行政院國家科學委員會專題研究計畫 期中進度報告

SMART-校園生活無線通無限學 技術研發與應用(2/3)
期中進度報告(精簡版)

計 畫 類 別 ： 整合型
計 畫 編 號 ： NSC 95-2218-E-002-038-
執 行 期 間 ： 95 年 11 月 01 日至 96 年 10 月 31 日
執 行 單 位 ： 國立臺灣大學電機工程學系暨研究所

計 畫 主 持 人 ： 顏嗣鈞
共 同 主 持 人 ： 趙涵捷、許素朱、郭斯彥、雷欽隆

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 96 年 09 月 07 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

SMART-校園生活無線通無限學技術研發與應用(2/3)

計畫類別：☐ 個別型計畫　　☑ 整合型計畫
計畫編號：NSC 95-2218-E-002-038
執行期間：　95 年　11 月　01 日至　　96 年　10 月 31 日

計畫主持人：　顏嗣鈞
共同主持人：趙涵捷　、許素朱　、郭斯彥　、雷欽隆
計畫參與人員：

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
☐赴大陸地區出差或研習心得報告
☑出席國際學術會議心得報告及發表之論文
☐國際合作研究計畫國外研究報告書

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：

中　華　民　國　　96 年　　8 月　　30 日

摘要

本計畫以科技人文整合與校園生活應用為出發點，整合不同領域之優秀團隊（包括台灣大學電機系、東華大學電機系、宜蘭大學電機系、台北科技大學資工系、台北藝術大學科技藝術研究所），建構先導示範性應用，落實人文科技在日常生活的應用與實際佈建，開啟智慧型生活的新時代。本年度第二期的計畫成果包括安全寰宇隨插即用技術與 IPv6 之寰宇隨插即用技術的開發，以及智慧型“校園生活無線通無限學”示範應用之基礎建設。

Abstract

For the concept of the Integration and the application in the campus from the technologies and humanities, top groups from E.E. Dept. National Taiwan University, E.E.Dept. National Dong Hwa University, CSIE Dept. National Taipei University of Technology, and Graduate School of Art and Technology, Taipei National University of the Arts are jointed to construct the demonstration for application of the humane technologies in the daily life. The achievements in this year consist of the developments of the Secure UPnP technology (SUPnP), UPnP technology over IPv6, and the infrastructure of the SMART campus.

ggggggggggg

報告內容

一、前言

伴隨著科技的演進，現代的都會生活變得格外忙碌，人們對於資訊的取得以及操作需求量日益劇增，數位內容與無線網路相關技術的日漸成熟，智慧型生活之呈現已經不再是電影與科幻小說中才能見到的遙遠夢想。大學校園生活是年輕學子追求完整學習與實現夢想的最佳園地。怎麼把已日漸成熟之高科技落實應用於校園生活，讓校園中的每個人無論在資訊的搜取獲得更容易、在學習效益能更起勁，讓校園變成一個創意學習生活空間。這是值得我們努力思考的課題。

本計畫以科技人文整合與校園生活應用為出發點，整合不同領域之優秀團隊（包括台灣大學電機系、東華大學電機系、宜蘭大學電機系、台北科技大學資工系、台北藝術大學科技藝術研究所），刺激與創造技術、創意與人才整合之契機，挑戰新一代科技生活所需的各項尖端技術，將通訊無線化、影音寬頻化、內容數位化，建構先導示範性應用，落實人文科技在日常生活的應用與實際佈建，開啟智慧型生活的新時代。

二、研究目的

智慧型校園其應用的範圍很廣，各種情境需要不同 I/O 介面以及相對應的技術，其中有多種新技術待研發、測試，以及整合。在前一年的計畫中，本團隊已經完成了資料庫與通訊協定介面開發，內容包括行動裝置感測定位技術、無線網路多媒體閘道器、IPv4/IPv6 NAT-PT 技術、以及 UPnP 通訊介面與智慧型家電控制器的開發。本計畫第二期的主題為智慧型控制系統與週邊系統整合，其具體目標分為下列各項：

1. Secure UPnP 架構

校園個人化資訊系統設計的理念除了讓使用者能夠方便快速地獲得個人化的資訊之外，對於服務提供者而言，我們也希望能降低資訊整合的門檻，並達到可以動態新增、移除或管理其服務的功能。因此本系統採用 Universal Plug and Play (UPnP)的架構做為底層傳輸管理的

平台。此外，一套個人化資訊系統要能付諸實行，b 資料傳輸時的安全性與隱密性是不可或缺的一環。原本的 UPnP 架構並沒有任何的加密與驗證機制，因此我們將現有加密機制整合進 UPnP 平台，利用階層式架構(layered structure)的觀念，設計出一套建置在 UPnP 之上的 Secure UPnP(SUPnP)架構。這套架構除了提供 UPnP 架構的加密與驗證機制之外，亦需要包含一套身份驗證的協定，並維持原本的 UPnP 架構中，具有彈性的用戶端與伺服器端新增與刪除的機制。

2. IPv6 基礎環境架設

目前在 IPv4 上已經有許多設備及應用程式支援 UPnP 的協定，例如：Windows XP, MSN messenger 等，但是 IPv6 支援 UPnP 的設備相對來說比較缺乏，並且有必要的必須重新實作在 IPv6 上 Control Point 及 UPnP。為提供 IPv6 環境下 UPnP 架構的實驗環境，有必要進行 IPv6 的 UPnP 架構基礎環境的架設。

3. IPv4/IPv6 轉換閘道器之實現

使用 UPnP 除了可以方便的找到裝置及服務外，最終的目的是使需求端和服務端可以 P2P 的溝通，所以更需要 NAT-PT，DNS-ALG 及 UPnP-ALG 等技術來做為 IPv6/IPv4 之間溝通的橋樑。

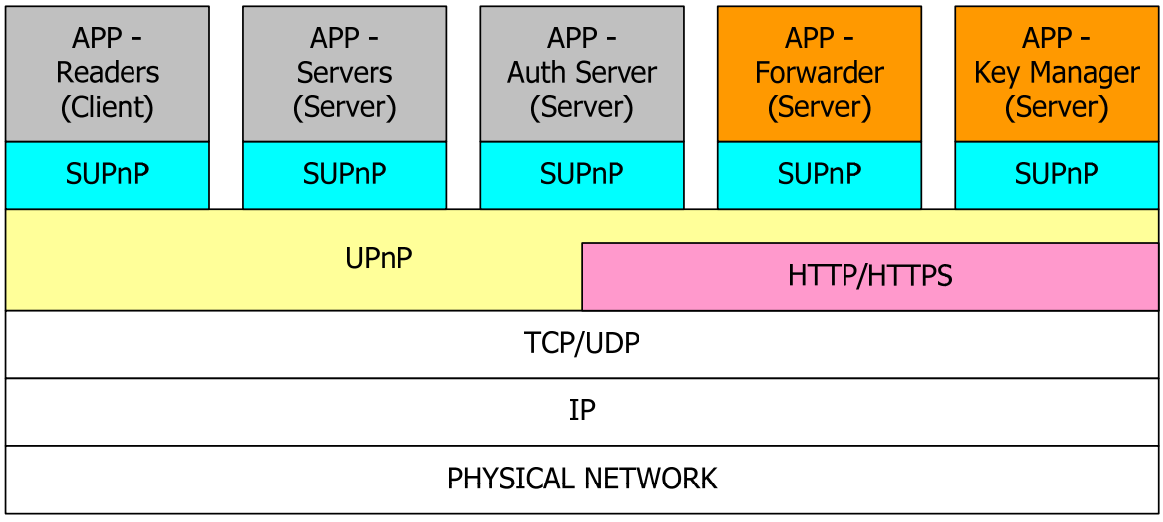
4. 智慧型“校園生活無線通無限學”示範應用之基礎建設

以前二期開發與整合的技術為基礎，在第三期的計畫中，以智慧型「校園生活無線通無限學」為主軸，配合人文啟發之思量、藝術造型之設計，讓所有技術、設備嵌入校園之生活機具中。經過「互動式數位造型」設計讓校園生活的機具如校園地圖導覽、單位公佈欄、…等具有數位資訊搜尋或學習功能，甚至形成「公共藝術」融入校園環境，達到校園美化目的。考量人文啟發與藝術要融入校園環境需要時間蘊釀，在技術面我們需先行架構示範應用所需之基礎建設，並設計多項腳本，以期在後續的計畫中，人文與藝術的元素可以越過技術的門檻，融入校園的環境中。

三、研究成果

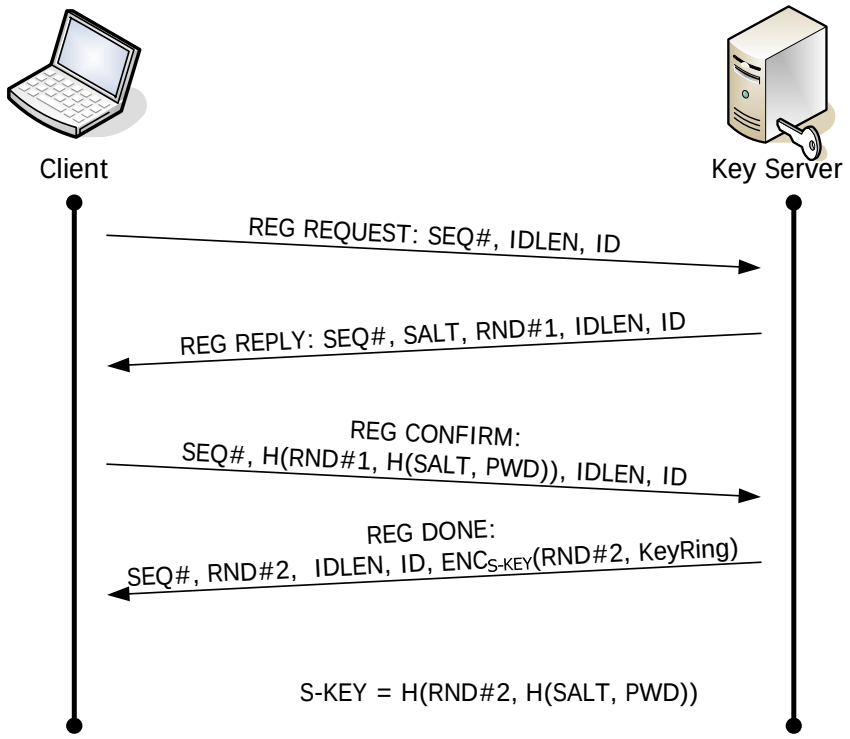
1. Secure UPnP 架構

我們所設計的建置在 UPnP 之上的 Secure UPnP(SUPnP)架構，如圖一所示。架構於 SUPnP 上層的各種應用伺服器只要以 SUPnP 所提供的 API 取代原本 UPnP 的 API，發送 UPnP 訊息時即具備加密傳輸的保障。另一方面，SUPnP 實做時採取將 UPnP 原有之 API 加以包裝，因此底層的 UPnP 也不需要做任何的更動，在管理維護上更為容易。



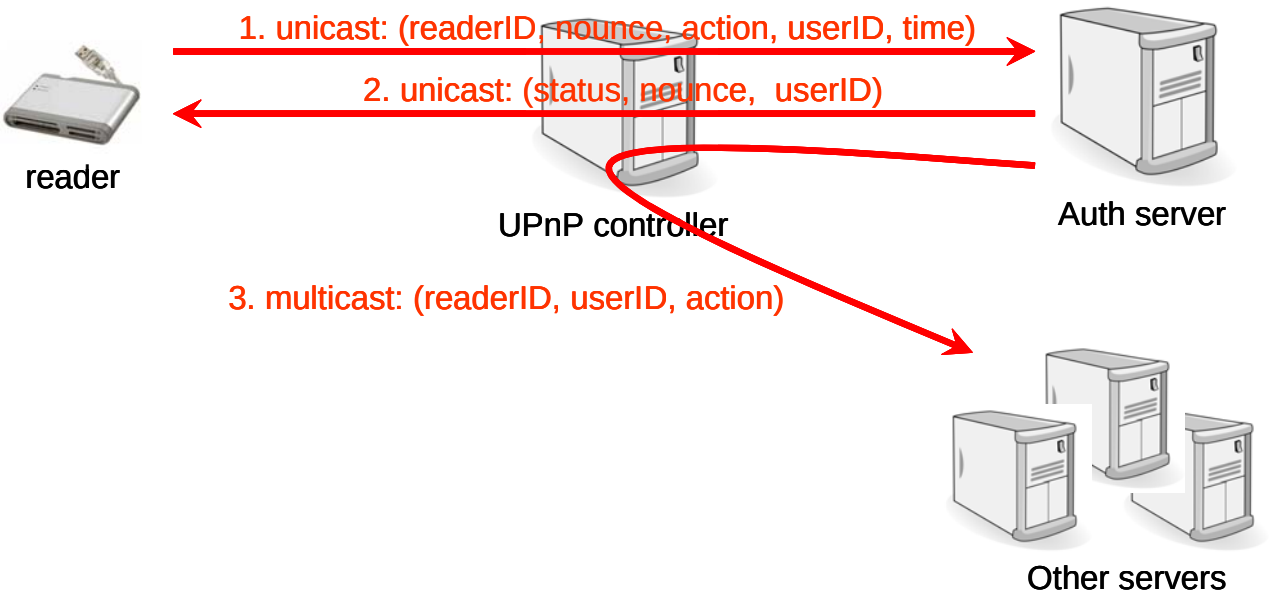
圖一 SUPnP 架構圖。

因應 UPnP 環境下用戶端-控制端(client to control point)與控制端-伺服器端(control point to server)封包傳送方式的不同，SUPnP 提供了點對點(unicast)和群播(multicast)兩種不同的加密方式，由控制端扮演加密轉換的角色。在群播金鑰管理的部份，我們採用著名的邏輯金鑰分配(Logical Key Hierarchy, LKH)來管理群播金鑰的更新與發配。另一方面，為了避免惡意裝置的入侵，每個新加入系統的裝置，不論是用戶端終端機或是後端伺服器，均需透過圖二所示之裝置註冊程序，向金鑰管理伺服器取得加解密金鑰後，才能與系統內其他裝置進行溝通。



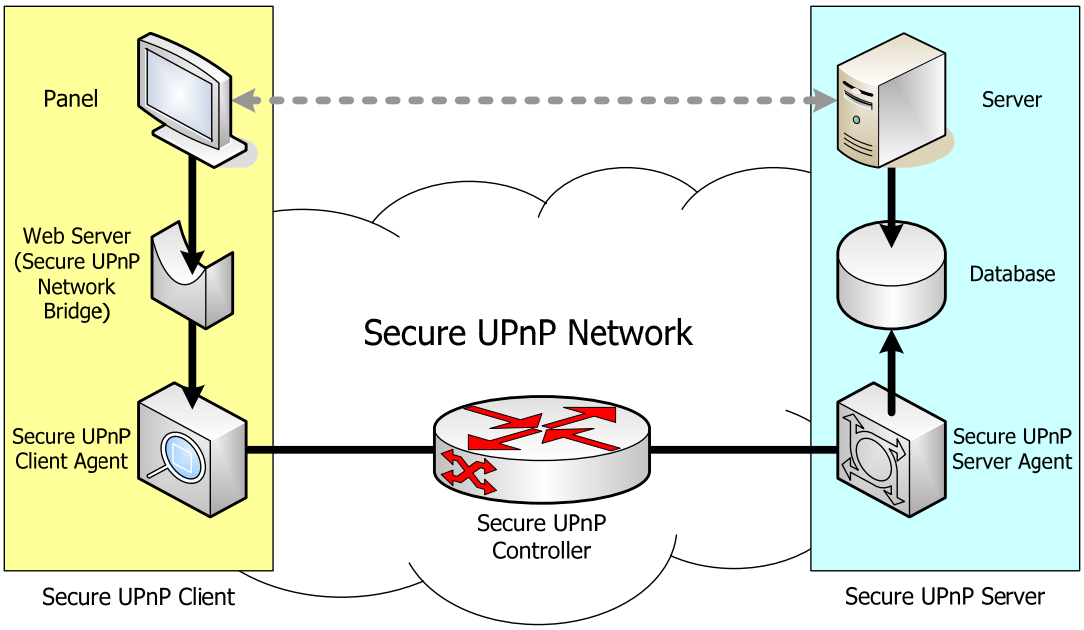
圖二 裝置註冊程序。

個人化服務是本系統開發的宗旨，為了確認使用者的身份，保障私密資料不被外人竊取，我們也設計了一套身份驗證的協定。當使用者抵達建置於校園各處的操作面板時，透過使用者事先申請的身份辨識裝置，例如 smart card 或 RFID 等，即可向遠端的認證伺服器進身份驗證的程序。圖三為認證流程的示意圖，通過身份驗證後，使用者便能進一步操作個人化的各項服務。



圖三 使用者身份驗證程序。

為了使資訊提供者(content provider)能夠在不需要清楚底層 SUPnP 架構下方便地將自己的服務整合進校園個人化資訊系統，我們在用戶端與伺服器端均提供了一套應用程式。



圖四 SUPnP 用戶端與伺服器端系統架構圖。

如圖四，使用者在用戶端點選某項服務後，使用者發出的請求會先透過架構於本地端的網頁伺服器(SUPnP 網路橋接器)做第一次的內容解析，找出裡面所有需要透過 SUPnP 網路向後端伺服器群組發送的訊息，再經由 SUPnP 用戶端代理程式對底層的 SUPnP 網路傳遞請求。經過 SUPnP 控制端的轉密後，這些請求會被相對應的伺服器透過 SUPnP 伺服器端代理程式上傳至資料庫，進行搜尋、組織等動作，待資料庫將資訊備齊後，會將產生好的網頁儲存在伺服器端，並透過 SUPnP 傳回該網頁的 URL 連結。用戶端的網頁伺服器收到傳回的 URL 連結後，便直接至伺服器端取回完整的網頁，再將資訊呈現在使用者面前。這樣設計的優點在於，大量的網頁內容並不會透過 SUPnP 直接傳回給使用者，可大幅減輕 SUPnP 控制端的轉密負擔，增加系統執行效率與穩定性。

詳細關於 SUPnP 的研究成果，已整理成 Design and Implementation of Secure Communication Channels over UPnP Networks 論文，並在南韓首爾舉辦的 2007 International Conference on Multimedia and Ubiquitous Engineering 國際會議上發表。

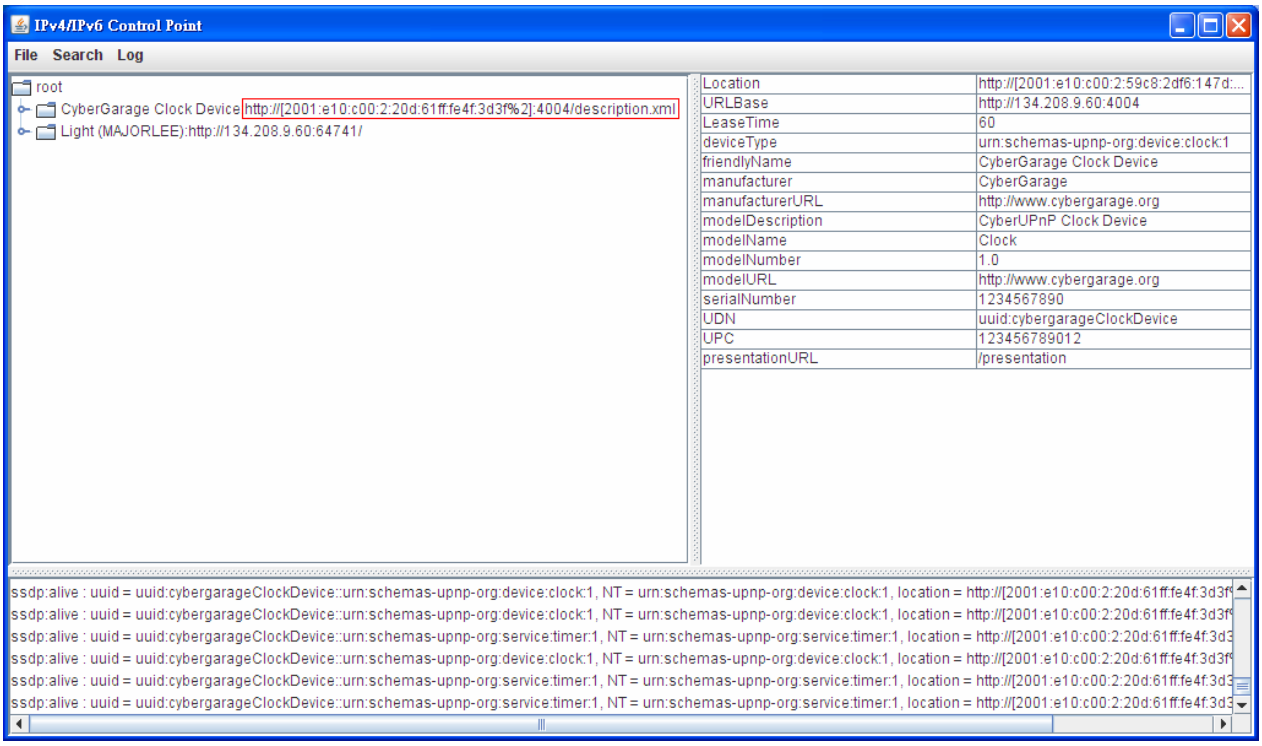
2. IPv6 基礎環境架設

UPnP 協定的網路作業可分為 Addressing, Discovery, Description, Control, Eventing 及 Presentation。而在 UPnP 在 IPv6 的網路環境需注意的項目如下：

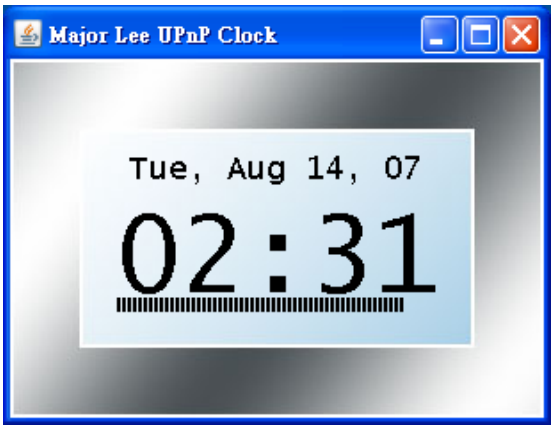
- Addressing：IPv6 的位址是採自動設定的方式。而在 UPnP 的協定下，需使用到 link-local 位址，multicast 位址及 global link 位址。
- Discovery：Control point 和 Device 需加入 [FF02::1]:1900 此一廣播群組。Control point 可藉由 SSDP 的 M-SEARCH 命令，搜尋區網內的 UPnP Device；UPnP device 可以以 SSDP NOTIFY 命令回覆。
- Description : Description 是 UPnP device 功能文件，功能說明是以 XML 的格式。 Control point 藉由 Discovery 階段所取得的 Location (例如: http://[2001:e10:c00:2:20d:61ff:fe4f:3d3f%2]:4004/description.xml)，以 HTTP GET request 取得 UPnP Device 的 XML 說明文件。

- Control: 在 UPnP 中，Control Point 是透過 SOAP 協定對 UPnP Device 控制或取值。而控制的 URL 是於 Description 的 XML <service>中的<controlURL>發佈。Control Point 可執行的動作共有，Action: Invoke, Action: Response, Query for variable, Query:Invoke, Query:Response。而 Control point 送出的 XML 命令，SOAL 的命令是包含 HTTP headers 和 XML 的 Envelop body
- Eventing: 由於 Control point 會從 UPnP device 讀取某個參數值，但於過程中，UPnP device 的參數值會隨時間而改變，造成 Control point 和 UPnP device 參數值的不一致，此刻是以 Event 動態通知 Control point 以更新數值。但是有即時通知的功能，Control 需事先向 UPnP device 要發出 Subscription 的訊息。
- Presentation: 僅是一個單純的網頁檔，用來說明 Device 的要呈現的內容及控制的方式。

IPv6 UPnP 必需支援 link-local 位址作為預設的設定；這表示可以在 Control Point 和 Device 可以在 Discovery 階段由 FF02::C 群播位址聽取及廣播 SSDP 的訊息。圖五是 IPv6/IPv4 UPnP Control Point，圖六是 IPv6 Sample Clock；結果顯示 IPv6 UPnP Control Point 可以偵測到網路上的 Sample Clock UPnP device 的訊息。



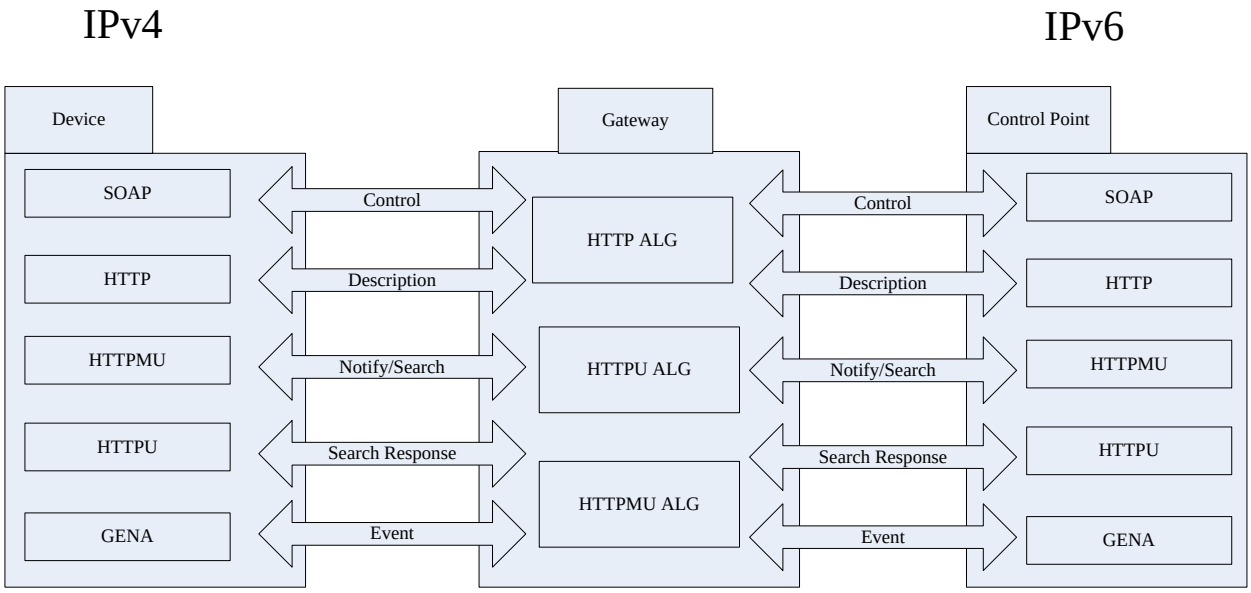
圖五 IPv6 UPnP Control Point



圖六 IPv6 UPnP Device : Sample Clock

3. IPv4/IPv6 轉換閘道器之實現

UPnP IPv6/IPv4 轉換閘道器只需實現應用程式層之資料轉換即可;更進一步的說明,UPnP 在網路化的過程的 6 個步驟：Addressing, Discovery, Description, Control, Eventing 及 Presentation，除 Addressing 是屬於 IP 層外，除於之步驟可以以應用程式閘道器的方式實現，在應用程式閘道器中，HTTP Application Level Gateway(ALG)模組，HTTPMU/HTTPMU ALG，運作原理如下：



圖七 UPnP IPv6/IPv4 轉換 Gateway

UPnP gateway 應該使 UPnP Control point 及 Device 在 IPv4 與 IPv6 的網路環境下可以雙向溝通。為了說明方便，以 UPnP IPv4 Device 與 UPnP IPv6 control point 之轉換做為範例。

a. HTTPMU Application Level Gateway 模組

在 HTTPMU 在 IPv4 的網路環境下，是使用 239.255.255.250:1900，在 IPv6 下是使用 [FF02::C]:1900。所以當為讓 IPv6 Control point 可以聽到 IPv4 device 的群播訊息，會對 Gateway IPv4 的 multicast HTTP 訊息進行轉譯,此外要將 Location 的 URL 轉換為 IPv6 gateway 的代理網址。

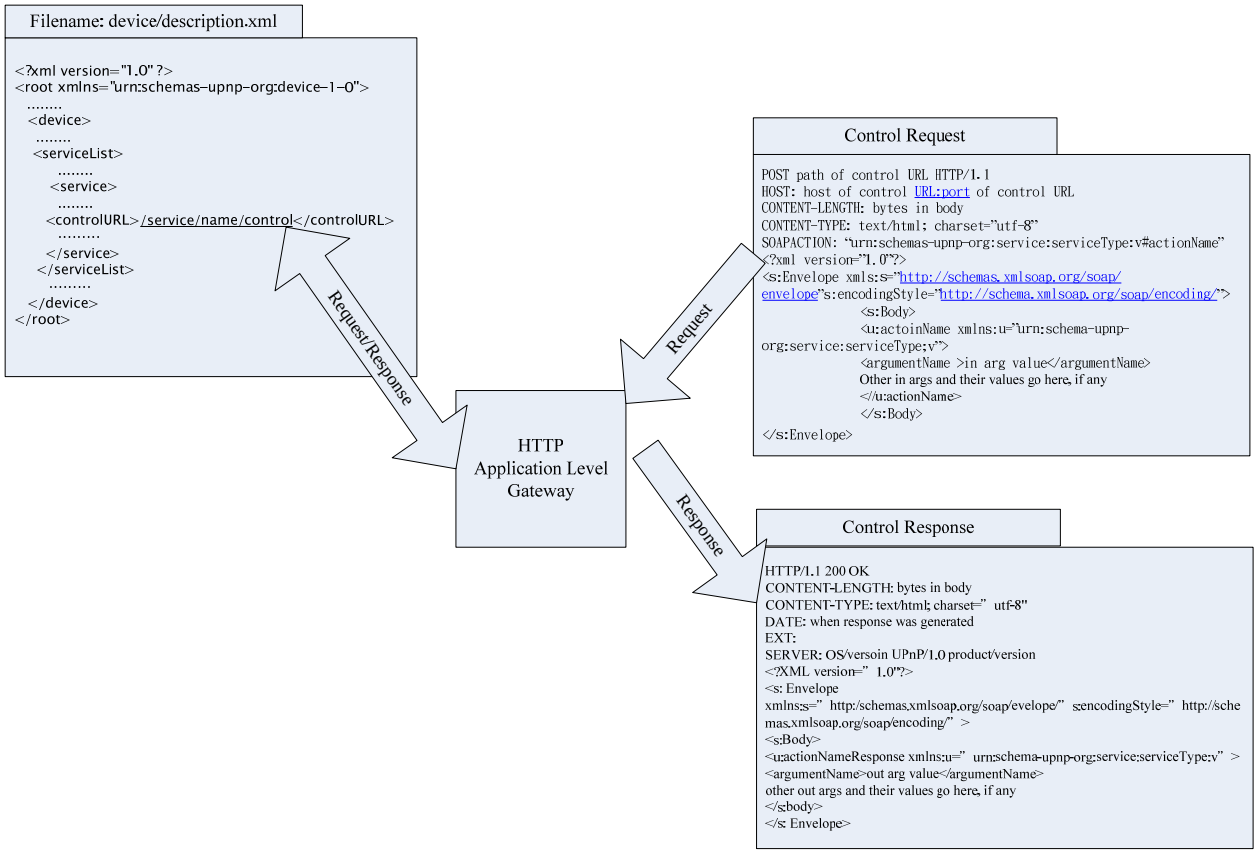
b. HTTPU/HTTPMU Application Level Gateway 模組

在 UPnP 在 IPv4 的網路環境下，是使用 239.255.255.250:1900，在 IPv6 下是使用 [FF02::C]:1900。所以當為讓 IPv6 的 Control point 可以聽到 IPv4 device 的群播訊息，會對 Gateway IPv4 的 multicast HTTP 訊息進行轉譯。

c. HTTP Application Level Gateway 模組

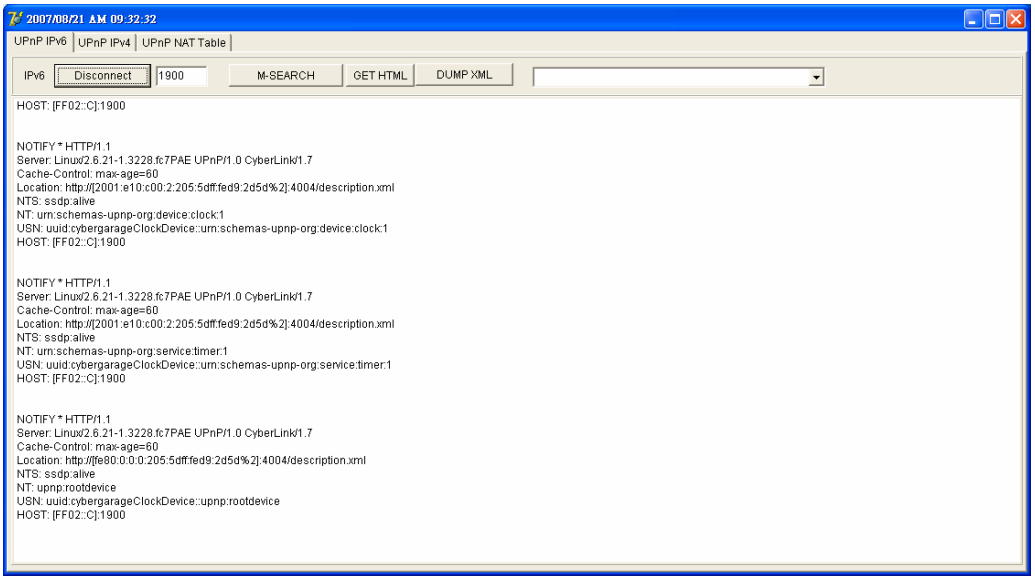
需兼具 HTTP ALG 及 Proxy 的功能。 在 IPv6 的網路環境中，Control point 會讀取 description, presentation 及 icon 的資訊,當 gateway 接收到此一命令時,會到相對應的 IPv4 UPnP device 讀回相對應的資訊，回應給 IPv6 control point。但是在 IPv6 網路端需將<URLBase>之 URL 轉至 gateway 相對應之網址，供 Control Point 進行讀取。另外於 Control 階段時，由於是透過 HTTP/SOAP (Web Service)的協定，動作於 description 和 presentation 類似。

IPv4 IPv6

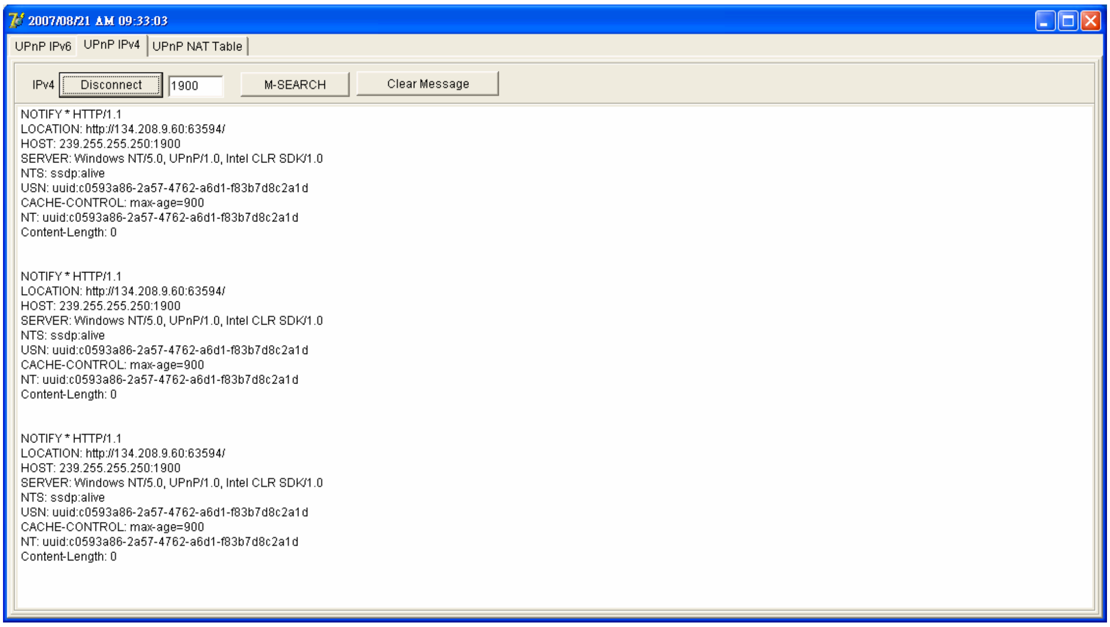


圖八 HTTP/SOAP

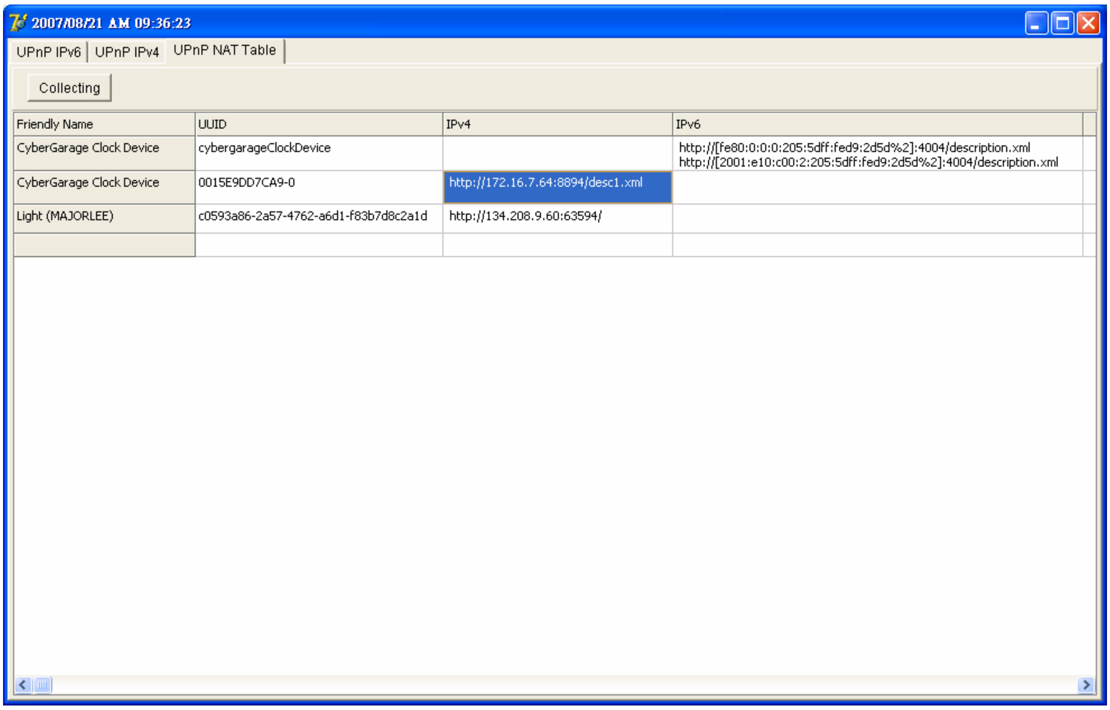
在 Control point 要接收 UPnP device 的 event 時，要先發出 subscribe 的動作。Subscription 的訊息仍透過 gateway 進行轉換，但是原本 CALLBACK 是以 IPv6 的 URL，gateway 會將之修改為 IPv4 的 URL，讓 UPnP device 可以通知此一 URL。在圖九、圖十及圖十一中，是 UPnP IPv4/IPv6 gateway 的實現，在此實現了 IPv4 及 IPv6 兩個介面，負責蒐集 UPnP devices，根據上述之各項原理，判斷 devices 所支援的 IP 協定，自動決定是否要進行 UPnP 各項網路之 IPv4/IPv6 之轉換動作。



圖九 IPv6 UPnP devices interface



圖十 IPv4 UPnP devices interface



圖十一 IPv6/IPv4 轉換

4. 智慧型“校園生活無線通無限學”示範應用之基礎建設

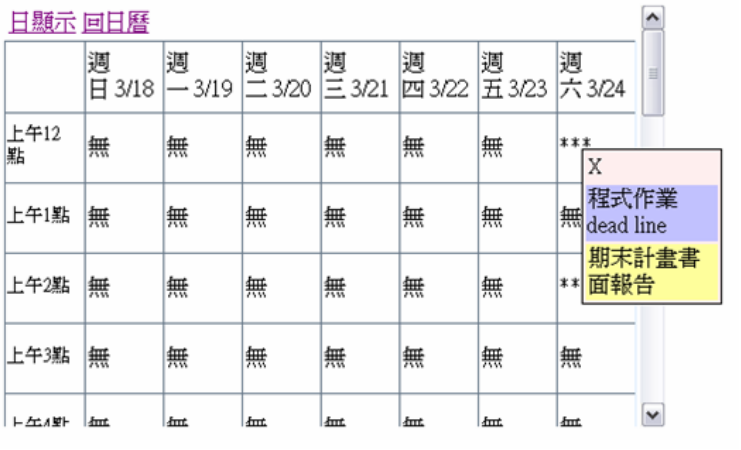
應用 SUPnP 架構，我們提出一個整合性的使用者操作平台，當各項服務加入 SUPnP 網路，這個平台可以動態地顯示使用者可以操作的服務。這個平台在示範應用的腳本中，將廣佈於校園的各個角落，其操作畫面如圖十二所示，使用者可以藉由觸碰式螢幕存取各項在平台上顯示的服務。

圖十二 應用 SUPnP 架構的使用者操作平台介面。

為示範此操作平台提供服務的彈性，我們設計了個人化校園資訊系統、個人化行事曆、以及智慧型校園導覽等基本服務。當註冊的使用者(例如在校學生)將個人的基本資料與個人偏好建檔之後，可以獲得個人化的基本服務。在個人化校園資訊系統中，使用者可以根據個人興趣與重要性顯示校園各項重大資訊，其介面如圖十三所示：

圖十三 個人化校園資訊系統

在個人化行事曆中，使用者可以管理自己的行事曆，加入個人化重要資訊，以利系統在適當時機對使用者加以提醒，其效果猶如個人之行動助理(如圖十四)。



圖十四 個人化行事曆的使用介面

在智慧型校園導覽系統中，使用者可以便利地檢索校園中重要地標，或藉由設定熱點，進行路徑規畫(介面如圖十五)。

圖十五 校園導覽系統的主頁

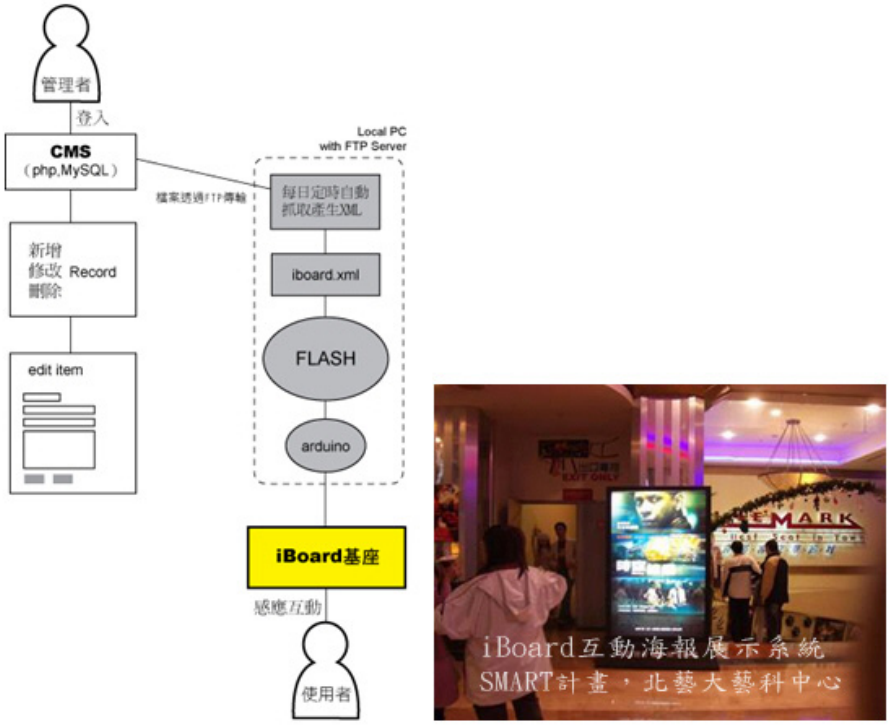
我們先行設計的三項基本服務在使用上均具有容易為其他服務所利用的特性。為驗證其易於利用的特性，這三項服務亦可彼此互相關聯，例如以下兩種腳本：

a. 當使用者操作校園資訊系統時，若校園資訊包含有地點的關鍵字，使用者可以藉由點選地點關鍵字的方式，直接進入導覽系統，以便查詢地點。若校園資訊包含有時間的關鍵字，使用者可以將校園資訊的摘要依照時間加入個人的行事曆。

b. 當使用者操作校園導覽系統時，可以點選系統中的熱點，根據對應的地標，可以篩選校園資訊系統中與該地標相關的資訊，以利瀏覽(如圖十六)。

圖十六 校園導覽系統與校園資訊系統的整合

此一平台在新的年度，更將擴充 iBoard 互動海報展示系統，讓無人靠近海報看板時，就像是一個海報看板，但當有人靠近於一定距離內(約一公尺，視現場環境調校)時，海報則會開始改變畫面，可以是文字效果或是影片，但是如果要有特效，都必須另外在 Flash 裡面製作，可統一由上層 Flash 控制影格之播放。當影片播畢或是人離開偵測範圍時，將會結束影格之播放，並重新讀取資料庫。其架構如圖十七。



圖十七 iBoard 互動海報展示系統

附件一

許素朱教授參加 SIGGRAPH 2007 出差報告

許素朱教授參加 SIGGRAPH 2007 出差報告

一、 出差目的與行程說明：

ACM Siggraph 是全球最大的電腦圖學會議。其中 Emerging Technology 單元更是世界互動式科技發表的重要舞台。許素朱教授前往美國參加今年之 SIGGRAPH 2007。藉由參與 SIGGRAPH，了解國外最新互動式媒體傳播的趨勢及發展技術，與會期間並蒐集 Emerging Technology 單元作品資料，未來將可作為計畫執行參考。

三菱電機公司在美國的 MERL 國際研究實驗室，是全世界第一個研發多處點觸控面版 DiamondTouch。於 2006 年許素朱教授已得到三菱電機公司在美國的 MERL 國際研究實驗室的國際合作贊助承諾,提供台北藝術大學藝術與科技中心價值頗高的DiamondTouch 面版作為多點觸控互動研究，乃為國際合作跨出一步。今年於 SIGGRAPH 研討會中向 MERL 國際研究實驗室作簡單應用報告。

許素朱教授於 96 年 8 月 3 日至 96 年 8 月 9 日至美國聖地牙哥 SIGGRAPH 2007(國際電腦繪圖及互動式科技研討會)。出國差旅經費的其中五天生活費共 NT30,000 元由國科會「SMART 計畫-智慧型藝術校園與教學無線學」補助。

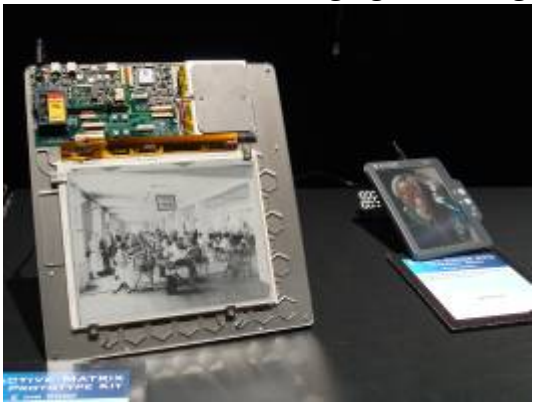
1. 聖地牙哥每日差旅生活費為 US$182（US$182x5 天 x 匯率 33=NT30030 元）
2. 其餘差旅費(機票與不足差旅費)由經濟部學界科專「數位創意生活應用技術研發」計畫補助。

二、 SIGGRAPH 2007：http://www.siggraph.org/s2007/

SIGGRAPH 2007 大會現場



SIGGRAPH 2007 –Emerging Technologies 部分作品



E Ink Electrophoretic Displays

E Ink 公司的電子紙張展示，將來將可應用至 visual medium. Electronic books, electronic billboards, watches, memory cards, smart cards, and shelf labels。

Globe4D

Universiteit Leiden 的四渡空間地球儀展示，運用投影並偵測地球儀被旋轉角度，即時呈現所對應位置影像。

附件二

雷欽隆教授出席 2007 IEEE 安全與隱私國際會議心得報告

出席 2007 IEEE 安全與隱私國際會議心得報告

雷欽隆

國立臺灣大學電機工程學系教授

會議名稱：2007 IEEE Symposium on Security and Privacy

會議地點：The Claremont Resort, Oakland, California, USA

會議日期：2007/5/20 – 2007/5/23

一、 參加會議經過

IEEE Symposium on Security and Privacy 會議今年依往例在美國加洲 **Oakland** 的 **Claremont Resort** 舉辦。**IEEE Symposium on Security and Privacy** 從 1980 年開始年年舉辦，此會議至今已是第二十八屆。今年 **IEEE Security and Privacy** 會議共有 249 篇論文投稿，Technical Program Committee 成員有 37 位，皆爲一時之選。經過審稿過程，最後選出 29 篇論文。這些論文分別在三天（5/21 ~ 5/23）八個 sessions 發表，會議議程如下：

Monday, May 21, 2007

7:30-9:00	Continental breakfast
9:00-9:15	Opening Remarks (Deborah Shands, Birgit Pfitzmann)
9:15-10:15	Keynote Talk *Reflections on the Future of Security and Privacy* Peter G. Neumann
10:15-10:45	Break
10:45-12:15	Session: Network Security Session Chair: Birgit Pfitzmann *Accurate Real-time Identification of IP Prefix Hijacking* Xin Hu and Z. Morley Mao (30 minutes) *DSSS-Based Flow Marking Technique for Invisible Traceback*

	Wei Yu, Xinwen Fu, Steve Graham, Dong Xuan and Wei Zhao (30 minutes) *On the Safety and Efficiency of Firewall Policy Deployment* Charles C. Zhang, Marianne Winslett and Carl A. Gunter (30 minutes)
12:15-13:45	Lunch
13:45-15:30	**Session: Authentication** Session Chair: Tuomas Aura *The Emperor's New Security Indicators: An evaluation of website authentication and the effect of role playing on usability studies* Stuart Schechter, Rachna Dhamija, Andy Ozment and Ian Fischer (30 minutes) *Cryptanalysis of a Cognitive Authentication Scheme* Philippe Golle and David Wagner (15 minutes) *A Systematic Approach to Uncover Security Flaws in GUI Logic* Shuo Chen, José Meseguer, Ralf Sasse, Helen J. Wang and Yi-Min Wang (30 minutes) *Forward-Secure Sequential Aggregate Authentication* Di Ma and Gene Tsudik (15 minutes) *Extended abstract: Provable-Security Analysis of Authenticated Encryption in Kerberos* Alexandra Boldyreva and Virendra Kumar (15 minutes)
15:30-16:00	Break
16:00-17:30	**Session: 5-minute Work-in-Progress Talks** Session Chair: Yoshi Kohno
18:00-20:00	**Reception**

Tuesday, May 22, 2007

7:30-9:00	Continental breakfast

9:00-10:30	**Session: Privacy** Session Chair: Ninghui Li *Endorsed E-Cash* Jan Camenisch, Anna Lysyanskaya and Mira Meyerovich (30 minutes) *Network Flow Watermarking Attack on Low-Latency Anonymous Communication Systems* Xinyuan Wang, Shiping Chen and Sushil Jajodia (30 minutes) *Improving the Robustness of Private Information Retrieval* Ian Goldberg (30 minutes)
10:30-11:00	Break
11:00-12:15	**Session: Access Control and Audit** Session Chair: Dan Wallach *Beyond Stack Inspection: A Unified Access-Control and Information-Flow Security Model* Marco Pistoia, Anindya Banerjee and David A. Naumann (30 minutes) *Usable Mandatory Integrity Protection for Operating Systems* Ninghui Li, Ziqing Mao and Hong Chen (30 minutes) *Enforcing Semantic Integrity on Untrusted Clients in Networked Virtual Environments (Extended abstract)* Somesh Jha, Stefan Katzenbeisser, Christian Schallhart, Helmut Veith and Stephen Chenney (15 minutes)
12:15-13:45	Lunch
13:45-15:15	**Session: Information Flow** Session Chair: Anupam Datta *Information Flow in the Peer-Reviewing Process (Extended Abstract)* Michael Backes, Markus Duermuth and Dominique Unruh (15 minutes) *A Cryptographic Decentralized Label Model*

	Jeffrey A. Vaughan and Steve Zdancewic (30 minutes) *Gradual Release: Unifying Declassification, Encryption and Key Release Policies* Aslan Askarov and Andrei Sabelfeld (30 minutes) *Fuzzy Multi-Level Security: An Experiment on Quantified Risk-Adaptive Access Control* Pau-Chen Cheng, Pankaj Rohatgi, Claudia Keser, Paul A. Karger, Grant M. Wagner, Angela Schuett Reninger (15 minutes)
15:15-15:45	Break
15:45-17:30	Session: Host Security Session Chair: Crispin Cowen *Exploring Multiple Execution Paths for Malware Analysis* Andreas Moser, Christopher Kruegel and Engin Kirda (30 minutes) *Lurking in the Shadows: Identifying Systemic Threats to Kernel Data* Arati Baliga, Pandurang Kamat and Liviu Iftode (15 minutes) *ShieldGen: Automatic Data Patch Generation for Unknown Vulnerabilities with Informed Probing* Weidong Cui, Marcus Peinado, Helen J. Wang and Michael Locasto (30 minutes) *Minimal TCB Code Execution* Jonathan M. McCune, Bryan Parno, Adrian Perrig, Michael K. Reiter and Arvind Seshadri (15 minutes) *Using Rescue Points to Navigate Software Recovery (Short Paper)* Stelios Sidiroglou, Oren Laadan, Angelos Keromytis and Jason Nieh (15 minutes)
17:30-17:45	Break
17:45-18:30	Business Meeting

Wednesday, May 23, 2007

7:30-9:00	Continental breakfast
9:00-10:30	**Session: Hardware and Replication** Session Chair: Wenke Lee *Moats and Drawbridges: An Isolation Primitive for Reconfigurable Hardware Based Systems* Ted Huffmire, Brett Brotherton, Gang Wang, Tim Sherwood, Ryan Kastner, Timothy Levin, Thuy Nguyen and Cynthia Irvine (30 minutes) *Trojan Detection using IC Fingerprinting* Dakshi Agrawal, Selcuk Baktir, Deniz Karakoyunlu, Pankaj Rohatgi and Berk Sunar (30 minutes) *On the Optimal Communication Complexity of Multiphase Protocols for Perfect Communication* Kannan Srinathan, N. R. Prasad and C. Pandu Rangan (30 minutes)
10:30-11:00	Break
11:00-12:30	**Session: Encryption** Session Chair: Patrick McDaniel *Ciphertext-Policy Attribute-Based Encryption* John Bethencourt, Amit Sahai and Brent Waters (30 minutes) *Attacking the IPsec Standards in Encryption-only Configurations* Jean Paul Degabriele and Kenneth Graham Paterson (30 minutes) *Multi-Dimensional Range Query over Encrypted Data* Elaine Shi, John Bethencourt, T.-H. Hubert Chan, Dawn Song and Adrian Perrig (30 minutes)
12:30-12:45	**Closing Remarks** (Patrick McDaniel, Avi Rubin, and Yong Guan)
11:00-13:00	Boxed lunch

從議程的安排可以看出目前安全與隱私研究趨勢的主流在 Network Security、Authentication、Private Information Retrieval、Access Control and Audit、Information Flow、Host Security、Hardware Protection 及 Encryption 等。特別值得一提的是本次的 keynote speech 特別邀請 Prof. Peter G. Neumann 演講，講題是 *Reflections on the Future of Security and Privacy*，Prof. Neumann 細說安全與隱私過去 28 年之發展過程及各階段之重要成果及里程碑，同時也探討安全（系統、實務）與隱私（理論、密碼）兩派學者間之競合，十分精采，同時大會也特別配合，將過去在本會議發表的所有論文整理並製作成光碟。

本人於 5 月 20 日下塌 **The Claremont Resort**，直到 5 月 23 日都待在此地；並與參加會議的各國學者交換研究心得，特別是和 UC Berkeley Doug Tygar 等教授商討合作事宜。

二、 與會心得

此次遠赴美國參加會議，有數點心得：

1) 有不小比例的論文，都是自己定出一個新的題目，而不只是拿舊的題目繼續改進而已。一旦定出新的題目，對於該領域還是很有貢獻——因爲它延伸了這個研究領域的範圍。因此，日後除了專研原有的題目外，也應該多花一些時間來做「延伸思考」。

2) 好的研究通常會持續地延伸下去，不論在廣度或深度。它們不一樣的地方就是在「別人已經喊停的地方」堅持下去，這時就很可能出現很多不一樣的觀點或成果。

三、 建議

我覺得此次參加國際會議獲益良多，建議有志於學術研究的學者們多多爭取參加國際頂尖學術會議的機會。尤其整個會議是採用 Single session 方式進行，每篇論文都是精華，不論在研究，或是視野都有十分的助益。

四、 攜回資料名稱及內容

會議論文集一本

1980 ~ 2007 會議論文光碟片

附件三

趙涵捷教授參訪上海理工大學、北京交通大學等大陸學術單位進行交流活動心得報告

國立東華大學
專任教師出席國際學術會議報告

報告人姓名	趙涵捷	服務機構及職稱	國立東華大學電機所 正教授
會議時間		會議地點	
會議名稱	(中文) (英文)		
發表論文題目	(中文) (英文)		

報告內容應包括下列各項：

一、參加會議經過

二、與會心得

三、考察參觀活動(無是項活動者省略)

四、建議

五、攜回資料名稱及內容

六、其他

一、參加會議經過

本人本次出國的主要目的是代表計畫出訪中國大陸的數位發展相關單位，針對技術成果加以推廣，並與中國相關技術研發系所進行討論。同時在北京交通大學與山東煙台大學獲聘為兼任教授一職，未來希望持續加強學術領域之實質交流活動。期待能夠把創新生活運用的技術觀念帶給中國大陸的友好系所，並透過演講與座談的方式，透過腦力激盪延伸出新的運用與發展方向。本次參訪除了成功的完成推廣計畫成果的任務，同時也確立了兩岸學校實質合作的方向。

本次出國行程主要如下

4/21 由台北前往上海參訪上海理工大學與數位傳播內容發展單位。
4/24 由上海前往北京，至北方交大發表演說(並獲聘為兼任教授)
4/26 前往煙台大學拜訪,發表演說. (並獲聘為兼任教授)
4/28 返回台灣

4/25 於北京交通大學演講
4/25 經過昨天一個下午的準備，針對北京交通大學電子訊息學院的師生發表學術演說，內容著重在 Corss-Layer 的設計上。

在演講之前，首先獲頒北京交通大學兼任教授之榮譽聘書。並與副校長及合作的訊息學院院長與書記同時合影留念。透過實質上的師生互換，老師擔任兼任師資等動作，希望能夠加速兩校間的交流。

趙教授針對 CrossLayer Design 提出學術報告。

北京交通大學訊息學院對於本合作演說相當重視，所有學院之博士生均參加本次演講。演講後，學生提出很多問題與思考的方向。由於趙教授的實做經驗豐富，所以也針對相當多的實做問題提出解釋。舉例來說其中一個運用是無線定位技術，學生就提出為何不簡單使用三角測量來解決問題。而趙教授回應，基本上的大方向沒有錯，但是針對訊號之衰減考量並不是理想。所以考量到實際的狀況，還是有必要建立相對應之場強分佈圖。

會後首先拜會了李副院長，針對後續的實質合作進行協商。基本上確定了將來會以研究生為主進行實質交換。而今年度開始兩邊的研究生，將有少數挑選過領域相近的學生開始進行共同指導。

4/26 一早代表團飛抵煙台國際機場。煙台市給人的映像就是非常的乾淨與高度規劃設計之城市。而煙台大學就是山東區域的重點大學。

煙台大學校長頒發煙台大學聘書給趙涵捷教授。

趙涵捷教授針對數位創意生活發表專題演說。

當天現場聚集了相當多的學生。

同學們在會後針對感興趣的問題提出發問，包含了實用層面的考量與技術層面的問題。會場大家的共識是，其實技術上往往都已經有了相關的解決方案，重點是如何透過整合結合不同的技術來達成作品概念的表現。由於作品本身如果需要展示並商品化，技術的整合度就需要達到完善。同時考量到將來的銷售問題，所以某些技術需要自己發展或是客製化。

二、與會心得

自 1950 年至 2000 年，台灣地區的大專院校數由 4 所增加到 150 所，目前還有 29 所正在籌設中，但大多數都是學生人數少的小型新興學校或技術學院，超過 15000 名學生以上的綜合型大學只有 8 所。在教育經費得不到保證的情況下，依然在擴大辦學規模，導致了台灣學術品質的下降。研究顯示，台灣學生的學習動力、學習態度及語言能力逐漸落後亞洲其他國家或地區。

北京交通大學訊息學院的學生對於相關的合作演說相當重視，所有學院之博士生均參加本次演講。演講後，學生提出很多問題與思考的方向。由於本團隊的實做經驗豐富，所以也針對相當多的實做問題提出解釋。舉例來說其中一個運用是無線定位技術，學生就提出為何不簡單使用三角測量來解決問題。而趙教授回應，基本上的大方向沒有錯，但是針對訊號之衰減考量並不是理想。所以考量到實際的狀況，還是有必要建立相對應之場強分佈圖。

大陸的學生在所提出的問題，包含了實用層面的考量與技術層面的問題。感覺上已經逐漸有國際的水準。而台灣目前學生的優勢，應該是在整合與創意上。利用現有的技術上的解決方案，透過整合結合不同的技術來達成作品概念的表現。但是在研究的努力上，台灣的學生還是需要好好努力。

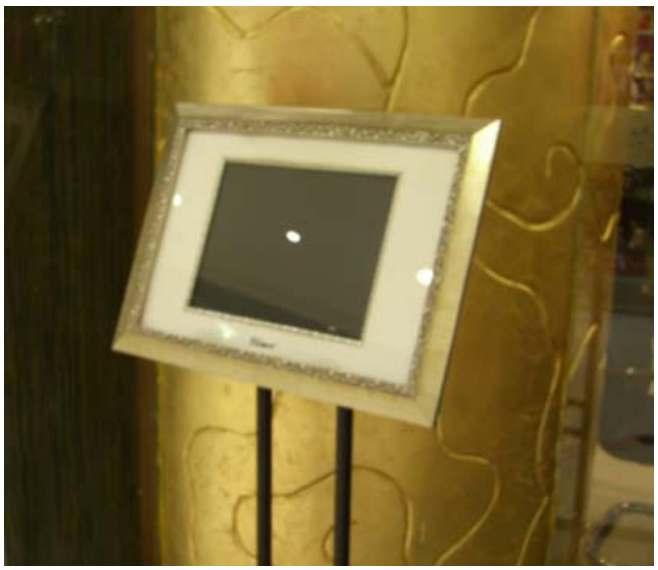
三、考察參觀活動(無是項活動者省略)

4/21 早上由台灣出發，在香港轉機後飛往上海

在香港機場轉機時，同時針對香港機場的導覽系統進行研究。針對目前計畫內設計之導覽系統加以比較，歸納出目前所作之導覽系統之優缺點，以作為後續改進之方向。香港的導覽系統具有初步之 3D 導覽功能，不過導覽系統本身的互動性與擴充性部分還有加強的空間，這也是本計劃所努力的方向。

目前在上海的街頭，可以發現相關的導覽與城市廣告等創意系統散佈於城市的各個角落之中。她們共同的特色是充分利用現有空間與設備加以延伸，結合數位化快速中央控制的廣告內容。

上圖是北京的電子廣告佈告欄，但是並不是獨立一個佈告欄，而是充分利用空間與電話亭整合。並透過電話亭的數據線路提供電源與統一傳遞數位畫面。



而在一般的餐廳門口，也不再只是過去死板的菜單；改以數位化之菜單結合豐富的照片介紹，提高顧客上門之意願。

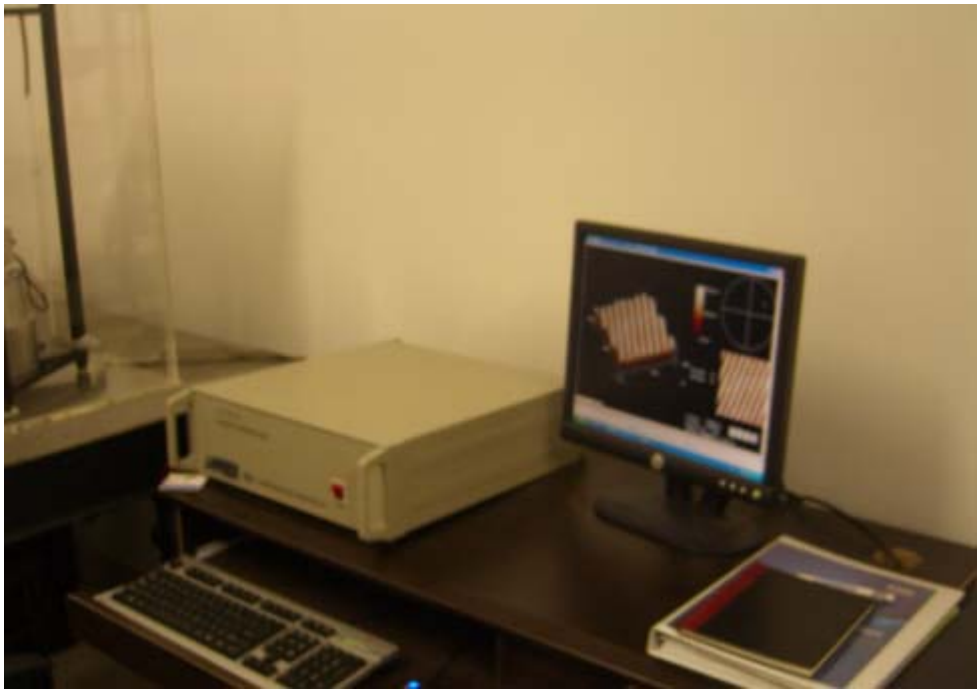
4/22 前往上海理工大學電子訊息工程學院進行訪問

在 22 號受邀前往上海理工大學電子訊息工程學院拜訪，宣傳計劃相關成果。並了解雙方進一步合作之可能。

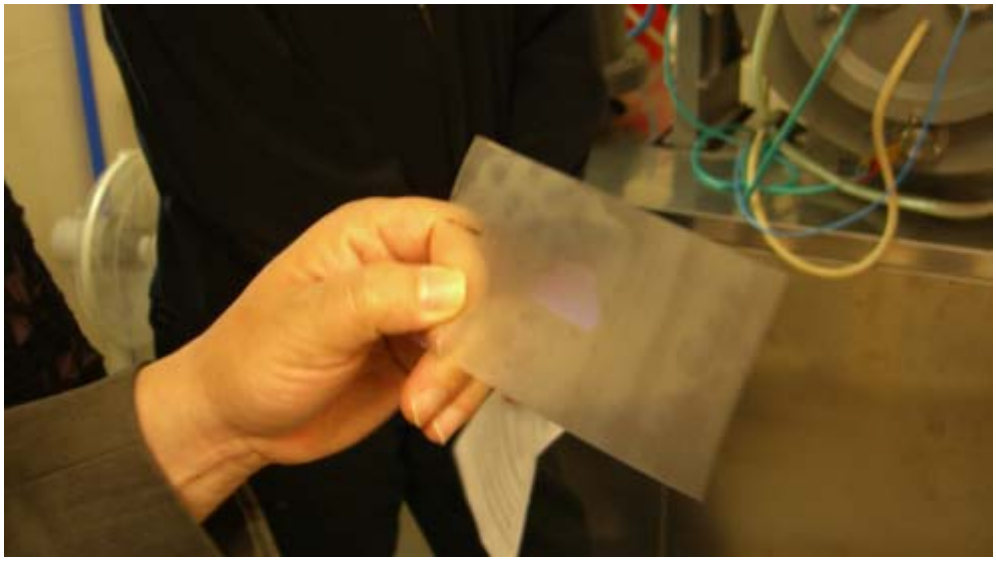
在本次拜會中，莊松林院長特別撥空了解本計劃之內容與具體成果。並特別針對上海理工大學與國立宜蘭大學之間的實質人員交換合作，做出積極努力的表示。目前正在針對ＭＯＵ合作協議的細節進行磋商。

莊院長與本人(趙涵捷教授)合影

接下來在院書記的陪同下參觀上海理工之科學研究之成果，並針對相關核心技術了解是否有運用在計畫中之可能。上海理工除了擁有大陸國家級的研發能量，參與國防高端研究，並擁有獨立之國家量測實驗室。



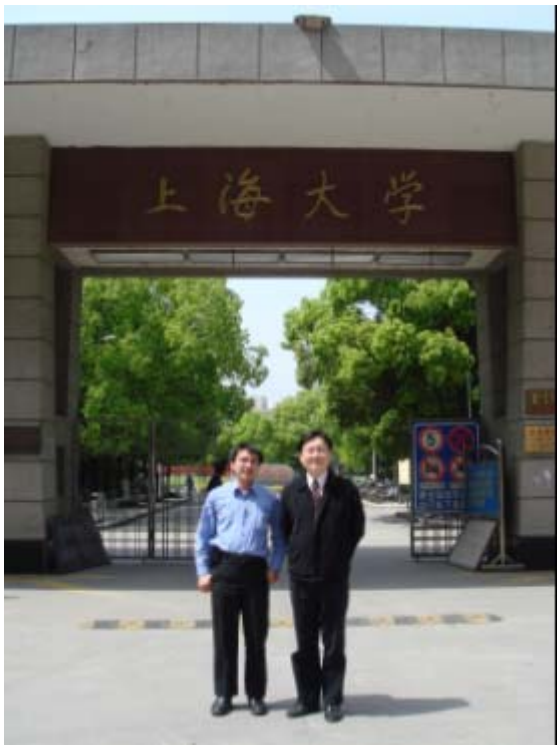
這是高精密度的影像分析設備。



這項技術是多方向顯示浮水印技術，可以運用在防伪或是創意影像之運用。這項運用模式已經運用在許多的路邊廣告上。不過上海理工的技術更為專精，可以表現出更多顏色變化的細緻程度。

中午受邀與對方學院之教授進行餐聚。彼此在餐聚中針對科研計劃之執行方向與方式交換意見，並了解上海理工之實際學生求學環境，以利後續人員交換合作之規劃。

4/23 前往上海大學與上海市經濟管理幹部學院進行訪問
延續前一天之學術拜會行程，23 號接著拜訪上海大學。

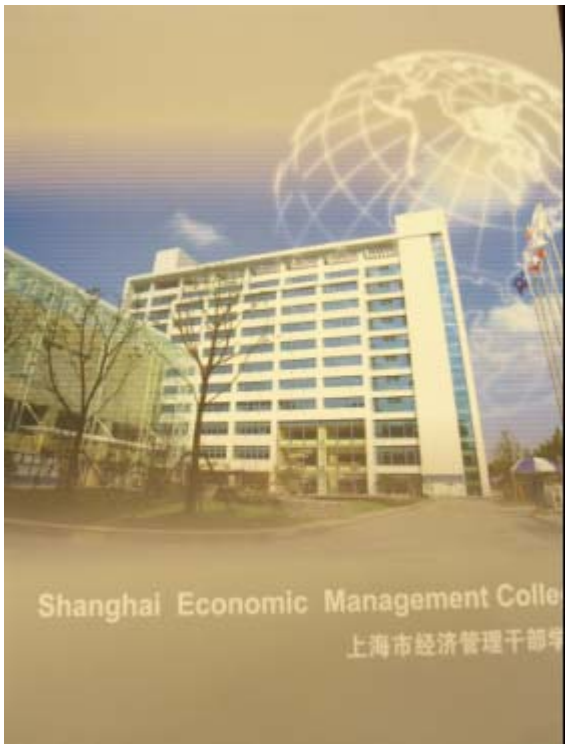


宜蘭代表團成員於上海大學前留影。

於上海大學校訓前留影紀念。

接著趙教授參訪微電子研究中心留影。目前計畫在經過後端數位處理後，最重要的是前端該如何與使用者互動。達成互動必須要仰賴自動化控制或是低成本之微機電處理技術，透過自動化之技術可以達成虛擬與實際世界之整合。過去這段是團隊比較弱的部份，所以在本次參訪的行程中特別注意結合不同領域之技術成果，思考整合運用之方向。

下午接著參訪上海市經濟管理幹部學院，針對數位內容產業之經營與推廣進行討論。在討論中，希望找出大陸產業的另外一個發展方向，避免淪為單純的代工製造國家。



上圖是上海市經濟管理幹部學院的簡介手冊。此學校每年培育出三萬多名受訓學員，廣佈大陸各主要企業之領導階層。如果能夠從此開始推廣數位創意文化產業，將能夠在推廣的工作上收到事半功倍之效果。

宜蘭大學的代表與經濟幹部學院的代表們針對如何合作推廣數位文化產業的概念彼此交換意見。在會議中，彼此都認為單純的製造並沒有辦法達成下一個經濟的起飛，必須要發展創意與創新運用產業。

會後趙院長與對方代表交換彼此之介紹文宣，並合影留念。

上海經濟幹部學院的上課場地硬體設施相當的完善，未來如果有需要在中國大陸進行數位產業之推廣，可以借用相關場地並透過學院之關係聯繫相關人員參與研討會。

4/24 前往　上海工人文化藝術宮參訪

4/24 早上利用前往北京前的一點時間，參訪上海工人文化藝術宮。

上海市工人文化宮藝術中心，角色主要是內容的提供商。擁有獨立的數位攝影棚與相關的節目製作設備，也進行電影的拍攝。本次拜會主要希望得到關於理想中的數位內容推廣平台的意見。期待在本計劃中，能夠針對數位產業需要之發展平台進行發展。

趙教授與上海市工人文化工的副主任和影留念


代表團一行人參觀正在製作中的電視撥出內容。

正在剪接之節目剪接室。


談話性節目之室內攝影棚。

在訪談的過程中，我們了解到目前有許多的內容提供商都希望由過去被動的授權電視媒體播放，改為能夠在網路上進行獨立播放的動作。而 DRM等問題就是需要被考量的，因為某些特殊考量尤其希望採用自有的技術而不採用美國公司的商業化解決方案。另外一個原因則是著名的 DRM 保護機制由於過於著名，所以已經成為駭客破解的目標。

4/25 於北京交通大學演講

4/25 經過昨天一個下午的準備，針對北京交通大學電子訊息學院的師生發表學術演說，內容著重在 Corss-Layer 的設計上。

在演講之前，首先獲頒北京交通大學兼任教授之榮譽聘書。並與副校長及合作的訊息學院院長與書記同時合影留念。透過實質上的師生互換，老師擔任兼任師資等動作，希望能夠加速兩校間的交流。

趙教授針對 CrossLayer Design 提出學術報告。

北京交通大學訊息學院對於本合作演說相當重視，所有學院之博士生均參加本次演講。演講後，學生提出很多問題與思考的方向。由於趙教授的實做經驗豐富，所以也針對相當多的實做問題提出解釋。舉例來說其中一個運用是無線定位技術，學生就提出為何不簡單使用三角測量來解決問題。而趙教授回應，基本上的大方向沒有錯，但是針對訊號之衰減考量並不是理想。所以考量到實際的狀況，還是有必要建立相對應之場強分佈圖。

會後首先拜會了李副院長，針對後續的實質合作進行協商。基本上確定了將來會以研究生為主進行實質交換。而今年度開始兩邊的研究生，將有少數挑選過領域相近的學生開始進行共同指導。

下午同時拜訪了北京交通大學的校長，針對未來的合作提出想法。北京交通大學的校長也希望能夠把合作的層級提升到校對校。校長熱心的說明大陸重點的科研計畫之方向，並提出未來合作之可能與形式。北交大的校長充滿了學者風範，令人留下深刻的印象。

在拜會的過程中，北京交大的校長特別請校書記取得北京交通大學之校徽章，親自爲趙涵捷教授別上。希望趙教授未來能夠排定時間，撥出更多時間在北交大授課，並合作科研項目。

趙涵捷教授致贈國立宜蘭大學與本計劃之文宣資料予北交大的校長。

趙涵捷教授與北交大的校長與院長等重要領導幹部合影留念。


明湖


科學會

趙教授與陳偉銘教授在對方院秘書陪同下參觀校內之基礎建設設施，並了解上次碩士班學生訪問北京交通大學之狀況。希望下次學生交流的時候，能夠有機會有更深更緊密之研究機會。

晚上，北京交通大學的電子訊息學院張宏科設宴招待宜蘭大學代表團。在餐聚中了解北京交通大學即將於六月訪問台灣，到時候會針對今年新收的碩士班學生進行挑選，選出適合進行兩校交流互換之學生。並預計進行一個月以上之學生交換工作。

4/26-27 於煙台大學發表演講

4/26 一早代表團飛抵煙台國際機場。煙台市給人的映像就是非常的乾淨與高度規劃設計之城市。而煙台大學就是山東區域的重點大學。

中午與煙台大學的書記與學校學院重要幹部合影。

煙台大學校長頒發煙台大學聘書給趙涵捷教授。

趙涵捷教授針對數位創意生活發表專題演說。

當天現場聚集了相當多的學生。

同學們在會後針對感興趣的問題提出發問，包含了實用層面的考量與技術層面的問題。會場大家的共識是，其實技術上往往都已經有了相關的解決方案，重點是如何透過整合結合不同的技術來達成作品概念的表現。由於作品本身如果需要展示並商品化，技術的整合度就需要達到完善。同時考量到將來的銷售問題，所以某些技術需要自己發展或是客製化。

4/28　返回台灣

四、建議

目前大陸的學術發展類似過去的台灣，還著重在製造業上。台灣該如何利用成熟的技術與創意，脫離與大陸之間的成本競爭，相信是台灣未來需要認真思考的。

五、攜回資料名稱及內容

本人此次與會，帶回以下資料可供洽詢

１．北京交通大學與電子訊息學院的簡介資料
２．上海大學的簡介資料
３．上海理工學院的簡介資料
４．上海經濟幹部培訓學院簡介
５．煙台大學簡介

六、其他