行政院國家科學委員會專題研究計畫 成果報告

P2P 應用對 DNS 系統暨網路基礎建設的影響－使用型態與運作效能探討

研究成果報告(精簡版)

計 畫 類 別 ：個別型
計 畫 編 號 ：NSC 97-2221-E-009-136-
執 行 期 間 ：97 年 08 月 01 日至 98 年 07 月 31 日
執 行 單 位 ：國立交通大學計算機與網路中心

計 畫 主 持 人 ：陳昌盛

報 告 附 件 ：出席國際會議研究心得報告及發表論文

處 理 方 式 ：本計畫可公開查詢

中 華 民 國 98 年 10 月 31 日

行政院國家科學委員會補助專題研究計畫 ■ 成 果 報 告
□期中進度報告

P2P 應用對 DNS 系統暨網路基礎建設的影響--使用型態與運作效能探討

計畫類別：■ 個別型計畫　　□ 整合型計畫
計畫編號：97-2221-E-009-136
執行期間：97 年 8 月 1 日至　98 年 10 月 31 日

計畫主持人：陳昌盛副教授
計畫參與人員：陳政國、蘇俊憲、黃柏翰、王英鼎

成果報告類型(依經費核定清單規定繳交)：■精簡報告　□完整報告

本成果報告包括以下應繳交之附件：
□赴國外出差或研習心得報告一份
□赴大陸地區出差或研習心得報告一份
■出席國際學術會議心得報告及發表之論文各一份
□國際合作研究計畫國外研究報告書一份

處理方式：除產學合作研究計畫、提升產業技術及人才培育研究計畫、列管計畫及下列情形者外，得立即公開查詢
□涉及專利或其他智慧財產權，□一年□二年後可公開查詢

執行單位：國立交通大學計算機與網路中心

中　華　民　國　98　年　10　月　31　日

P2P 應用對 DNS 系統暨網路基礎建設的影響--使用型態與運作效能探討

A Study of P2P Computing, DNS and Network Infrastructure – Usage Pattern and Performance

計畫編號：97-2221-E-009-136
執行期限：98 年 10 月 31 日
主持人：陳昌盛副教授　國立交通大學計算機與網路中心
計畫參與人員：陳政國、蘇俊憲、黃柏翰、王英鼎

一、中文摘要

本研究嘗試探討當前網路主流 P2P[8]應用以及校園網路架構運作效率的關聯[1][2][5][9]，以期提供後續網路系統架構調整的參考。本研究的重點在於，將一些網路量測與統計分析的技術，應用到包含 P2P 應用服務以及 DNS[4][7]系統的研究上。本研究主要的資訊蒐集來源，是交通大學校園網路的真實運作記錄(network traffic traces)。以交通大學為例，當前幾種典型網路服務模式(包含有線與無線網路)：(1)學生宿舍網路測試平台(對稱式寬頻網路)，(2)非對稱式 NCTU-ADSL[3]服務為代表，(3)無線區域網路使用平台。本研究的目的在於，針對特定的校園網路平台，長期持續地記錄網路使用流量變化(Netflow traffic analysis)與 DNS 查詢記錄與分析，定期摘要性地記錄系統的運作資料，一方面幫助管理者掌握相關平台的運作狀況，另一方面網際網路服務的變化多元且快速，管理者通常也必須調整系統資源的配置(包含增加應用 DNS server 、Mail serve 數目與位置，改變網路連接設備的銜接架構等)，作為整體考量的依據，多方兼顧整體使用效能(performance)、穩定度(reliability)、可延伸調整(scalable)等功能，以利特定用戶族群的網路使用。

二、英文摘要(Abstract)

Currently, P2P traffic dominates most of the network applications' traffic on many Internet sites. For example, about 70%-80% of the daily traffic at our university, National Chiao Tung University (NCTU, one of leading Internet service provider on Taiwan Academic Internet Community), is contributed by P2P applications. In this project, we would like to study the topic on how different network architectures (i.e., asymmetric vs. symmetric network) influence the network traffic and the user behaviors with the peer-to-peer (P2P) applications. Through the integrated analysis of Netflow traffic, DNS traffic and network infrastructure, we would like to make a comparison of how user behaviors differ from one another and produce some insights for facilitating network performance tuning. Most importantly, we hope that NCTU experiences could provide some valuable suggestions for interested network administrators (e.g., academic institutions, ISP, etc.) to improve the network performance of their sites.

三、計畫緣由與目的

由於網際網路基本建設的成熟，頻寬增加，數位內容的傳遞日益蓬勃。然而，這些新興多樣化的需求，如數位影音，網路電話等，由於要求高頻寬、高品質，傳統的 Client-Server 服務方式，在 Server 端將造成極大的瓶頸。於是，利用 Client 端的計算、傳輸能力的解決方案，因應而生。其中最為稱著者，為 P2P(Peer to Peer)服務模式。在 P2P 服務模式之下，原有階層化的服務模式，幾乎完全扁平化、分散化到各個有相同需求的 Clients 族群中。

交大網路服務伴隨台灣學術網路(TANet)一起成長，我們長期觀察歷年來網路流量的變化，以我們交大校園流量為例，大約短短十年之間，可以發現一些有趣的趨勢：

- 從早期 FTP 佔 30%，到 WWW (http) 佔 70%，再到 P2P 佔 90% 總流量。
- 從 30% 的人使用 70 % 的頻寬，到現在的 10% 的人使用 90% 的頻寬。

本研究之目的在於，嘗試連續且持久地記錄校園 P2P 網路服務流量分佈運作資訊，透過長期的觀測調整學習，輔助網路

管理者掌握、管理及分配路由器的流量，進而提出管理政策，以及網路基礎架構之調整。

As mentioned above, the pattern of P2P traffic poses another problem aside from the sheer volume. Therefore, we would like to further study the topic on how different network architectures (i.e., asymmetric vs. symmetric network) influence the network traffic and the user behaviors with the peer-to-peer (P2P) applications. As shown in Fig. 1, using both the ADSL service (i.e., asymmetric network) and the Beta Site Services (i.e., Dorm-Net, symmetric network) on our campus network as examples (i.e., with roughly the same range of people served), we would like to make a comparison of how user behaviors differ from each other on these two typical network architectures and offer some insights for facilitating network performance tuning.

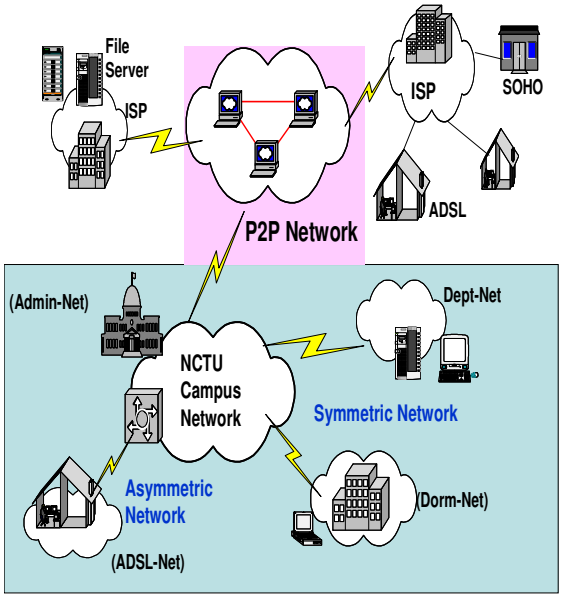

Fig.1: NCTU Campus Network – Asymmetric vs. Symmetric Network

本研究的重點在於，將一些網路量測與統計的技術，應用到 P2P 網路服務和網路基礎架構之相關性探討（包含系統效能、目前的使用型態、操作問題等正面以及負面的相關性），進而對現有網際網路基礎設施，提出研究的對策，以因應未來相關網路技術的變化趨勢。

- P2P 與 DNS 查詢的關連性探討

  In general, DNS traffic consists of independent queries from different sources and of different types (e.g., A, MX, and PTR, etc.). In principle, as shown in Fig. 2, a typical site might have several independent advertising and/or recursive DNS servers for serving incoming and outgoing queries (e.g., two for the former and another three for latter) about the forward and corresponding domain zones.

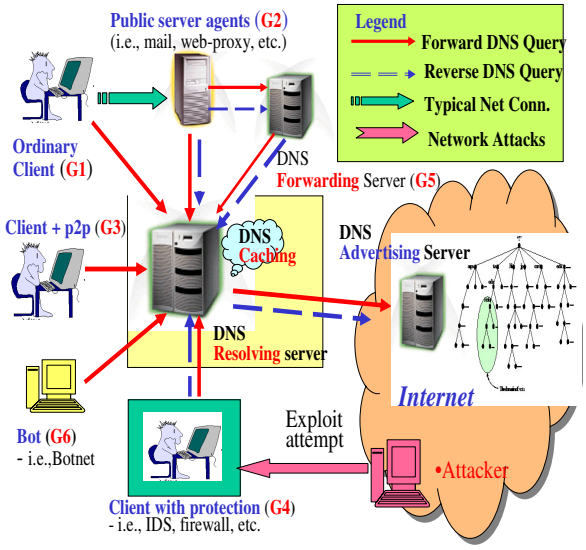

Fig. 2: A simple operation model of DNS

Table 1: Typical users/programs of an ordinary DNS resolving server

Category	Examples (refer to Fig.1)
1. Ordinary clients (G1)	Ordinary clients without specialized protection mechanism
2. Normal server (G2, G4)	Mail, web proxy etc. (G2), Personal firewall systems (G4)
3. P2P clients (G3)	• VoIP: Skype, FreePP, etc. • File Transfer: BitTorrent, eDonkey, etc. • Video Streaming: ppstreaming, etc.
4. DNS server (G5)	Downstream DNS forwarding servers
5. Malicious program	• Botnet (e.g., Trojan, etc.), network virus/worm (mail,

(G6)	web, etc.), etc. • intrusion attempts (SSH/Telnet/Ftp exploits, etc.), etc.

According to domain expertise, the DNS traffic distributions vary from site to site and slightly from time to time on the same site. However, in practice, most of the DNS queries are conducted on some major hosts in daily use. For example, Table 1 shows some potential top users (or programs) of typical DNS servers of our campus network. Under normal conditions, the DNS clients listed in categories 1, 2, 4, and 5 are usually recognized and acceptable. However, on the other hand, the traffic introduced by hosts in categories 3 and 6 are usually not welcome. Often, either they are malicious programs, or they are underground client/server processes. All of these might consume lots of network and system resources. If the administrators could not recognize the problem sources in time and handle them properly, under severe emergent situations, some may even crash the entire network or related systems.

四、想法與討論

實務上，單純作流量統分析不可能做出 P2P 最佳網路建議，因為 P2P 路由不是網管理者決定的，而是 P2P 應用程式自動計算反應效率決定最佳化路由。

本計劃試圖探討比較主流 P2P 應用、DNS 使用，以及現今各單位網路架構的關聯，以期提供後續網路系統架構調整的參考。

■ The DNS Traffic Analysis

Most Internet services are based on the working model that there will be some Domain Name System (DNS) queries before the communication activities. Therefore, patterns of DNS queries are suggestive of network user behaviors. By intuition, a statistical approach (as shown in Fig. 3a & 3b, running the *dnstop* program) might be such a typical solution to find the patterns.

50 new queries, 73922 total queries

Sources	count	%
140.113.1.1	15962	21.6
140.113.216.36	2322	3.1
140.113.147.32	2036	2.8
140.113.23.125	1103	1.5
140.113.122.46	846	1.1
140.113.28.194	796	1.1
140.113.158.9	789	1.1
140.113.39.200	748	1.0
140.113.168.127	687	0.9
140.113.27.54	672	0.9
140.113.146.21	629	0.9
140.113.38.249	614	0.8
140.113.92.143	585	0.8
140.113.20.228	582	0.8
140.113.238.43	573	0.8
140.113.27.181	547	0.7
140.113.212.26	505	0.7
140.113.27.133	471	0.6
140.113.70.135	467	0.6
140.126.166.58	374	0.5
140.113.4.6	372	0.5
140.113.123.128	371	0.5
140.113.145.62	368	0.5
140.113.172.233	362	0.5
140.113.23.2	333	0.5
140.113.211.83	317	0.4
140.126.180.1	316	0.4
140.113.122.172	309	0.4
140.113.209.19	279	0.4
140.113.13.222	229	0.3
66.35.254.64	202	0.3

Figure 3a: Top-N list by sender IP

50 new queries, 94160 total queries

3LD	count	%
nctu.edu.tw	8340	8.9
113.140.in-addr.arpa	6652	7.1
tracker.animeun.com	2690	2.9
tracker.desitorrents.com	2555	2.7
windowmaker.org	2026	2.2
tracker.bt-chat.com	1580	1.7
160.202.in-addr.arpa	1125	1.2
tpe.yahoo.com	869	0.9
tracker.prq.to	806	0.9
www.potuk.org	643	0.7
lineage1.04dj.com	462	0.5
kkman.com.tw	455	0.5
news.yahoo.com	449	0.5
www.yahoo.com	447	0.5
assets.macromedia.com	409	0.4
il.yimg.com	403	0.4
privatetracker.limitedivx.com	398	0.4
142.68.in-addr.arpa	390	0.4
bc.yahoo.com	387	0.4
tracker.thepiratebay.org	386	0.4
rad.msn.com	378	0.4
love.witlog.net	372	0.4
relays.ordb.org	372	0.4
boughtem.nowslate1703.info	366	0.4
mail.google.com	339	0.4
pic.wretch.cc	338	0.4
tw.yahoo.com	327	0.3
tk.greedland.net	316	0.3
tw.yimg.com	314	0.3
tracker.hkorz.com	307	0.3

Figure 3b: Top-N list by DNS queries

其次，我們將透過 netflow（如 Fig.4）等平台工具，設計網路流量統計與分析程式，蒐集校園網路幾個特定平台（ADSL, WLAN, BetaSite 測試平台）網路流量。

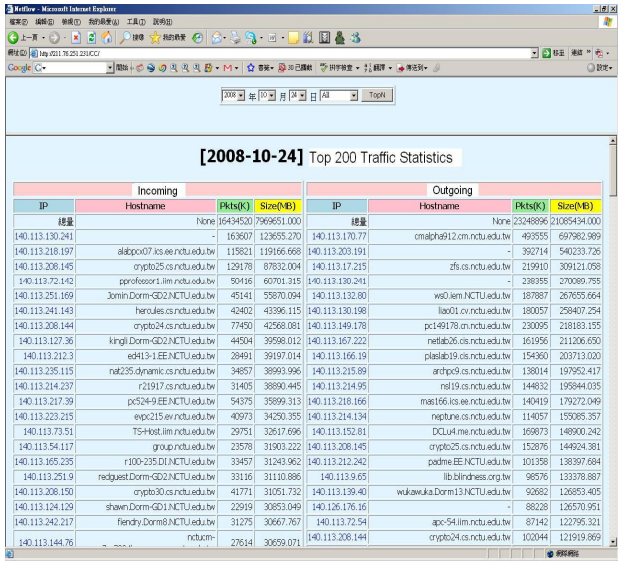

Fig.4: Traffic statistics (Netflow) from NCTU campus network.

■ 網路流量輔助管理系統

As shown in Fig. 5, we also install some other kind of network service control

platforms for conducting high-capacity stateful application and session-based classification and control of application-level IP traffic per subscriber [6].

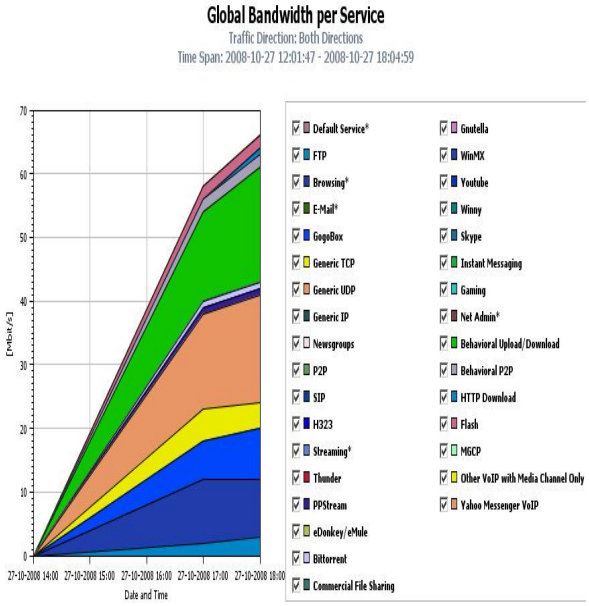

Fig.5: Global Service Type Distribution on NCTU Campus Network

- **The P2P-Network-Architecture Ontology**

Fig.6 shows the skeletal model of the P2P-network ontology. Based on the P2P-network ontology hierarchy, we could construct the following heuristic rules to help improve the network performance.

- Heuristic 1: Adjust the network infrastructure to facilitate P2P applications and benefit most users of typical Internet sites.

As mentioned above, P2P traffic dominates most of the Internet traffic. We could collect the required statistics by conducting typical Netflow traffic analysis and DNStop traffic analysis.

- Heuristic 2: Build a symmetric network infrastructure to facilitate P2P computing.

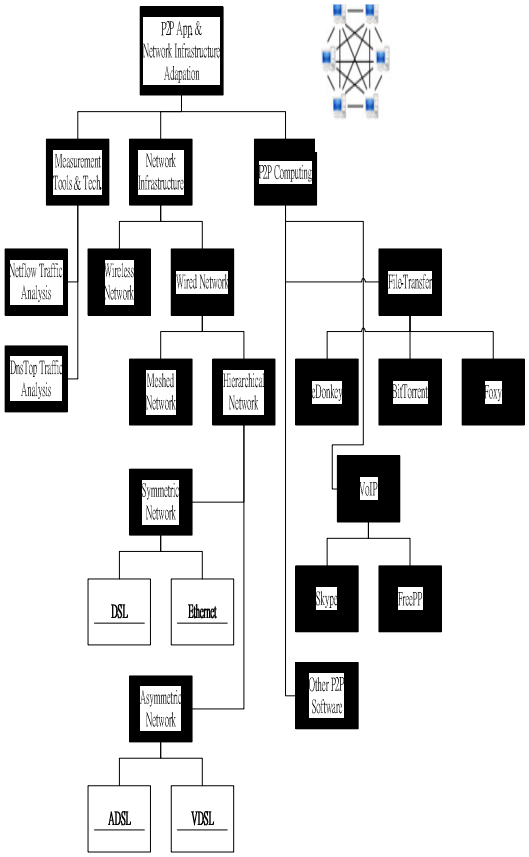

Fig. 6: The skeletal model of the P2P-network ontology.

Currently, most of the typical users (e.g., SOHO, home user, etc.) of Taiwan domestic ISPs use ADSL services. In practice, the bandwidth of the download capacity of typical ADSL is much higher than the upload capacity, which is not very good for conducting P2P computing tasks. As mentioned before, symmetric network rather than asymmetric network (e.g., ADSL) is more suitable for conducting P2P applications. It is highly suggested that ISPs had better upgrade (or replace) current ADSL services with other xDSL services to have a better support of P2P applications.

- Heuristic 3: Build meshed network (e.g., fully or partially meshed) to enhance the network performance.

P2P application routings are primarily based on user communities rather than on

conventional network routings (e.g., determined by network administrators). For example, as most people know, BitTorrent starts with a random set of peers, but then prefers peers that deliver better bandwidth. Therefore, it is very helpful to build meshed network to neighboring sites since these users share lots of similar interests on common things (e.g., language, culture, geographical areas, etc.).

- 討論

網路行為改變很快，建構網路者如何因應，提供網路服務平台者如何因應，毫無疑義地要優先適應網路主流應用[1][2]。在實務運作的觀察上，P2P 應用在抓取資料後會同時分享給許多人，因此對稱式網路架構下的使用者，往往會成為出超的資訊提供者。相對而言，非對稱式架構(如 ADSL)的使用者，則容易成為入超的資訊擷取者。根據交大使用 ADSL 的經驗觀察與分析，非對稱式 ADSL 限制了使用者 P2P 應用，使用者外送頻寬不足，限制了使用者抓取外部資料的效率。國內 ISP 使用者大部分為 ADSL 用戶，下載頻寬大於上傳頻寬，對於 P2P 運作模式不利。相對而言，固網業者、ISP 如果能建構對稱式網路，再搭配扁平式網路架構，對 P2P 應用負擔最小，更能滿足使用者需求。

五、初步計畫成果自評

本研究試圖探討主流 P2P 應用以及現今各單位網路架構的關聯，透過 P2P 統計資料的建立與流量的搜集與分析，結合 DNS 查詢記錄的關連性探討，進而發掘出校園網路應用的中長期使用趨勢，可以用來作為資源調整重新配置的依據。例如，可以透過這一些統計資訊，評估時作類似 DNS load balancing 系統[2]、影音 Streaming Server 的網路規劃與 Server 配置，因應長期使用趨勢變遷，以改善相關系統的使用效能。

目前本計畫的研究成果，共計發表兩篇會議論文[2][5]，本研究的產出結果，將可用於促進整體網路使用效能(performance)，提高可用度 (availability)，以及可延伸調整(scalable) 等功能。最後，感謝此計劃的推動及補助，能讓該研究相關領域有更進一步的探討及進展。

參考文獻

[1]. 劉大川，“P2P 對網路架構的影響”, in Proceedings of TANet2007 conference, Oct. 22-24，2007。

[2]. 蘇俊憲、陳昌盛，"CDN 服務與 DNS 最佳化對網路使用效能之影響"， in Proceedings of TANet2009 conference, Oct 28-30，2009。

[3]. ADSL overview, http://en.wikipedia.org/wiki/ADSL

[4]. Albitz, P. and Liu, C. (2001). DNS and BIND 4th edition, O'Reilly & Associates, Inc., Sebastopol, CA, 2001

[5]. Chang-Sheng Chen (陳昌盛), Ta-Chung Liu (劉大川), Chun-Shian Su (蘇俊憲), " Exploring the correlation between P2P Applications and Network Architecture", in Proceedings of ICACT2009 conference, Feb 15-19, 2009, Korea.

[6]. Cisco SCE (Service Control Engine) systems, http://www.cisco.com/en/US/products/ps6151/, Retrieved on Oct. 26, 2008

[7]. Mockapetris, P., "Domain Names - Concepts and Facilities," RFCs 1034, November 1987.

[8]. Roger Clarke, “*Peer-to-Peer (P2P) - An Overview*”, accessed on March 2, 2006, http://www.anu.edu.au/people/Roger.Clarke/EC/P2POview.html.

[9]. S.C. Yang , L.M. Tseng, “Flow-based P2P Traffic Measurement (Chinese)”, in Proceedings of TANet2007, Oct. 22 – Oct.25, 2007

附件 - ICACT2009 學術會議成果報告表

填表日期：98 年 03 月 16 日

會議名稱	(中文) 第 11 屆先進通訊技術國際學術研討會 (英文) The 11th International Conference on Advanced Communication Technology (ICACT 2009)
主辦單位	中文:電機電子工程師學會第十區分會(韓國) 英文: IEEE (Institute of Electrical and Electronics Engineers) Region 10
贊助單位	中文: 電機電子工程師學會 (美國) 英文: IEEE (Institute of Electrical and Electronics Engineers)
會議地點	韓國、江原道、平昌郡 (in Phoenix Park, Gangwon-Do, Republic of Korea.)
會議時間	98/02/15~18
參加對象及人數	國立交通大學計算機與網路中心陳昌盛副教授 1 人
國科會經費預算	60,000 元

會議成果	一、參加會議經過 2009/02/14 08:00 AM ~ 20:30 PM 從台灣啟程，傍晚投宿南韓首爾市的飯店。 2009/02/15 ■ 09:00 AM ~ 05:30 PM 從首爾市出發搭車到 ICACT 2009 會場辦理報到手續，並參加下午場次的講座。 2009/02/16 ■ 9:00 AM ~ 12:30 PM，參加上午場次的分組論文發表，並發表論文(1F 場次, 09:00-10:20 AM)。 ■ 2:00 PM ~ 05:30 PM 參加下午場次的分組論文發表活動 2009/02/17 ■ 9:00 AM ~ 12:30 PM，參加上午論文發表場次並發表論文 ■ 2:00 PM ~ 5:30 PM 參加下午場次的分組論文發表活動 2009/02/18 ■ 9:00 AM ~ 12:30 PM 參與研討會各項分組論文發表活動 ■ 下午離開會場，傍晚再次投宿南韓首爾市的飯店。 2009/02/19 ■ 08:30 AM 賦歸 二、與會心得 IEEE（電機電子工程師學會）所共同舉辦的 2009 年先進通訊技術國際學術研討會，屬於網路與通訊相關領域重要的研討會活動之一。會場為韓國的鳳凰渡假村，會議期間除了參與研討會之議程外，休息時間也可直接與各種學術人才交流與溝通。本次會議期間除了接觸到不少來自台灣地區北中南(台大, 成大, 義守大學等)師生，也接觸到許多臨近地區包含南韓、越南以及大陸地區的許多師生（上海交大等），與會收穫極為豐富。 會議期間，除了發表論文演講外，本人也負責主持兩場資訊安全有關論文發表，從中對國際性研討會的進行及論文發表方式，學到不少的經驗。本次會議期間，整體觀察，中國大陸地區師生研究投稿類似 ICACT2009 的國際會議的比率，已經顯著提高。其次，除了與國外學者專家、論文發表的研究生進行心得交換，吸收許多網路及通訊相關技術發展知識外，過程中也結交不少外國友人，增加不少對鄰近國家風土人情的認識。尤其與在東亞各國在通訊與網路有深入研究國家的教授及學生深談，進一步了解國際間其它國家的發展，以利未來相關研究的進一步思考。 最後，與會期間晚上也利用時間，與同樣來自台灣地區的師生，相約參觀此一美麗的渡假村，同時也欣賞難得雪景，為此國際研討會之行留下許多美好回憶。 三、攜回資料名稱及內容 ICACT2009 第 11 屆先進通訊技術國際學術研討會論文光碟