Report on

Wireless LAN War Driving Survey 2006

Hong Kong

Version 1.0

Mar-2007

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

[15/Oct/2006] War-tramming using 5dBi omni-directional antenna (some with GPS)

[Back row from left]: Jason Luk (PISA), James Chan (PISA), Eric Leung (WTIA) and Alan Tam (PISA)
[Front row from left]: Joseph Leung (WTIA), Alan Ho (PISA), Ken Fong (WTIA) and Trevor Leung (PISA)

[15/Oct/2006] War-Tramming Team on the tram

[On the left]: Joseph Leung,Jason Luk and James Chan
[On the right]: Alan Tam, Eric Leung, Trevor Leung, Ken Fong and Alan Ho

Photos

[15/Oct/2006] War-tramming survey finished at Shau Kei Wan

[From left]: Joseph Leung, Trevor Leung, Ken Fong, Jason Luk,
Alan Ho, Eric Leung and Alan Tam

[26/Nov/2006] The War Driving Team gathered at Tin Hau MTR Station and then took a mini-bus for a round trip of the Hong Kong Island

[Back row from left]: Jim Shek (PISA), Jackson Lee (WTIA), SC Leung (PISA), Eric Leung (WTIA),
David Cheung (WTIA), Edwin Lee (WTIA), Charles Lam (WTIA), Norman Chan (WTIA), James Chan (PISA)
[Front row from left]: Ken Fong (WTIA), Alan Ho (PISA) and Alan Tam (PISA)

Photos

[26/Nov/2006] Sat at the front hoping to get a better detection of WLAN APs

[26/Nov/2006] Various sizes of notebook PCs were used and usually the built-in wireless devices of newer notebook PCs could detect more APs and also faster

Photos

[26/Nov/2006] A few of the war-drivers had a GPS so that we could trace/plot mini-bus route on the Google Map afterwards

Photos

[26/Nov/2006] The mini-bus drove along the main roads on or in parallel to the tramway (west and east of northern Hong Kong Island) and then drove from east to south and then from south to west of the Hong Kong Island

[26/Feb/2006] The mini-bus was driving to Admiralty to finish the trip

[Back row from left]: Jim Shek (PISA) and Alan Tam (PISA)
[Front row from left]: Jackson Lee (WTIA) and Jeff Cheung (e-Zone)

Terms used

WLAN	Wireless Local Area Network. 802.11a/b/g are more popular standards now: • 802.11a: using 5GHz, 54Mbps • 802.11b: using 2.4GHz, 11Mbps • 802.11g: using 2.4GHz, 54Mbps • 802.11n: using 2.4GHz, 108Mbps • "Pre-N": A Pre-N wireless router uses two transmitters and three receivers to double the speed of existing 802.11 devices to 108 Mbps. Pre-N products let customers boost speed before 802.11n devices are available.
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. Third generation GPS devices is capable of acquiring satellite signals even in challenging situation e.g. between tall buildings. Compared to the previous generation, power consumption is reduced, higher sensitivity & fast signal acquisition and higher accuracy.

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
WPA2	IEEE 802.11i is an amendment to the 802.11 standard specifying security mechanisms for wireless networks. WPA implemented a subset of 802.11i and full implementation of 802.11i is called WPA2. The 802.11i architecture include: 802.1X for authentication, Robust Security Network (RSN) for keeping track of associations, and AES-based CCMP to provide confidentiality, integrity and origin authentication. Another important element of the authentication process is the four-way handshake.

Executive Summary

In Oct 2006, the two associations **PISA** and **WTIA** jointly conducted the "War Driving 2006" field survey along the classic tramway of Hong Kong Island and in Nov 2006 on a mini-bus around the Hong Kong Island. It was our **5th round** of the annual war-driving survey since 2002. 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 four previous studies conducted by PISA in 2002, and by PISA & WTIA in 2003 & 2004 to plot the profile of Hong Kong WLAN security development. The survey indicated that the number of WLAN implementation had skyrocketed in the past four or five years, and yet there was some improvement in the adoption of security strategies.

The overall percentage of AP with encryption continued to improve and has already exceeded 60% both in the tramway survey (62.96%) and the round Hong Kong Island survey (61.80%). Regarding the encryption mode of the APs, 79.31% are using WEP and 20.69% are using WPA/WPA2.

There was not much difference in the use of default SSID as compared to past years (i.e. there were 40+% APs using default SSID).

As compared to last year, the number of discovered APs in the tramway had notably increased by 63.92% as well as the percentage of adoption of encryption setting has improved 9.04%.

As the 802.11g market is getting matured and more products are available, the adoption rate of 802.11g AP was already over 80% (i.e. 81.68% in the tramway 82.77% in the round Hong Kong Island surveys). As compared to the tramway figures of last year, the adoption rate of 802.11g has increased by 15.26%.

We found that the overall results of the tramway and round Hong Kong Island surveys were similar in terms of encryption rate, 802.11g adoption and the use of factory default SSIDs.

As some of war-drivers were equipped with GPS, we tried plotting the war-driving results to the Google Map. It is interesting as we can "visualize" the results geographically!

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

We have been doing WLAN war-driving surveys since 2002. The one held in Oct 2006 & Nov 2006 was our 5th round war-driving survey. Below is an introduction of the past WLAN war-driving surveys.

Annual War Driving	Description
1st War Driving	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
2nd War Driving	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
3rd War Driving	In Nov 2004 & Jan 2005, **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: • the whole tramway, covering the business corridor of the HK Island • 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
4th War Driving	In Dec 2005 & Feb 2006, **PISA** and **WTIA** conducted the 4th "War Driving" again to benchmark the improvement for the WLAN Security in Hong Kong. Highlights of the 2005 war driving include: • the whole tramway, covering the business corridor of the HK Island • riding on bus/car in some areas of Kowloon
5th War Driving	In Oct 2006 & Nov 2006, **PISA** and **WTIA** conducted the 5th "War Driving" again to benchmark the improvement for the WLAN Security in Hong Kong. Highlights of the 2006 war driving include: • the whole tramway, covering the business corridor of the HK Island • round trip of Hong Kong Island (by a mini-bus)

.

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 conduct a non-intrusive***** information security study with responsible disclosure of information
3. 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 masked.
- We do not connect to the IP network of any insecure AP to further explore their vulnerabilities.
- We do not interfere / jam any wireless traffic.
- We limit to the scope we state above only.

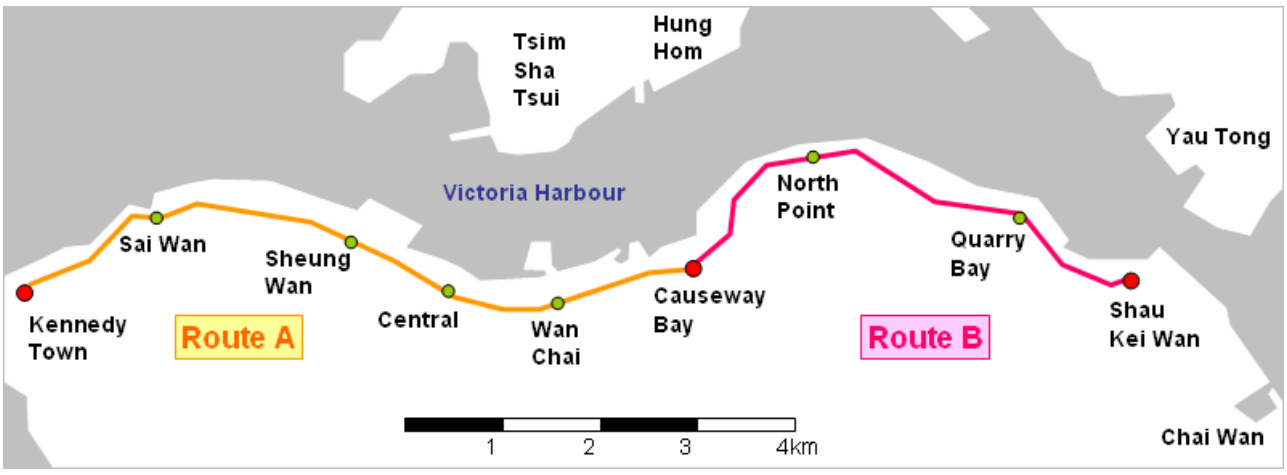
Methodology and Equipment

The War Driving was divided into 2 parts: ***War Tramming*** and ***War Driving round Hong Kong Island***.

Part I: War Tramming (Tramway War Driving)

- 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, 2003 and 2004 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 and 2004 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).

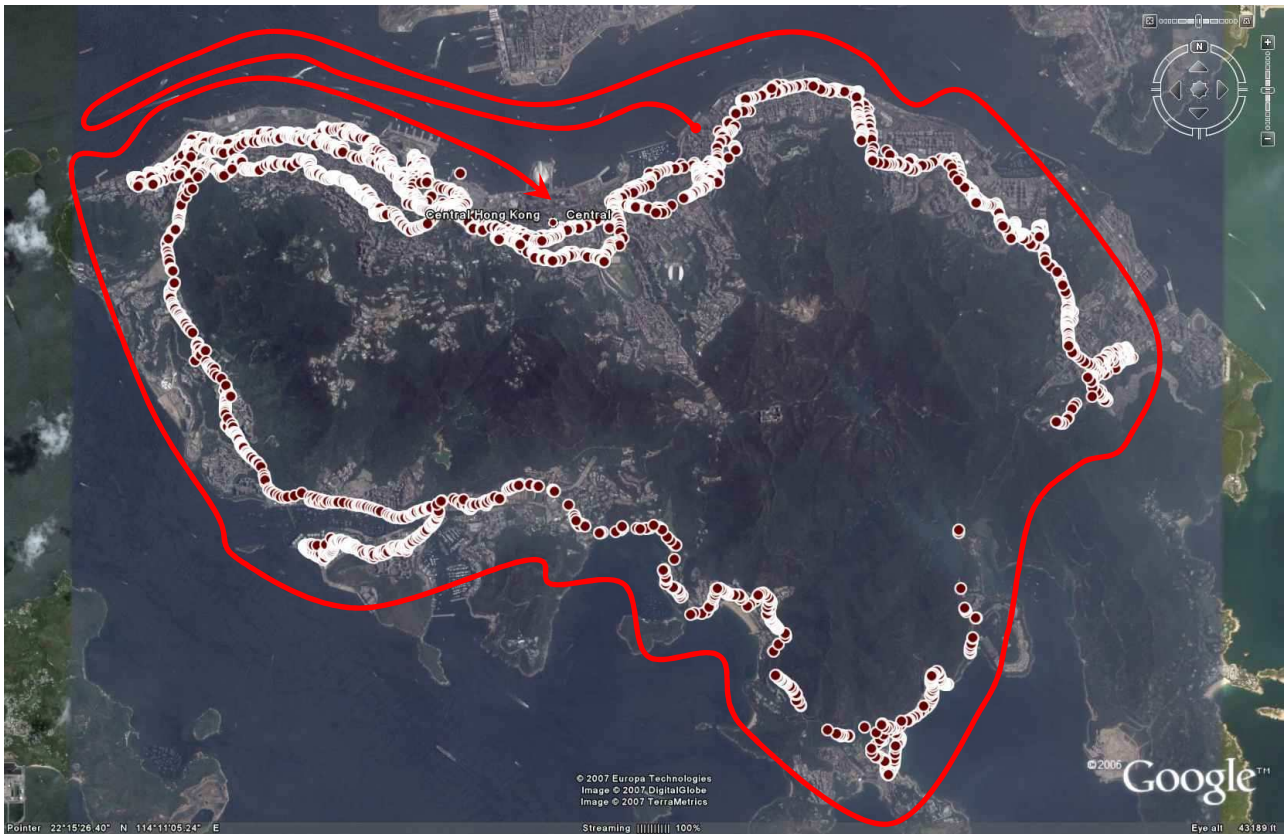
Date:	15-Oct-2006 (Sunday)
Time:	10 am -1 pm
Equipment:	*Hardware:* Notebook computers, WLAN cards & some with a +5dB omni-directional antenna and GPS *Software:* Netstumbler *(Netstumber results of antennae of +5dB or below were used as a control to compare with previous years' results)*
Route:	• Route A: o Taking a tram from Queensway, Admiralty westwards to Kennedy Town terminus, then a return tram from Kennedy Town terminus to Sogo Department Store, Causeway Bay (this was the same route as in War Driving 2002, 2003 and 2004) • Route B: o Taking another tram from Causeway Bay to Shau Kei Wan terminus (this was the same route as in War Driving 2003 and 2004)



Part II: War Driving round the Hong Kong Island

- In the past years, we conducted WLAN surveys in northern Hong Kong Island, in the sea or Kowloon. How about the situation round the whole Hong Kong Island? Would the statistics similar to the results of tramway? How about plotting the results/route to Google Map this time using our GPS longitude/latitude information?
- We rented a mini-bus for the round trip of the Hong Kong Island. At the beginning, the mini-bus drove along the main roads on or in parallel to the tramway (west and east of northern Hong Kong Island) and then later drove from east to south and then from south to west of Hong Kong Island.

Date:	26-Nov-2006 (Sunday)
Time:	10:30 am - 2:00 pm
Equipment:	Antenna used - + 5dB omni-directional antenna - null antenna Other equipment - WLAN card (built-in/external) – 802.11b/g or 802.11a/b/g - GPS device (serial/USB/bluetooth) for recording longitude/latitude information



Findings and Analysis

Part I: War-Tramming (Tramway War Driving)

Note: the war tramming statistics (NetStumbler) below was generated by the consolidated log from war drivers with antenna having a 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	2492
Route A + B: Tramway, from Kennedy Town to Shau Kei Wan	4344

2. Overall the implementation of 802.11g in Hong Kong is around 81.68%.

Route A: Tramway, from Kennedy Town to Causeway Bay	80.98%
Route A + B: Tramway, from Kennedy Town to Shau Kei Wan	81.68%

(We found that there were 0.16% APs of 802.11a for both Route A and Route A + B)

3. WEP/WPA Encryption is disabled for around 37.04% of APs

Route A: Tramway, from Kennedy Town to Causeway Bay	36.16%
Route A + B: Tramway, from Kennedy Town to Shau Kei Wan	37.04%

4. The proportion of AP with factory default SSID [1]

Route A: Tramway, from Kennedy Town to Causeway Bay	43.34%
Route A + B: Tramway, from Kennedy Town to Shau Kei Wan	44.01%

5. Used Channels

- The most common channels are 1, 6 and 11 (81.91% of total).
- We found that there were 802.11a channels during the tramway (namely, 36, 48, 52, 56, 60 and 64)

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 factory default SSID, SSID with vendor-specific string, SSID same as trailing hexadecimal of AP's MAC address

6. How are the results compared with War Driving of past years?

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	2005	2006
Date	07-Jul-02	05-Oct-03	28-Nov-04	04-Dec-05	15-Oct-06
Day	Sunday morning				
Weather	occasional light shower	sunny	sunny	Sunny	occasional raining
Route	Kennedy Town - Causeway Bay				
No. of AP	187	474	926	1576	2492
% of WEP/WPA disabled	77%	69%	60%	45.56%	36.16%
% of factory default SSID	51%	39%	44%	39.47%	43.34%
% of 802.11g AP			8.32%	68.15%	80.98%

(1) The number of detectable deployment along the tramway, comparing with last year, has increased by 58%.

(2) The percentage of APs with WEP/WPA turned on has improved by 9.4%.

(3) The percentage of APs with factory default SSID has increased by 3.87%.

(4) Adoption 802.11g AP has increased from 68.15% to 80.98%

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

	2003 Overall	2004 Overall	2005 Overall	2006 Overall
Date	05-Oct-03	28-Nov-04	04-Dec-05	15-Oct-06
Day	Sunday morning			
Weather	Sunny			Occasional raining
Route	Kennedy Town - Shau Kei Wan			
No. of AP	784	1723	2650	4344
% of WEP/WPA disabled	70%	61%	46.08%	37.04%
% of factory default SSID	43%	46%	42.98%	44.01%
% of 802.11g AP		14.16%	66.42%	81.68%

(1) The number of detectable deployment along the tramway, comparing with last year, has increased by 63.92%.

(2) The percentage of APs with WEP/WPA turned on has improved by 9.04%.

(3) The percentage of APs with factory default SSID has increased by 1.03%.

(4) Adoption 802.11g AP has increased from 66.42% to 81.68%

Part II: War Driving round the Hong Kong Island

Note: the war driving statistics (NetStumbler) below was generated by the consolidated log from war drivers with antenna having a gain of +5dB or below.

1. Number of Access Points Captured

Location	Number of unique Access Points captured
The mini-bus drove along the main roads on or in parallel to the tramway (west and east of northern Hong Kong Island) and then drove from east to south and then from south to west of Hong Kong Island Mini-bus route: Tin Hau ➔ Admiralty ➔ Kennedy Town ➔ Admiralty ➔ Causeway Bay ➔ North Point ➔ Shau Kei Wan ➔ Chai Wan ➔ Tai Tam ➔ Red Hill ➔ Stanley ➔ Repulse Bay ➔ Aberdeen ➔ Pok Fu Lam ➔ Sheung Wan ➔ Admiralty Due to limited time at the later part of the trip, the mini-bus drove faster in the later part of the trip than the earlier part of the trip in the northern Hong Kong Island.	**10548**

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

AP Statistics	Percentage
Overall the implementation of 802.11g	**8731 (82.77%)**
AP with WEP/WPA disabled	**4029 (38.20%)**
AP with factory default SSID [2]	**4676 (44.33%)**
Encryption mode: WEP vs WPA/WPA2	**79.31% vs 20.69%**

(We found that there were 0.10% APs of 802.11a during the Hong Kong Island round trip)

When comparing with war tramming results along Kennedy Town to Causeway Bay, the percentage of 802.11g implementation, WEP/WPA disabled and the use of factory default SSIDs were similar.

We used Kismet to run a statistics of the adoption rate of WEP vs WPA/WPA2 encryption mode. For a sample of 6530 encrypted APs, **79.31%** was encrypted with WEP and **20.69%** with WPA/WPA2.

---

[2] In the above table, "AP with factory default 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 hexadecimal MAC address;
- SSID that uses a vendor-specific string or generic string like “any” or “default”;

Note that the readings of war tramming and war driving round the Hong Kong Island were taken on different routes. The comparison by absolute number thus has no statistical value. However, the comparison by the percentage, on the other hand, could be meaningful.

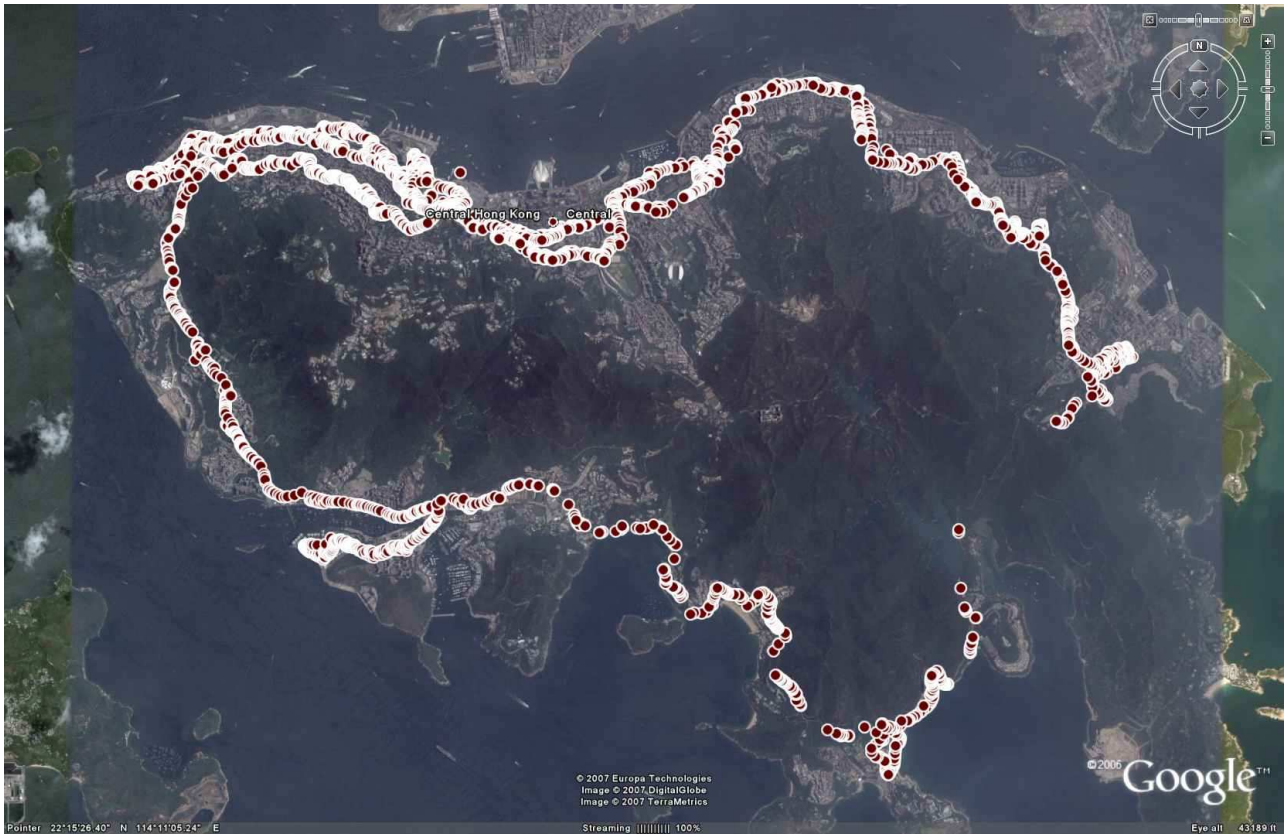
We found that the overall results of the tramway and round Hong Kong Island surveys were similar in terms of encryption rate, 802.11g adoption and the use of factory default SSIDs. Regarding the encryption mode of the APs, 79.31% are using WEP and 20.69% are using WPA/WPA2.

3. Plotting the war-driving results (or mini-bus route) on Google Map

As we can plot a location (by specifying the longitude/latitude) on Google Map, we can utilize Google Map to visualize our war-driving results! This year, we took this approach and below maps are our findings for the round Hong Kong Island war-driving survey. It is quite interesting!

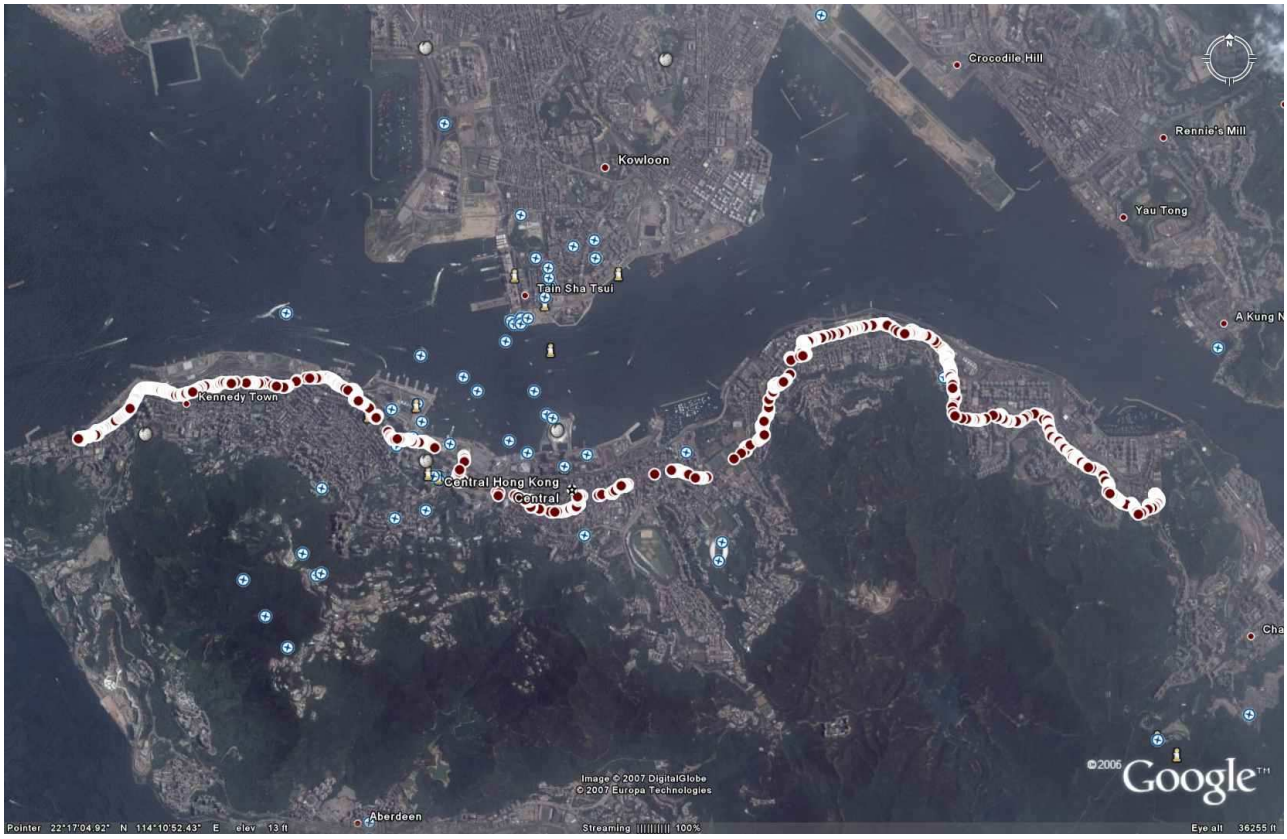
(a) Overall (see also page 13)

Tin Hau → Admiralty → Kennedy Town → Admiralty → Causeway Bay → North Point → Shau Kei Wan → Chai Wan → Tai Tam → Red Hill → Stanley → Repulse Bay → Aberdeen → Pok Fu Lam → Sheung Wan → Admiralty

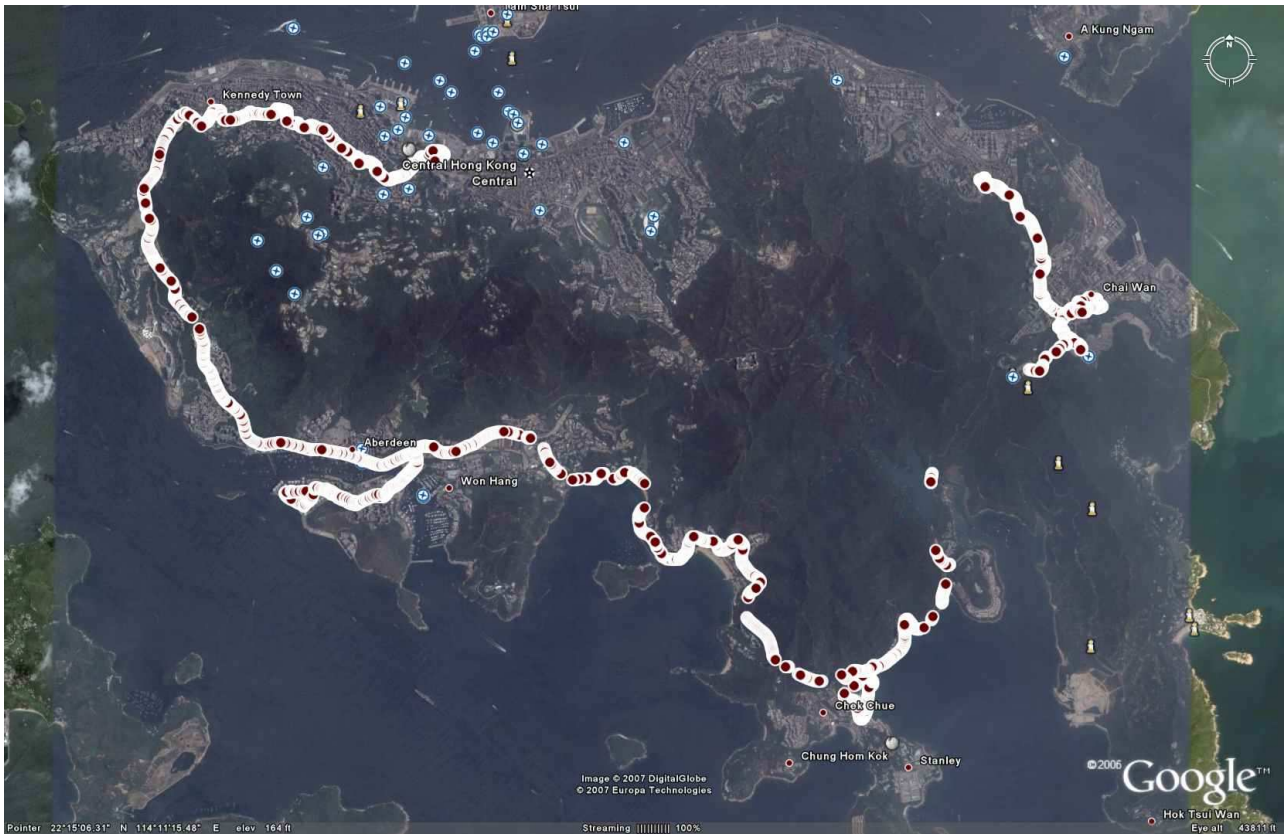


(b) Route: Tin Hau ➔ Admiralty ➔ Kennedy Town

(c) Route: Kennedy Town ➔ Admiralty ➔ Causeway Bay ➔ North Point ➔ Shau Kei Wan



(d) Route: Shau Kei Wan ➔ Chai Wan ➔ Tai Tam ➔ Red Hill ➔ Stanley ➔ Repulse Bay ➔ Aberdeen ➔ Pok Fu Lam ➔ Sheung Wan ➔ Admiralty



Other Findings

"FON" APs

During our Hong Kong Island round trip (on mini-bus) in Nov/2006, we found some "FON" APs (around 0.35%). FON is a WiFi community in the world. FON members (or Fonero) share their wireless Internet access at home and, in return, enjoy free WiFi wherever they find another Fonero's Access Point. However, from security point of view, sharing one's wireless Internet access at home with outsiders would have a security concern.

Early adopters of "pre-N" APs

During our 5th round war driving in Oct/2006 and Nov/2006, we found some "pre-N" APs (around 0.18% – similar percentage as in the 4th round of war driving). They are examples of early adopters of the pre-version of 802.11n technology.

In March 2006, the IEEE unanimously approved a draft version of 802.11n that is expected to become the next generation standard for wireless networks. The standard provides for increased range and speeds as compared to current 802.11g standards. Draft 802.11n will also have backward compatibility with current 802.11b and g products.

802.11n will support bandwidth greater than 100 Mbps. 802.11n will work by utilizing multiple wireless antennas in tandem (or "MIMO" (Multiple Input, Multiple Output)) to transmit and receive data.

Some manufacturers offer "pre-N" wireless equipment. A Pre-N wireless router uses two transmitters and three receivers to double the speed of existing 802.11 devices to 108 Mbps. Pre-N products let customers boost speed before 802.11n devices are available.

Conclusion

Part I: War Tramming

- We still see a drastic growth of the number of WLAN AP (increased by 63.92% as compared to last year) though the growth rate was flattened as compared to 2 years before.
- For the adoption of encryption in WLAN AP, we find out that the adoption rate was exceeded 60% (i.e. 62.96%). It showed an continuous improvement in this area.
- We found that there was not much difference in the use of default SSID as compared to past years (i.e. there were 40+% APs using default SSID).

Part II: War Driving round the Hong Kong Island

- We found that the overall results of the tramway and round Hong Kong Island surveys were similar in terms of encryption rate, 802.11g adoption and the use of factory default SSIDs.
- We also tried analyzing the adoption rate of the encryption mode this year since the use of WPA/WPA2 has been growing. We found that 79.31% are using WEP and 20.69% are using WPA/WPA2.
- As some of war-drivers were equipped with GPS and Google Map allows plotting a location by specifying its longitude/latitude information, this year we tried plotting the war-driving results to the Google Map. It is interesting that we can “visualize” the results geographically!

* * * The End * * *