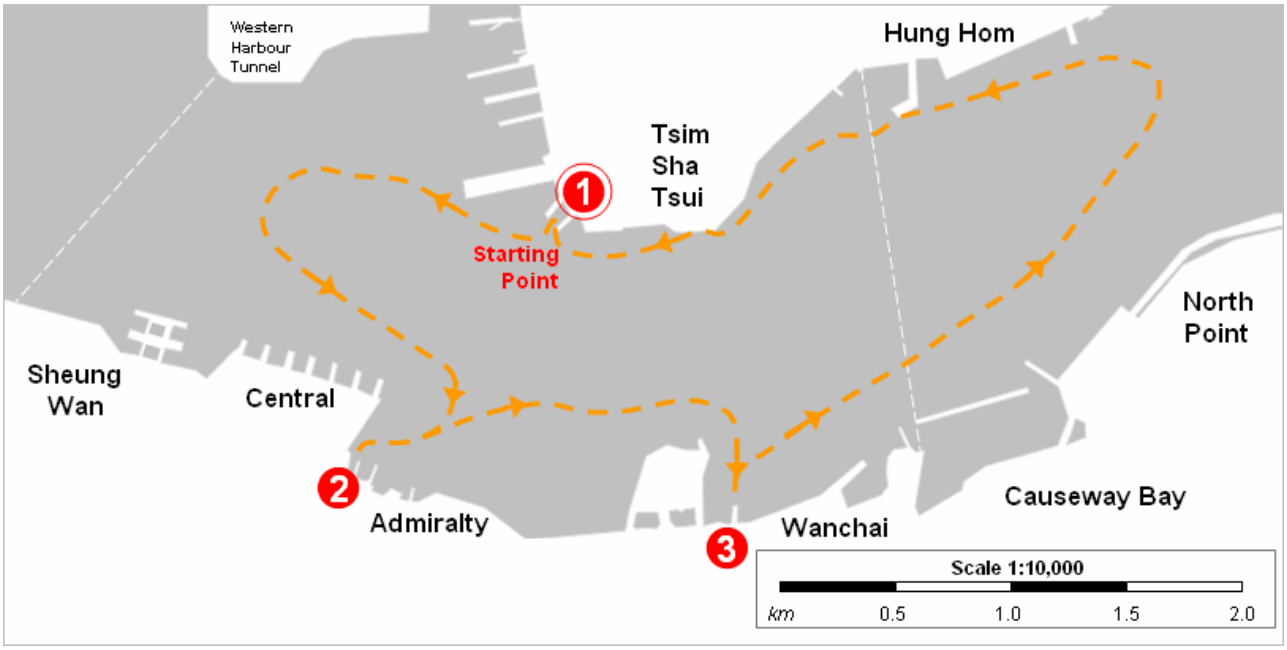
Handheld Global Positioning System



Netstumbler log showing the latitude and longitude of surveying points along the war driving path. The data was fed in by a GPS device connected to the PC.

Date:	09-Jan-2005 (Sunday)
Time:	11 am -3 pm
Equipment:	Same as "War Tramming", except that different antenna were used - +12dB planar antenna with 60° beam angle sensitivity for major mapping - + 8dB omni-directional antenna for connection test - + 5dB omni-directional antenna for control experiment - broadband horn narrow angle (45° beam angle sensitivity) antenna for control experiment (+7.9dB for 2.4GHz and +9.5dB for 5GHz) - null antenna for control experiment Mapping equipment - GPS device (serial/USB) - WLAN field work mapping software

- Arrangement of the War Sailing Route
  - We took a commercial Cruise Ferry for tourist sight-seeing in the harbour to conduct the War Sailing. The route of the cruise is a circular trip shown below. It started from Tsimshatsui (TST) Pier, going westward to West Kowloon. Then it headed southwards towards Sheung Wan of Hong Kong Island. When it came near Sheung Wan, it went eastwards. After stopping at Central Pier to pick passengers, it continued to go eastward towards North Point. At Wan Chai Pier was an optional stop. When the ferry reached North Point, it headed northwards towards Hung Hom Pier of Kowloon (where there was another optional stop). Finally it returned to TST.



Round trip route of Cruise Ferry starting at TST Pier

- We chose three points along the Victoria Harbour which were distant apart enough as the triangular references for the calibration of map. They are: ① TST Pier (starting point), ② Central Pier, and ③ Wanchai Pier.
- **There are several advantages of such Cruise Ferry arrangement for War Sailing**
  - The one hour round trip costs only HKD35, very affordable for amateur field survey. We needed to take 2 trips to gather sufficient data.
  - The route of the round trip had covered the central business area of HK Island and Kowloon peninsula.
  - The ferry was running at moderate speed so very suitable for war driving data collection which needs sufficient time to scanning all the channels of an AP.
  - Since the ferry was designed for sight-seeing, the stern and front deck ceilings were removed. It was excellent for GPS to locate the satellites.
- On the other hand, the **disadvantage of the Cruise Ferry arrangement for War Sailing is** that the eastern end of the round trip was North Point. Major IT office and residential areas at the further eastern ends, like Quarry Bay and Taikooshing, were not covered.

Findings and Analysis

Part I: War-Tramming (Tramway War Driving)

Note: the war tramming statistics below was generated by the consolidated log from war drivers with antenna having gain of +5dB or below.

1. Number of Access Points Captured

Locations	Number of unique Access Points captured
Route A: Tramway, from Kennedy Town to Causeway Bay	926
Route A + B: Tramway, from Kennedy Town to Shau Kei Wan	1723

2. Overall the implementation of 802.11g in Hong Kong was around 15%.

Route A: Tramway, from Kennedy Town to Causeway Bay	8.32%
Route A + B: Tramway, from Kennedy Town to Shau Kei Wan	14.16%

3. Overall the WEP/WPA Encryption is disabled for around 60% of APs

Route A: Tramway, from Kennedy Town to Causeway Bay	60.48%
Route A + B: Tramway, from Kennedy Town to Shau Kei Wan	60.94%

4. Overall the proportion of AP without securing SSID was around 46.5% [1]

Route A: Tramway, from Kennedy Town to Causeway Bay	43.84%
Route A + B: Tramway, from Kennedy Town to Shau Kei Wan	46.49%

5. Used Channels

- The most common channels are 1, 6 and 11 (80.33% of total).
- There are a few (18) APs using channels beyond 11, captured along the tramway.
- There was an AP using channels 64, captured along the tramway. Is it the software problem or a special configuration that induced this information?

Note:
- Some APs are ETSI channel models supporting channels 1-13.
- In some countries only channels 1 – 11 are allowed whereas while channel 14 is approved in Japan. See unofficial reference:
http://dqd.com/~mayoff/notes/ap500/Help/terms/frequency_channel.html

[1] Including default SSID, well-known SSID and SSID same as trailing hexadecimal of AP's MAC address)

6. How is the result compared with War Driving 2002 and 2003?

In order to make a comparison, we followed the same route of the War Driving 2002 from Kennedy Town to Causeway Bay in Route A of the journey and record the result. A table for comparison is drawn:

	2002	2003	2004
Date	7-Jul-2002	5-Oct-2003	28-Nov-2004
Day	Sunday morning		
Weather	occasional light shower	sunny	sunny
Route	Kennedy Town - Causeway Bay		
No. of AP	187	474	926
% of WEP/WPA disabled	77%	69%	60%
% of insecure SSID	51%	39%	44%

Comparison of statistics along Route A (Kennedy Town to Causeway Bay)

(1) The number of detectable deployment along the tramway, comparing with the year 2003, has increased by 95%.

(2) The percentage of APs with WEP/WPA turned on has improved by 9%.

(3) The percentage of APs with SSID secured has decreased by 5%.

- If we look at the whole tramway, we can still arrive at the similar conclusion.

	2003 Overall	2004 Overall
Date	05-Oct-03	28-Nov-2004
Day	Sunday morning	
Weather	Sunny	
Route	Kennedy Town - Shau Kei Wan	
No. of AP	784	1723
% of WEP/WPA disabled	70%	61%
% of insecure SSID	43%	46%

Comparison of statistics along Route A (Kennedy Town to Shau Kei Wan)

(1) The number of detectable deployment along the tramway, comparing with last year, has increased by 120%.

(2) The percentage of APs with WEP/WPA turned on has improved by 9%.

(3) The percentage of APs with SSID secured has decreased by 3%.

Part II: War Sailing (War Driving in Victoria Harbour)

Note 1: In War Sailing, We used several different antennae. We consolidated the readings from different war drivers into one single log. Duplicated records are trimmed.

Note 2: Unless otherwise specified, the statistics was generated by the consolidated log from different antenna.

1. Number of Access Points Captured

Location	Number of unique Access Points captured
Cruise in Victoria Harbour (Consolidation of 4 war drivers)	**1460**

Individual War Driver (note that overlapping existed)	Number of unique Access Points captured
no antenna, 802.11a/b card,	167
+5dB omni-directional antenna, 802.11b/g built-in	833
+7.9dB broadband 45° horn antenna, 802.11b card	746
+8dB omni-directional antenna, 802.11b card	1182

2. Implementation of 802.11g, WEP/WPA and SSID configuration

AP Statistics	Percentage
Overall the implementation of 802.11g	582 (39.90%)
AP with WEP/WPA disabled	834 (57.10%)
AP without securing SSID [2]	594 (40.68%)

[2] In the above table, "AP without securing SSID" refers to factory default settings like:

- SSID that uses the ASCII characters of the station's hexadecimal MAC address;
- SSID that uses the ASCII characters of the station's hexadecimal MAC address subtracted by 1;
- SSID that uses a vendor-specific string concatenated with the ASCII characters of part of the station's MAC address;
- SSID that uses a vendor-specific string;
- SSID that is well-known by hotspot wireless LAN service provider

When comparing with war tramming along Kennedy Town to Causeway Bay, more 802.11g implementation was found (War Tramming:24.72%); approximately the same rate of WEP/WPA being disable (War Tramming:59.05); less insecure SSID (War Tramming:45.40%)

Note that the readings of war tramming and war sailing were taking with antennae with different sensitivity. The comparison by absolute number thus has no statistical value. However, the comparison by the percentage, on the other hand, could be meaningful.

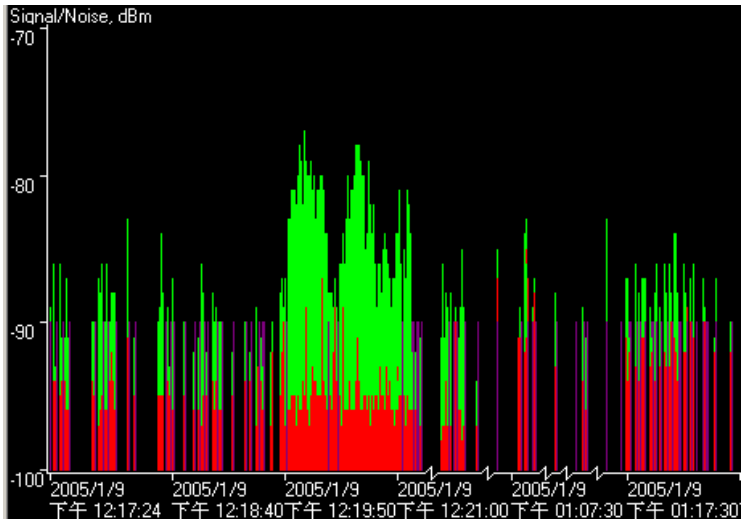
3. Connection Test

What has to be noted before conducting a connection test?

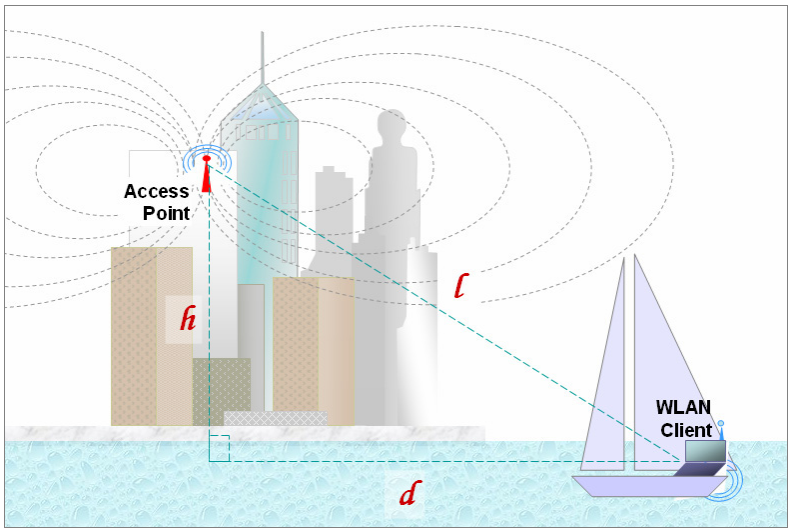
Firstly, authorization must be obtained from the owner of the access point to connect to it. Secondly, the TCPIP network setting of the wireless LAN network card must be enabled. Normally, this setting was disabled in war driving to avoid IP network connection being made. Thirdly, we had to ensure that the AP was not obstructed from the sight from the wireless LAN client in the harbour.

Can distant WLAN connection be made?

We used a notebook computer with a +8dB omni-directional antenna and an 802.11b card to conduct the connection test. The authorized AP located on the 30+ floor of a building in Admiralty. We discovered the AP from the Cruise Ferry when it approached the Central Pier and we tried to make the connection. The connection was very successful and the Internet browsing speed was very good. The Netstumbler log for the connected AP was revealed. We could see that the signal-to-noise dbm chart indicated a strong and steady signal during the connection.



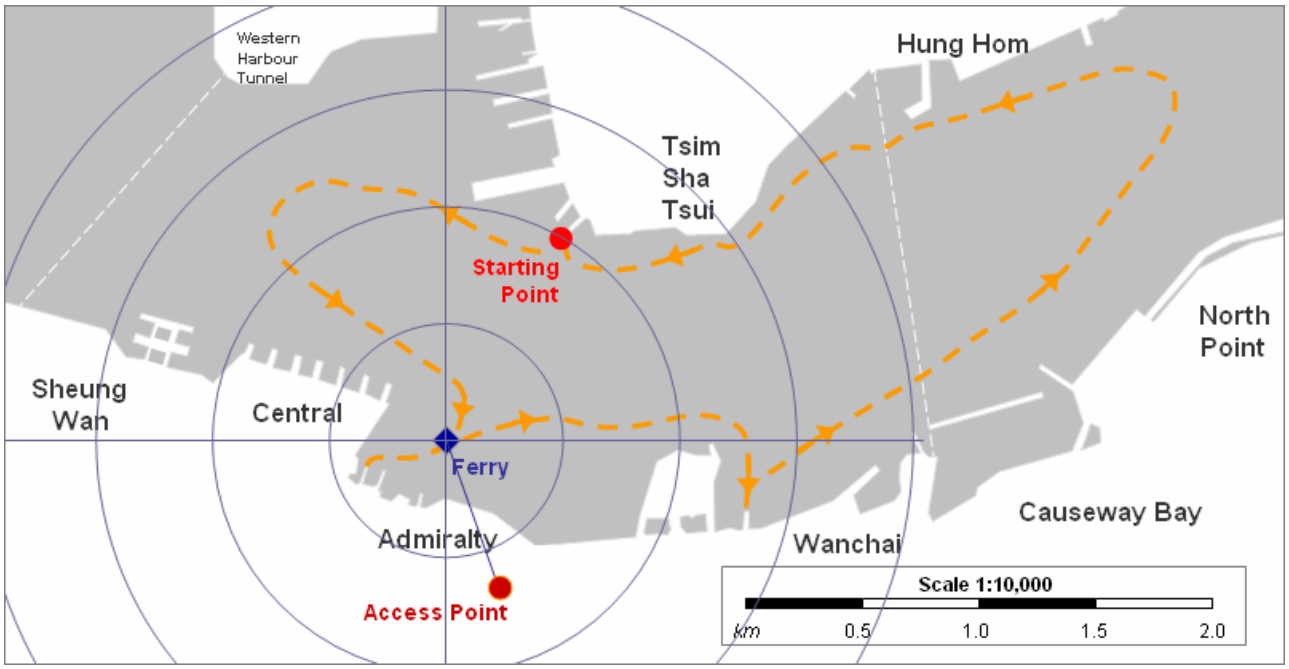
How to calculate the distance between the AP and the Ferry?



The AP and the Ferry were not at the same altitude. The distance of the AP from the ferry, ℓ, can be calculated by the Pythagoras Theorem.

$$\ell^2 = [h^2 + d^2]$$

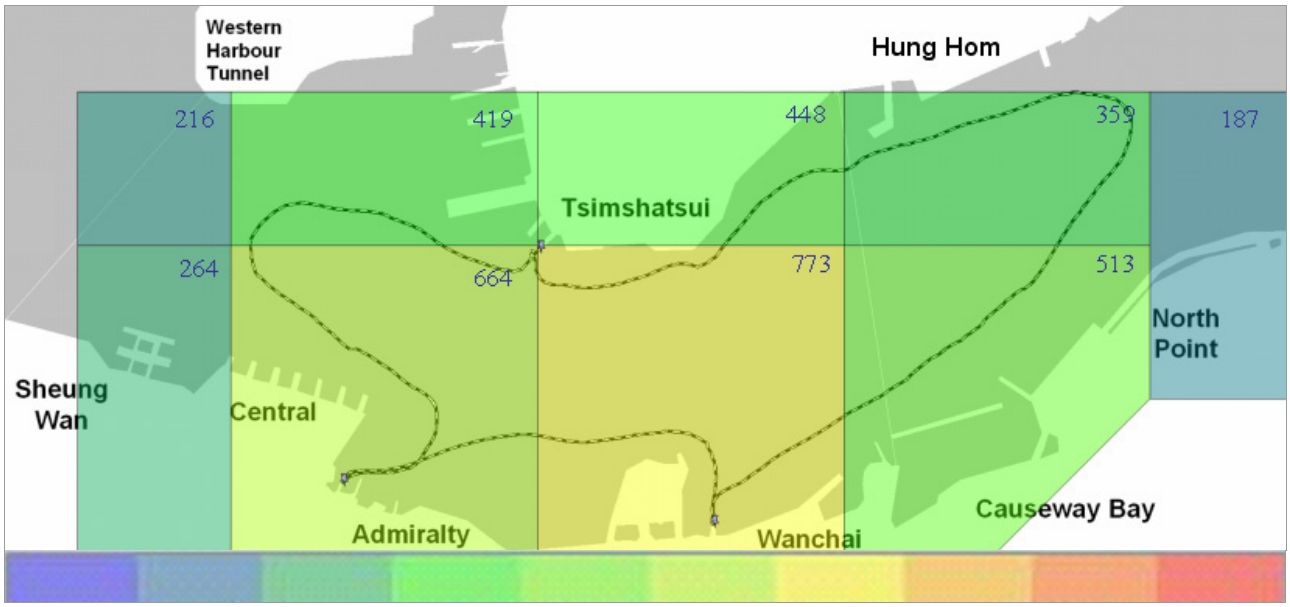
The locations of the Ferry and the Access Point are marked on the map below. The altitude of the AP was equivalent to the 30+ floor of an office building.



Altitude of AP,	h = 100m = 0.1km (on 30+ floor)
Sea-level distance between AP and ferry,	d = 0.62km (by measurement on the map)
Since, by Pythagoras Theorem,	$\ell^2 = [h^2 + d^2]$
Therefore, we have	ℓ = **0.628km (or 628m)**

Most commercial AP technical specifications state the range of AP without obstacle as 1000m. The distance of 628m was well within this specification. It is no wonder the signal of the connection made was strong and the network performance was very good.

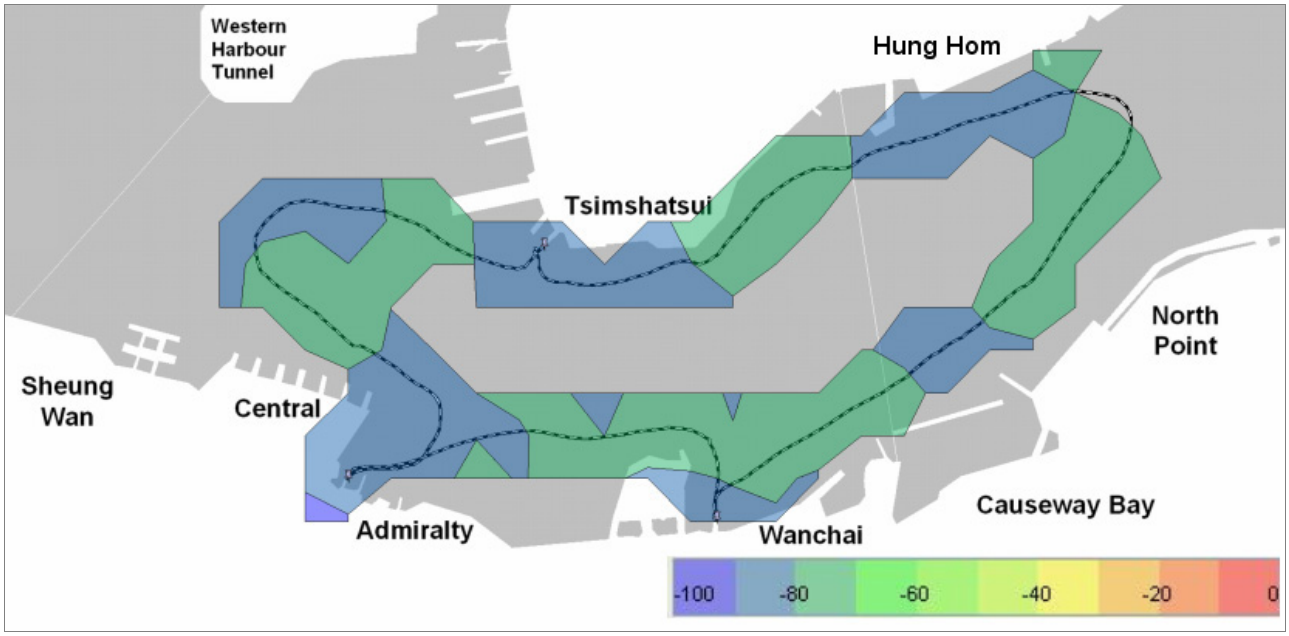
4. Comparative Concentration of WLAN Signals along the coast



The above figure divided the whole route into seven zones. The number marked in each zone is the number of APs whose signal can be detected in that zone. There were overlapping. An AP might be detectable in more than one zone and contributed to the statistics of all those zones. The numbers added up were more than the total number of unique APs.

We can see that Wanchai and TST areas had the highest concentration of AP signals, followed by Central and West TST, then Causeway Bay and Hung Hom and finally North Point. Since we were using omni-directional antenna,

5. Comparative Signal Strength along the coast



In the map, the color represents the best signal strength detected, with blue colour the weakest and red colour the strongest, as indicated by the legend at the bottom right.

The map of signal strength indicated that business areas like Central, Admiralty, Wanchai and TST East and TST West had APs with high signal strength. Residential area near North Point also produced very good signal strength. Perhaps it was due to increasingly improvement of household WLAN products.

Discussion

What are the factors to obtain good result in War Driving?

Line of Sight

- The AP had to be in the **line of sight**[3] with the WLAN client. When the ferry was moving along the coast, some building might have blocked the sight to the AP intermittently. We noticed that the connection dropped intermittently in that case.

Radiating Signal Strength and Sensitivity

- The higher the **sender and receiver signal strength and sensitivity**, the better the connection stability and the performance. In the case of WLAN connection, the AP and the WLAN client are both sender and receiver. At the AP side, signal strength can be improved by placing the AP near the window, amplifying the signal with an antenna or directing the signal with a reflector. At the WLAN client side, signal strength and sensitivity can be improved by an antenna.

Choice of Antenna

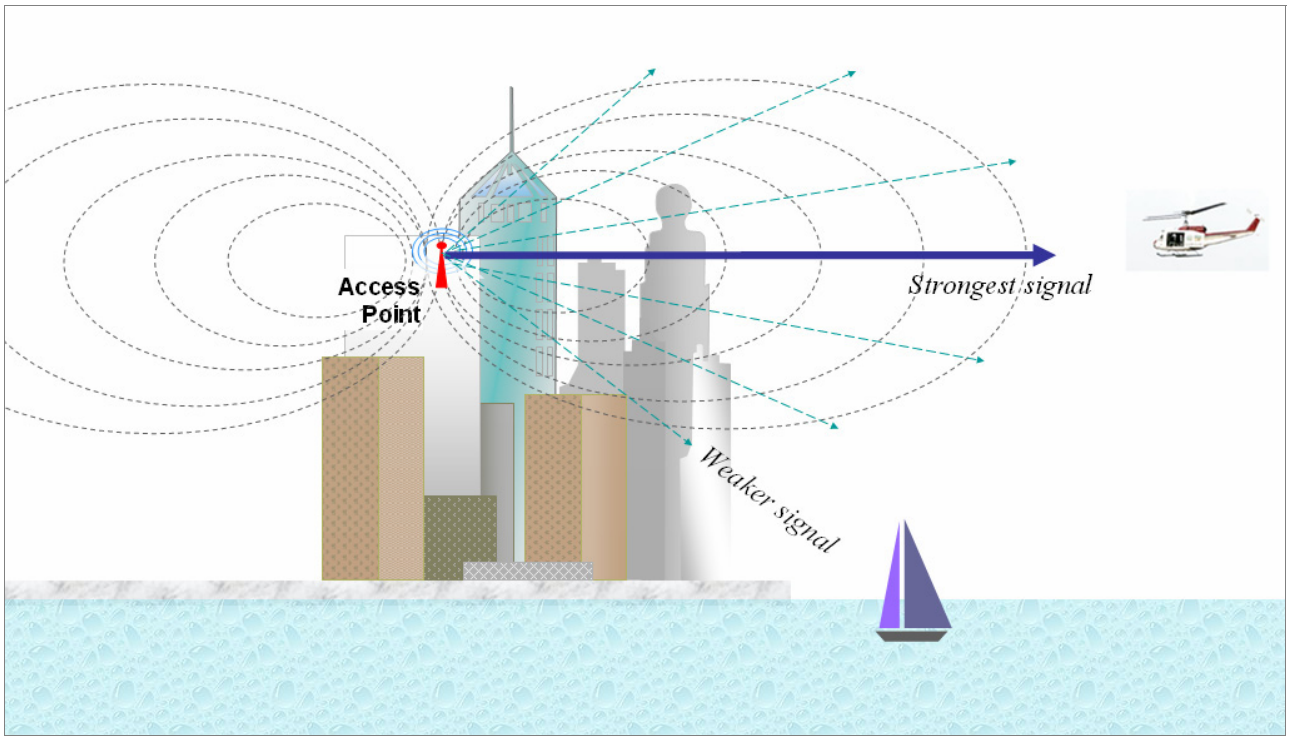
- In general an antenna with greater gain can improve the signal strength and sensitivity. The higher the gain the better the signal-to-noise ratio. More WLAN AP can be discovered when an antenna is attached.
- In stationed WLAN connections, the use of directional antenna can focus the radiation power in a certain direction to improve efficiency drastically. However, in WLAN war driving, since the WLAN client is moving, we **had to use omni-directional** (all direction in 2-D view) or **sectoral** (wide beam angle) antennae to cover wider angle of signals.

Individual War Driver (note that overlapping existed)	**Number of unique Access Points captured**
no antenna, 802.11a/b card	167
+5dB omni-directional antenna, 802.11b/g built-in	833
+7.9dB broadband 45° horn antenna, 802.11b card	746
+8dB omni-directional antenna, 802.11b card	1182

- From the comparison table, it is clear that an antenna with high gain can increase the signal strength and sensitivity, resulting in higher number of AP captured. Secondly, the horn antenna with 45° angle detected fewer APs than a similar gain omni-directional antenna.

[3] The “radio line of sight” and the “optical line of sight” are not equivalent. In a normal warm day, the two are very close. At cold night when the air near the ground surface is much colder (and thus denser) than the air above, the radio wave refract more and the WLAN signal can be transmitted further.

Relative Position of WLAN client to the AP



Radiation strength of a common omni-directional antenna

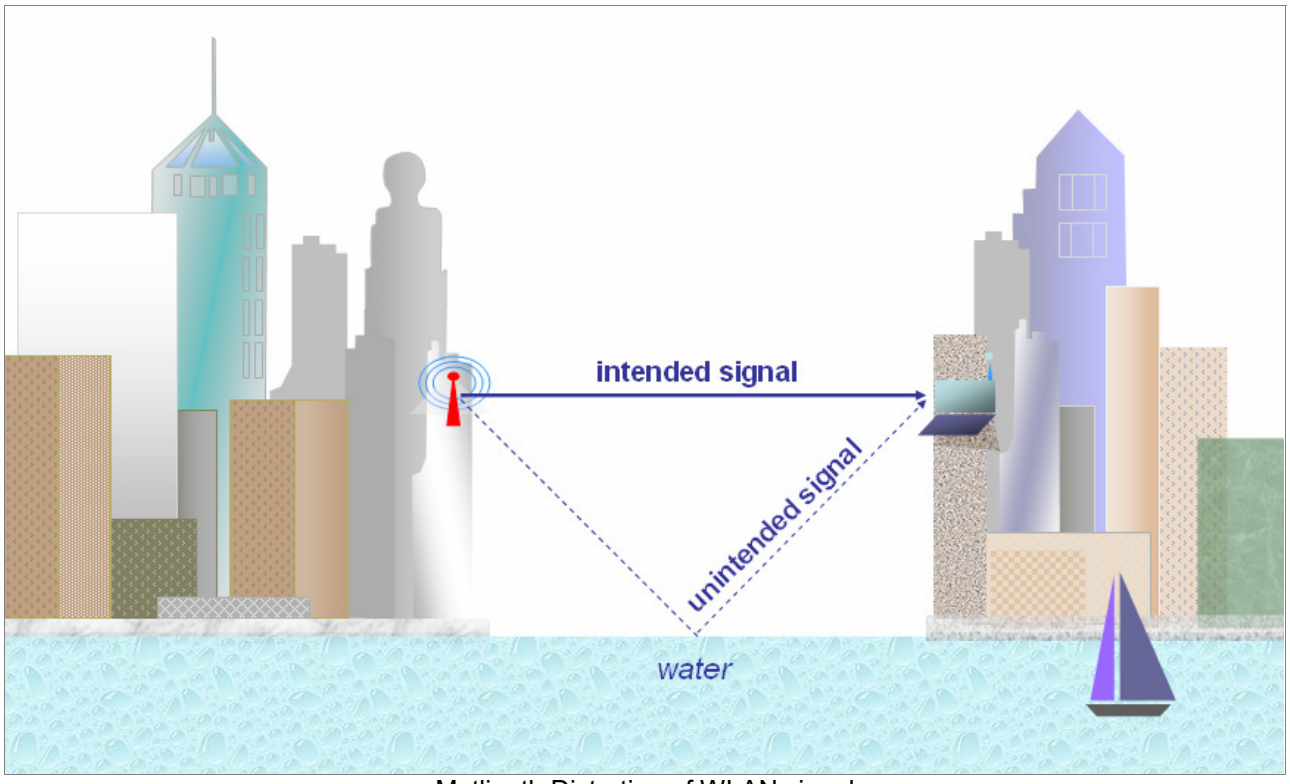
- The figure above shows the radiation pattern of a properly positioned AP with omni-directional antennae. You can see that the radiation pattern of the omni-directional antennae was not spherical. In other words, the location/direction of the WLAN client could affect the strength of signal received. The strongest signal is at the plane of same height of the AP. The greater the difference in the altitude, the weaker is the signal. We recall that the difference in altitude of the Cruise Ferry and the AP was about 100m. We could expect that if the WLAN survey was performed at a point on a higher level, e.g. from the helicopter or from tall building which was at the same level as the AP, the received signal would have been much stronger.

  So the success of war sailing in connecting an AP at the 30+ floor implies that a WLAN hacking at a distance at the same altitude as your office is totally feasible.

Multipath Distortion

- Multipath distortion is caused by the transmitted signal traversing to the receiver via more than one path. Reflection by water and tall building are the common causes of mutlipath distortion. In a big city like Hong Kong, people received echoed distortion of the WLAN signal more than they received the actual signal.

  In War Sailing, the ferry may receive the signal reflected from the water surface. Due to the low altitude of the ferry, reflected signal from water surface are mainly from lower level of the buildings.



Mutlipath Distortion of WLAN signal

Interference

- Passive interference can affect the signal coverage. Materials that can cause interference includes
  - building material used in the walls, floor and ceiling
  - permanently installed objects in the building such as elevator shafts and ductwork of air conditioners
  - other objects added by the occupants such as furniture, appliance and people.

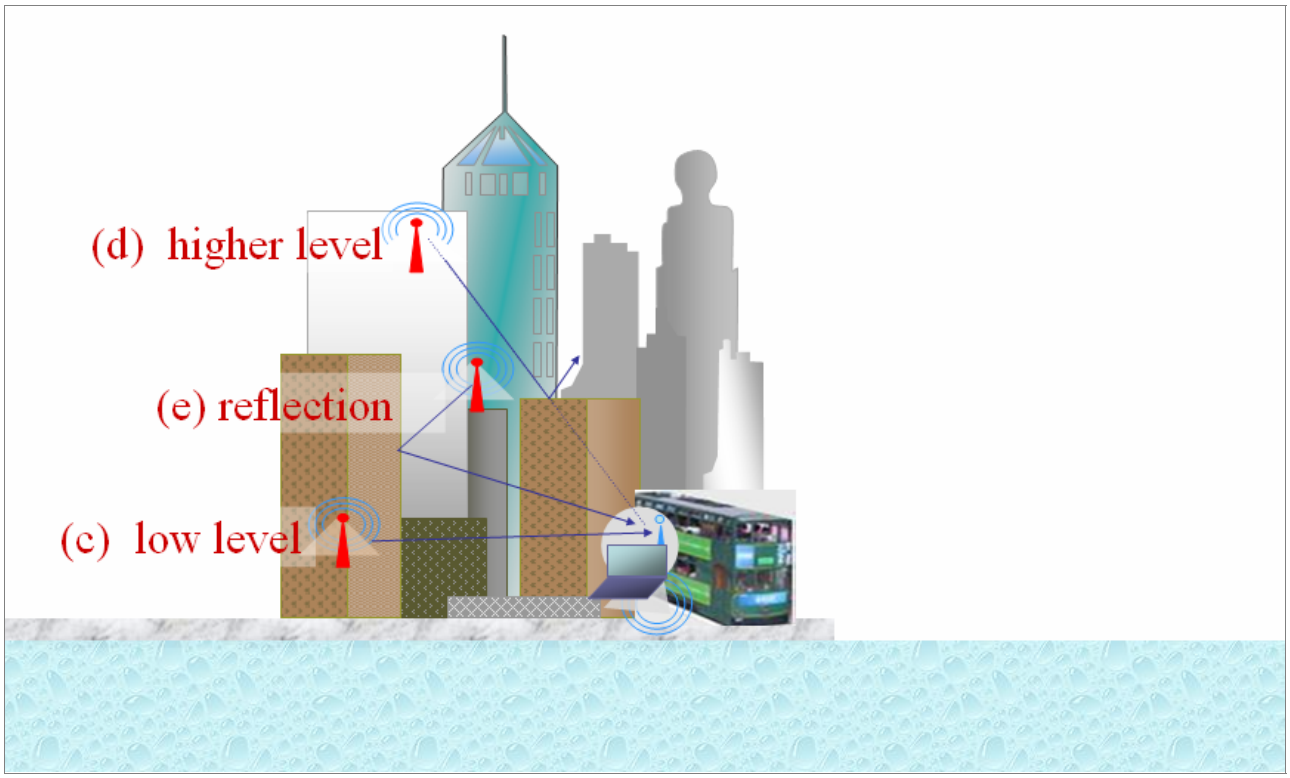
How was War Sailing compared to War Tramming?

Although on the face War Sailing was conducted in a similar way with similar equipment as War Tramming, several differences need to be noted.

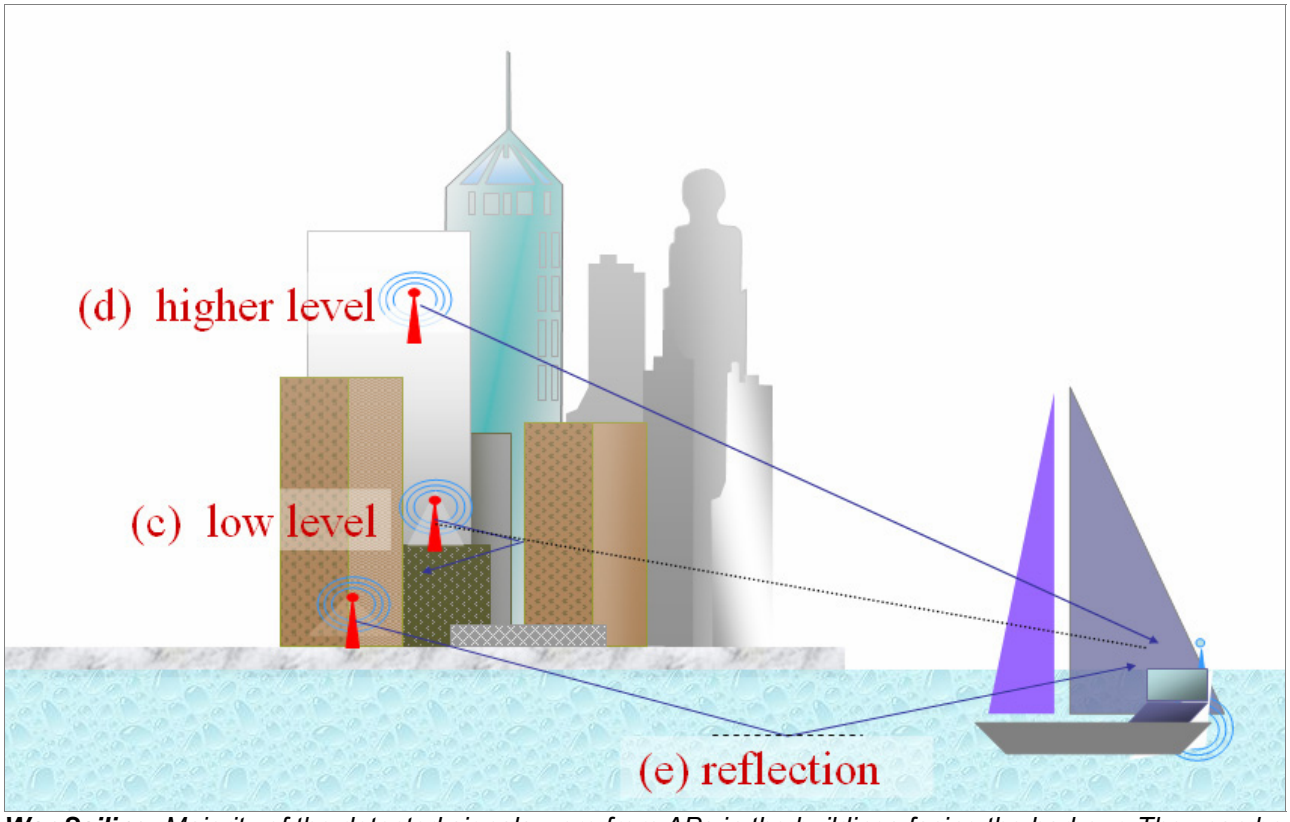
	War Tramming	War Sailing
a	War Driving in the streets in the business district.	War Driving in the middle of harbour.
b	APs are near. Small gain antenna is used.	APs are further away. Large gain antenna is used.
c	APs at the lower level can be detected.	APs at lower level are usually blocked by other building unless facing the harbour.
d	APs at higher level are usually blocked by buildings or signal attenuated after multiple reflections	APs at higher level can be detected.
e	Reflected signals come from all sides, from APs of lower and medium level, after reflections by buildings	Reflected signals come from sea surface. Due to angle of reflection, they are coming from APs facing the harbour at lower level.

Comparison of War Tramming and War Sailing

Two diagrams below are used to depict the differences of signals in War Tramming and War Sailing.



***War Tramming**: majority of detected signals come from low level along the tramway. Signals from high-level were blocked by building and constructions except those reaching the WLAN client via reflections.*



***War Sailing**: Majority of the detected signals were from APs in the buildings facing the harbour. They can be from high-level or from low level provided there is line of sight with the WLAN client. Some reflected signals from the sea surface can be received and they are mainly from the low level APs facing the harbour.*

Conclusion

Part I: War Tramming

- We can see a great leap in the use of WLAN (increased 120%) whereas the **overall improvement in security is average.**
- More people were using encryption. The percentage of AP with WEP/WPA disabled decreased from 69% to 60%
- Most APs broadcasted the SSID into the air. **Many APs were still using the factory setting of SSID**. The unchanged SSID could further imply that the owners of the APs might not have even changed other default settings like administrative password. A hacker can try to associate to the AP without much difficulty.

Part II: War Sailing

- With a sensitive antenna which was correctly oriented, it was possible to receive WLAN signals from a distance in the line-of-sight.
- With a stronger antenna, or a nearer distance, not only can WLAN signal been received but **connection from a distance and even different altitude is totally feasible.**
- APs with higher power, e.g. commercial use APs with antennae, can radiate signal to a further distance. The threat of AP exposure to jamming and hacking is higher.
- We thus **should not take for granted that WLAN is secured from hacker out-of-sight! Every effort should be taken to secure the wireless LAN network.**

* * * The End * * *