行政院及所屬各機關出國報告提要

出國報告名稱：赴美進修電信網路碩士學位

頁數33含附件：□是■否

出國計畫主辦機關/聯絡人/電話：台灣電力公司/陳德隆/(02)23667685

出國人員姓名/服務機關/單位/職稱/電話：

林孟穎/台灣電力公司/彰化區營業處/八等電機工程師/(04)7256461

出國類別：□1 考察■2 進修□3 研究□4 實習□5 其他

出國期間：96.9.3～98.7.2　　出國地區：美國

報告日期：98.9.2

分類號/目：

關鍵詞：移動式隨意網路(MANET)

內容摘要：

壹、計畫緣由及目的。

貳、出國行程概述。

參、進修學校及課程簡介。

肆、海外就學心得及生活經驗談

伍、研究主題: 移動式隨意網路路由安全。

近年來網路環境使用趨勢，從傳統的有線網路過渡到更便利的無線電信通訊，這使得我們擺脫有形線路連結的限制，進一步朝向行動上網的理想。為滿足人們在任何時間、地點通訊的需求，移動式隨意網路 MANET (Mobile Ad Hoc Network) 已應勢而生。 然而，無線網路的特性在安全性上有較有線網路有著更審慎的顧慮，在安全技術上更有值得探討的地方。而移動式隨意網路(Mobile Ad Hoc Network)，由於其獨特的移動式路由屬性與主機電力休眠的需求，面臨

的設計挑戰之一，便是網路的易受攻擊和路由的困難性。本文介紹移動式隨意網路所面臨的挑戰和機遇所構成的這種新網路環境，探索增進其通信安全的辦法，同時檢視並研究在路由方面哪些機制是有助於增進移動式隨意網路安全。

陸、建議事項

柒、感謝

本文電子檔已傳至出國報告資訊網(http://open.nat.gov.tw/reportwork)

出國報告（出國類別：進修）

赴美進修電信網路碩士學位

服務機關：台灣電力公司

姓名職稱：林孟穎　八等電機工程師

派赴國家：美國

出國期間：96.9.3～98.7.2

報告日期：98.9.2

目　錄　　頁次

壹、 計畫緣由及目的

隨著網際網路的快速發展，上網人口的急速增加，網際網路衝擊了人類生活的各個層面，電信通訊如今與每個人生活息息相關，網路商業行為已成為風潮。 各行各業面對這一波網際網路的世紀風潮，莫不卯足全力，加速企業網路化的腳步，積極因應此一發展趨勢以結合新知，掌握契機，善用網際網路所帶來的便利來滿足企業員工與社會大眾更即時多元與便利的服務，並因應時代的快速變化。 而相對的，各式各樣的通訊技術也正在蓬勃發展，現代的商業戰爭已是個資訊數位戰場；台電近年來亦應用各式各樣的通訊技術，積極善用網際網路的及時與多元的服務功能與社群學習功能，以提高公司員工的專業水準與工作效能，並針對眾多系統進行通訊網路及資通安全上的改善，以達成企業電子化、網路化的流程改造。

資訊系統網路化已是個正在進行的趨勢，網路不僅能夠提升公司員工的專業智能，也能夠在處理用戶問題時，結合更多的社會資源與群眾知識。 因此，善用各式通訊技術，學習網際網路的知識與技術，建構網路資源資料庫，並重視通訊安全，可在企業內部資源管理達成最適化，幫助公司內部各部門資訊緊密結合並提供用戶快速服務。

近年來網路環境使用趨勢，從傳統的有線網路過渡到更便利的無線電信通訊，這使得我們擺脫有形線路連結的限制，進一步朝向行動上網的理想。 在消費者的需求以及網路業者的推波助瀾下，政府亦大力推展行動台灣政策，許多家庭、辦公室及會議室紛紛採取無線通訊作為另一種連結網際網路的解決方案 。然而，無線網路的特性在安全性上有較有線網路上更謹慎的顧慮，因為不受有

線連結限制而經由開放電波更易侵入企業網路窺探及存取資訊，使用者資訊亦更容易遭受竊取的特性，在安全技術上更有值得探討的地方。

為因應本公司未來業務需要，公司舉辦菁英留學計畫，針對不同項目人才要求不同的進修主題，選派人員出國進修。在參加公司「96 年菁英留學計畫」出國進修博碩士人員甄選中，在單位主管及公司同仁的大力支持下，本人有幸入選 96 年度台電 10 位出國人員名單，進修主題是電信，並申請至加州州立大學東灣分校(California State University, East Bay)進修電信網路(Telecommunication Systems)碩士學位。

貳、出國行程概述

時間	地點	工作概要
96 年 9 月 3 日	台北 ⟶ 舊金山	去程
96 年 9 月 3 日 → 98 年 6 月 30 日	加州州立大學東灣分校	攻讀電信網路碩士學位
98 年 7 月 1 日 → 98 年 7 月 2 日	舊金山 ⟶ 台北	回程

出國期間：96 年 9 月 3 日～98 年 7 月 2 日共 22 個月整

叁、進修學校、環境及課程介紹

進修學校與進修環境介紹

加州州立大學東灣分校 (California State University East Bay) 成立於1957年，是加州州立大學23所分校之一，早先校名為Hayward分校，近年改名為東灣 (East Bay) 分校。校園佔地340多英畝，分為Hayward及Concord二座校園，主要校園為Hayward校區，緊鄰舊金山海灣。加州州立大學東灣分校的地理位置距舊金山及聖荷西都會區均約1小時車程，地理位置位於加州灣區 (Bay Area) 的東灣，是加州州立大學23個校區中少數位於矽谷區的校區，以電腦，理工及商學為最強。加州州立大學東灣分校分為數個學院：科學院、教育學院、社會科學院、商學院、藝術學院、人文學院、理工學院、純藝術學院等。最熱門的是商學系及資訊科系，為不同背景的學生提供各式課程，學校重視實務應用，均採小班制教學，上課人數通常由10多位至30多位學生，老師同學間互動密切，教授亦多數具有矽谷實務工作經驗。CSUEB課程眾多，提供49門主修、64門副修學士學位及33門專業領域的碩、博士課程，課程理論與實務並重。

加州州立大學東灣分校地理位置

加州州立大學東灣分校學生人數超過1萬4千人，國際學生來自超過80個國家，學制為Quarter制度，為學生提供豐富課程選擇，並採取小班制教學，正式課程平均每班26人的安排，讓學生有更多機會與師長互動，學生與教職員人數比約17：1，各式各樣包含體育隊伍，學生報紙、廣播、和電視臺、音樂、舞蹈、宗教等學生社團及組織超過90個，學生生活多彩多姿。 學校內設備齊全，有餐廳、學生宿舍及超過2萬平方呎的室內運動中心、2個奧運標準游泳池、藝術表演及演 講廳、大型圖書館、體育館、網球場、壘球場及棒球場等。

加州州立大學東灣分校校園一隅

加州州立大學東灣分校座落於矽谷(Silicon Valley)區，是全美的科技中心所在。 其提供的各種大學部和研究所的課程也吸引了眾多各國的矽谷專業人士來此學習，而矽谷當地的公司大量雇用從當地畢業的學生亦拉高此區各學校於全美排名名次，在校時，學校同學亦有許多來自矽谷公司內部的在職進修。 矽谷右邊靠近沙漠，擁有全年溫暖的氣候，全年約有 11 個月都是陽光普照的天氣。舊金山和聖荷西兩大城都距離 CSUEB 校園只有一小時的車程。夏天時，學校有舉辦許多健行、露營活動，在冬天的時侯，滑雪及其他高山活動亦都非常盛行。

矽谷因為區內有許多良好的大學，尤其是世界知名的柏克萊及史丹福大學均位於此區內，在優秀的人才主導下，上千所高科技公司的總部都設在矽谷；在世界上所有獨立的經濟體中，矽谷的產值排行高居不下，台灣新竹科學園區下單的廠商有許多來自這裡，並與此地企業有密切的合作，每年亦有無數的創投公司成立於矽谷；在矽谷的知名公司有諸如 Google、 Yahoo 雅虎、 Oracle 資料庫、Sun 昇陽、Apple 蘋果、 eBay 拍賣網站、HP 惠普、Cisco 思科、McAfee 防毒軟體、SanDisk 記憶體、National Semiconductor 國家半導體等知名科技公司總部均坐落於此。 因此在當地學術氣氛助長之下，當地居民相較於全美教育程度極高，有碩、博士教育背景的比比皆是，外國移民亦佔極大比例。在這樣的科技氛圍下學習，求學的過程中，感覺到學習到的不只是最新、 最進步的科技技術，並感受到來自許多不同國家、不同領域及不同文化的人文陶冶。

進修科目介紹

學校相當重視學生基礎理論的扎實程度，此次進修科目所修習學科包含以下科目並介紹如下：

修習科目	修習內容綱要
寬頻網路通訊 (Broadband Networks and Communication)	進修電話系統及區域網路、廣域網路應用技術整合介紹，包含 ADSL、Cable、FDDI、Ethernet、ATM、Satellite 等原理。
通訊網路分析及設計（Communication Network Analysis & Design）	學習在設計一個網路系統時需要考慮的重點諸如成本、拓樸架構、延遲率、頻寬、及可升級性、骨幹網路架設地點等因素一一做出分析。
無線及行動式通訊網路架構(Wireless & Mobile Network Architecture)	學習各代無線通訊網路差異，各無線網路 Protocol 及優缺點，撰寫 Socket 程式及無線控制模擬系統以了解各代無線通訊系統。
分散式系統 (Distributed Systems)	學習針對分散式網路系統所使用的不同程式設計方法與網路系統架構，學習諸如 RPC，CORBA， RMI，RMI-IIOP 等程式與網路平台的使用。
物件導向程式設計 (Object Oriented Programming & Design)	學習 JAVA 程式的寫作，為網路分散式系統的設計打好基礎。
進階軟體工程 (Advanced Software Engineering)	JAVA 及 TCL 程式的寫作，學習及應用各式 Java Pattern，及練習 TCL 程式及 Java 混合應用寫作技巧。

資料庫管理 (Database Systems Administration)	針對資料庫交易可復原性、一致性、獨立性等理論做進一步進修。學習做為資料庫系統管理者所需要的技巧，包含架設、開啟及管理，備分 ORACLE 資料庫系統的能力。
作業系統設計 (Operating Systems Design)	以 linux 作業系統為例，深入學習可下載核心模組、記憶體管理、系統呼叫等作業系統設計原理。
英語寫作(English Advanced Writing) 及科學寫作 (Science English)	學習論文寫作之標準格式，英文修辭學以及辯論式作文和回應式作文寫法。
專題研究 (Project) --行動式隨意網路 (MANET)安全分析研究	針對行動式隨意網路所面臨的挑戰和機遇所構成的這種新網路環境做出介紹與認知，並探討增進其通信安全的辦法，同時檢視並說明有哪些機制可有助於增進行動式隨意網路安全。

肆、海外就學心得及生活經驗談

海外留學應該是所有學子共同曾經的夢想，大家都夢想著能嘗試出國所能享受到的完整海外生活經驗，過獨立生活，擴展視野，並接觸不同人文風情的美好。 曾經以為以自己十多國的自助旅行經驗，一向與外國友人交往無礙的活潑個性，到了國外生活必定如魚得水，沒想到長期住下來，從物價到租屋、車子過戶等法律層級的問題，一切都不是從前短期旅遊所曾遇到的麻煩接踵而來，這時候才開始真的感受到何謂訓練自立能力，並了解何謂人的潛力無窮；心情亦從一開始的孤立無援到結識各國好友進而感受到異國生活的美好之處。

因為喜歡到世界各國四處看看，瞭解世界不同的文化的個性，從以前就覺得自己比相對年齡的人獨立，可是到美國生活後一切重新適應，然而，初到美國的前三個月我還是有了嚴重適應不良的感覺。 首先，加州矽谷高昂的物價大約台灣中部生活的 2.5~3 倍，住房更達到 6~7 倍的租屋價格，不論去哪裡都要長距離的開車，人際關係亦不像台灣雞犬相聞的熱鬧，我與朋友相約，總需一個星期前就開始約下個禮拜的活動；從開車習慣到許多生活的小細節均截然不同，在經過三個月的文化驚嚇(Culture Shock)洗禮後，我下定決心徹底拋棄自己在台灣的生活習慣，重新適應美國的生活文化，真正心靈沉澱下來後，才開始感受到美國簡單生活的樂趣。 在美國的生活，受到諸多朋友的照顧，也真的重新認識什麼叫獨立的生活與「在家靠父母，出外靠朋友」的真諦。在此寫出自己對美國印象較深的地方，希望以此篇文章，對曾經幫過我的人及海外共處的友人，表達深深的感謝之意，並期許也許能幫助到將來有意要前往美國進修的後進。

在此寫出對美國印象深刻的幾點感想：

一、 開車：大家都說在美國沒車，就像是沒有腳一樣，這件事除非你住在舊金山或紐約這類型的大都市市中心，基本上這句話都是成立的。 可是長住美國要開車卻是要重新學習當地的開車習慣，並了解他們對法律的規定說一不二，我剛到達美國時，因一晚較晚回家而無社區停車位，將車子放在所住社區保留給來賓的位置，想說隔天一早上課就遷走，在台灣覺得這是一種彈性可行的辦法。結果半夜四點多車子就被守衛叫拖吊公司拖走，當天從拖吊場領車就花費300 美金才將車子領出，真的是給我上了一門震撼教育課。亦因為車子是從別州買來並於排到駕照路考的日期較晚，開車的第一個月就被警察攔下因為車子上驗排氣的牌照過期並因而被查出還未更換加州車牌，罰金為近 1400 美金，當場快要昏倒。 在不了解美國交通法規的條件下，丈二金剛也無法當場跟開罰單的警察申訴。 幸好在我跑了監理所，警察局，並至簡易交通法庭向法官申訴我初來乍到，完全不了解這些規定後，罰金調降為 289 美金。之後我在有關法律規定上頭非常小心翼翼，不論從汽車保險到租屋條款我均仔細閱讀 。 亦慶幸自己在出國求學之前語言已有了一定的基礎，不然在陌生環境下，如果語言不通對國外規定亦不了解的情況下，萬一遇到事故面對這種違規重罰的國家還真得只能有苦說不出。

在人生地不熟的環境下，我們對他國的法律更為陌生，並一不小心可能就帶著原本的生活習慣過去，可是每一個國家都有著自己對法律的理解與認定，我只能奉勸要出國進修的人要多了解當地的法律規定並切實遵守，並於出國前先將語言打好基礎。

二、 戶外活動：到美國後我最開心的是開始從事各式各樣的戶外活動，並認識一群喜好戶外活動的好友，這對在台灣運動只會跑室內健身的我算是一大

改變，加州的氣候非常適合戶外活動，舉凡健行、攀岩、滑雪、泛舟、露營等都成了我的最愛，閒暇時亦喜歡在住家附近的公園跑步，也開心與朋友因這些活動而更熟絡。 在美國，室內活動並不是像台灣的方便，大家周末相約並不是像台灣般約去喝茶、 看電影，有許多的比例是約了進行各式戶外活動，因為天氣溫暖，加州人對運動健康極為重視，他們覺得這樣才是真正的享受生活。 在這裡亦鼓勵有幸去國外留學的朋友，要積極利用在國外地理環境來享受台灣感受不到的各種活動，並藉而能真正的融入美國的生活。

三、 人種：矽谷是尖端科技集中地，大部分的產業是 IT，但也有一部份的生物研發產業。大家都說在路上撞到人，一問職業 70~80%是工程師，再來就是為公司作帳的會計師，我認識的朋友也多為這 2 種職業。在此地有相當多比例的外籍人士，對於外來人口的包容力極大。 矽谷算是充斥著印度人和華人的地區，我的學校雖然人種分佈平均，但是因為在資訊學院，同學卻有 70%的印度人，以及部份亞洲人及白人。 因為台灣留學人數越來越少，同學裡遇到的亞洲人多為極度認真的中國人，能出國留學的中國人大多已在其求學的過程經歷許多的比較中脫穎而出，有些相當家境富裕並受到相當良好的教育，在這裡深刻感受到對岸同學的拼勁。 不過台灣學生的相對優勢是較為活潑，有些人較會參與各種活動而積極融入當地生活。 至於印度人因為英語是其官方語言之一的優勢，印度人相當敢表達自己的意見，在上課時，他們不見得懂得較多，甚至回答可能是錯的，但總是非常積極回答老師的問題或表達自己的意見，印度腔有些因為口音濃重的關係，有些人發音相當難懂，但是他們積極的個性，一開始上課把我唬得一愣一愣的，以為每個人均是臥虎藏龍。 不過他們勇於表達的個性，還是相當值得我們學習。 我的印度室友就叫我沒事就跟汽車保險公司或銀行免費客服專線打電話詢問各類事宜，除了沒事練英文外，問多了還可能撈到各類

折扣。比如有些汽車保險公司就有好學生折扣、工程師折扣或本國優良駕駛記錄折扣，這些都是保險公司不會主動告知的事項，問到適用的項目在物價高昂的美國還真幫我省了部分支出，我的汽車保險就因此而降了一半保費。

四、男女平等：在美國路上挖馬路、指揮交通的工人有許多是女性，因為人工相當昂貴，不論男女大家都被訓練得是非常獨立的個性。 你說一個女生非常強壯事實上是一種讚美，教授說需要移動課桌椅，女生同學馬上就直接過來幫忙。 我在美國車子爆胎，請人幫助過一次後，也學會挽起袖子來換輪胎，舉凡幫朋友刷油漆、 扛重物幫忙搬家以及拔滿院子的雜草的事情我都做過，在美國並不欣賞女生柔弱的價值，男性雖被教育為需要尊重女性及保護女性，但是並不會因此輕忽女性的力量。 在這裡重視的是你個性是否成熟獨立並且為能獨立判斷的個體，而不是你的性別為何。

五、 矽谷的企業福利：因為矽谷華人聚集，很開心地陸續聯絡到好幾個多年未聯絡的大學同學，高中同學，甚至國中同學都聯絡到幾個，在這些已多年定居在當地的同學、以及進而認識的學長姐的帶領下，也去了許多人的公司參觀。印象深刻的是在矽谷的企業固定供給員工各式免費飲料、 食物，提供員工通勤補助、運動補助等福利措施。Google 甚至提供洗衣、洗車、帶小孩服務，就是為了讓員工不需煩惱生活瑣事，而希望員工能將所有心思與時間均貢獻於公司事務上。 大部分公司員工亦可選擇每星期一天在家工作，企業對員工相當的禮遇與照顧，並極端尊重每一個員工的需求。 不過相對的是公司對於績效相當重視，員工績效不好隨時有被裁員走人的可能性，公司員工對公司忠誠度亦低，若有其他公司用更好的福利、薪水挖角，員工隨時可能跳槽。

在這裡企業常會舉辦各種公益活動，如員工賽跑募款、 騎腳踏車募款，幫助遊民活動，讓員工的身心健康與公益活動緊密結合。 企業亦會建置類似小巨蛋的場地，與外界藝文活動結合，如 Oracle 的體育館經常舉辦各類運動賽事，HP 的體育場常辦演唱會等藝文活動，而這些場所亦都成為當地的地標，因而大幅的加強該公司的企業形象並與當地社區緊密結合。

六、簡單生活的樂趣 ： 剛到美國時，我總愛問這邊的移民美國到底是哪一點好，常常得到回答是簡單。 一開始我不是相當能理解，對於從歐洲或亞洲過去的人，總覺得生活相當的不便利。人工昂貴，所以大家什麼都自己動手做，像是園藝，家庭修繕，以及小至修表、 大至簡單的修車都是動手 DIY，我從不諳廚藝到可做蛋糕、麵包及一些簡單的台灣小吃。開車至各處亦總花費許多時間。一開始我總覺得美國生活超級不方便，但在適應美國的生活後，我開始體會到什麼叫簡單 ：沒有雞犬相聞的吵鬧，也少了人際間的人情應酬， 大家都給予對於個人的空間相當的自由與尊重，雖然一切不如台灣的便利，卻反而你只需要做自己想做的事，在社會規範下的行為，絕對不會有人來干涉你該怎麼做，或需要配合社會期望該怎麼做。 生活化到即簡後，人不會有那麼多的慾望和彼此間的比較後，反而可以感受到簡單的幸福，這點會是我想念美國的地方。

七、絕對的服務品質 ：在美國，有部分走高價商品策略的商店諸如 Nordstrom 百貨及 REI 運動商品專賣店提供給消費者百分之百的商品絕對滿意保證服務，只要你保留商品購買收據，它提供終生換貨、退貨或商品終生保固之保證。曾看過有人運動鞋穿破一個洞一年後去 REI 換貨，有人太陽眼鏡 3 年後因折損維修而 Nordstorm 因無法維修，全額退回原購買價給消費者的事。原本就聽說美國極度保護消費者而懷疑這些商家是如何能賺取利潤並生存下來，但是因為

這種品質保證的態度，反而讓這些企業在消費者心中建立絕對至高無上的品牌形象。 即使售價相對高昂，消費者仍因這樣的安心機制而願意購買這家企業的產品。真的期許有一日，台電也能在每一個流程做到盡善盡美，也可以在用戶心中建立這樣高標準的金字招牌。

伍、研究主題

在美國進修途中，主要是針對無線網路通訊進行研究。 以下是針對無線網路中行動式隨意網路安全機制 (Securing Routing in MANET) 之研究專題進行介紹與報告：

一、前言

近年來網路環境使用趨勢，從傳統的有線網路過渡到更便利的無線電信通訊，這使得我們擺脫有形線路連結的限制，進一步朝向行動上網的理想。 但是網際網路並非隨時可用，因此無法滿足人們在任何時間、 地點通訊的需求，因此行動式隨意網路 MANET (Mobile Ad Hoc Network)已漸漸受到全世界的重視並在應用與技術上不停的進行改良。 然而，無線網路的特性在安全性上有較有線網路有著更審慎的顧慮，因為不受有線連結限制而經由開放電波更易侵入企業網路窺探及存取資訊，使用者資訊亦更容易遭受竊取的特性，在安全技術上更有值得探討的地方。 而行動式隨意網路(Mobile Ad Hoc Network)，因為不須經由任何存取點或基地台等基礎設施的便利性，現在已有更多的採取臨時網路用於商業用途的趨勢，由於其獨特的行動式路由屬性，其一個主要的設計挑戰，便是網路的易受安全攻擊。 本文將會針對行動式隨意網路所面臨的挑戰和機遇所構成的這種新網路環境做出介紹，並探討增進其通信安全的辦法，同時檢視並說明有哪些機制是有助於增進行動式隨意網路安全。

二、行動式隨意網路(Mobile Ａd Hoc Network)介紹：

無線網路種類

無線網路可分為兩種類型：有基礎建設(Infrastructure)和無需基礎建設(Non-Infrastructure)2 種；前者是利用基地台 (Base Station) 或存取點 (Assess Point)的方式來收發訊號，目前無線網路架設多屬於此種網路(如 Fig1)。以有基礎建設來說，這種通訊方式雖訊號較為穩定亦較為簡單控制，但若是遇到某些外在因素破壞（如戰爭或天災等），將導致所有的行動式主機無法進行網路傳輸。 而行動式隨意網路(Mobile Ad Hoc Network；MANET)因不需基礎建設架構，它的建置可以不受時間、地點或環境的限制。

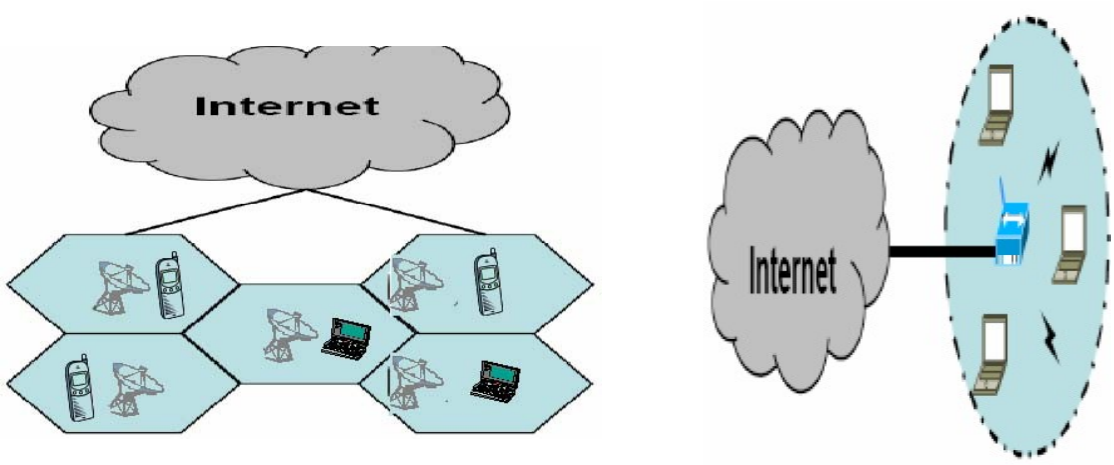


Fig1:左圖為經由基地台蜂巢網路連結之無線網路；右圖為經由無線存取點連結之無線網路，二者均需倚賴基礎設施連線。

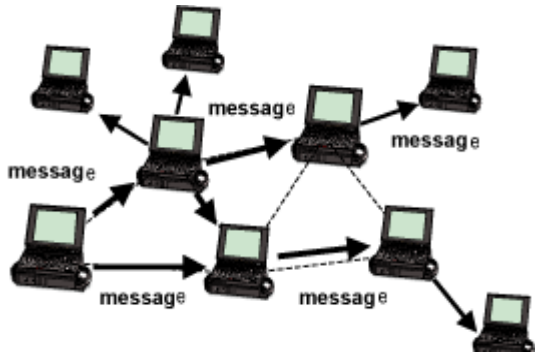


Fig2：MANET 由無線通信的行動式主機在點對點狀態下組成的通訊網路

隨意網路(MANET)是一種經由無線通信的行動式主機（Mobile Host，我們亦稱之為節點）所架設的網路。 在沒有固定的基礎設施（Infrastructure），如基礎台（Base Station）和移動交換中心的情況下，符合ＩＥＥＥ 802.11 規格的無線節點在彼此的無線電波範圍內通過無線電波連接。因為 Ad-Hoc 網路行動式主機皆處在平等地位下，其路由具備自我組織的能力，網路的建置簡化並具有高度動態的彈性；並且，它能在針對如節點隨時位置的移動，和不可預估的網路流量負載下，作最適的資源利用。由於它網路容易建置的特性，Ad-Hoc 網路有許多實際的用途，如一般家庭或辦公室區域網路、軍事用途或緊急救災甚而臨時商業網路的建置等等。

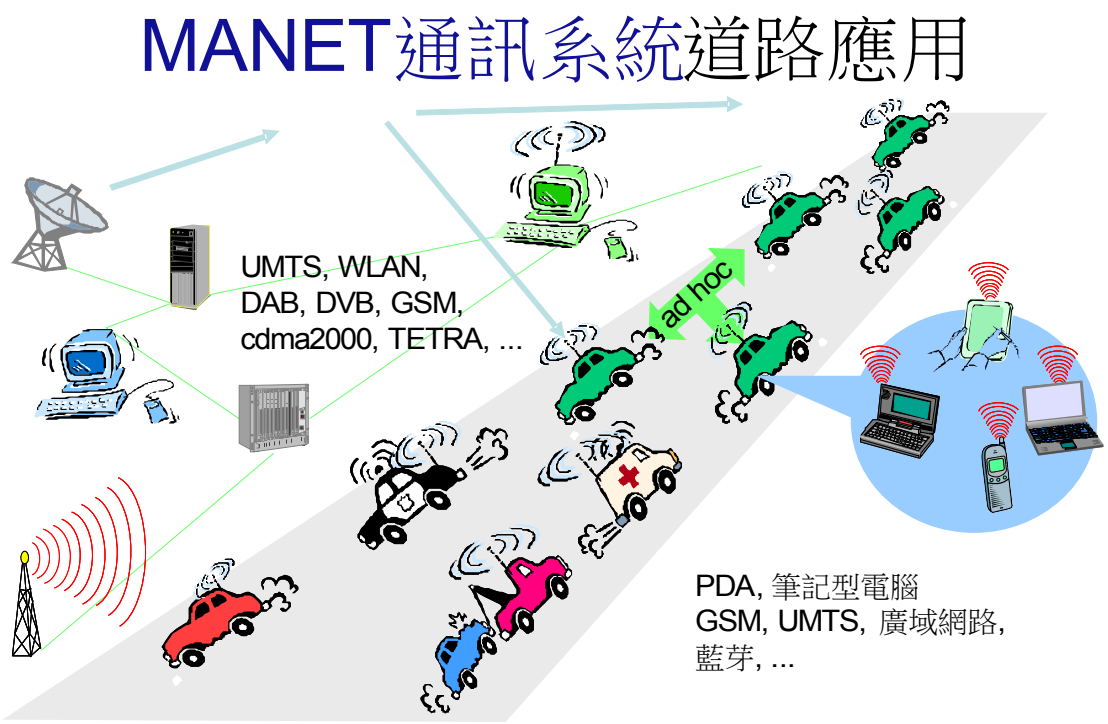


Fig3 ：架設 Ad Hoc 網路之道路系統：隨時移動的車子上裝上符合 802.11 規格的無線發射器，每台車均可成為其他節點的路由，網路可不需任何基礎設施，具備高度彈性，但因其移動性，此等網路亦提升其路由的困難性及資通安全上的脆弱性（vulnerability）。

Mobile Ad - Hoc 網路是通過網路內每個節點(Mobile Host)與其鄰居節點(Neighbor Host)的協力合作轉發網路封包，這通常牽涉到資源共享，通訊聯繫和應用系統的緊密聯結。 例如，在行動式 Ad - Hoc 網路經由每一個節點的訊息交換以及與鄰居建立連接，將網路封包（packet）轉發給它的鄰居以對傳輸目的地建立路由拓樸架構（topology）。 由此產生的路由基礎（infrastructure）是高度動態 (highly-dynamic) 的，不僅是因為每一個節點（Mobile Host）的移動性，也因為其缺乏保障的網路連接性。 例如，網路訊號因受到地形地物的干擾散射以及每一節點的通訊能力不同均會有影響。

常見的無線網路攻擊：

相對於傳統有線網路，攻擊者要竊取傳輸資料，必需要連接上實體線路或設備才能監聽傳輸內容，無線網路只要經由開放的空中電波，不需經由實體線路連結存取，輕易地就可以竊取傳輸資料，造成了更多網路安全威脅。無線網路容易受到的攻擊有諸如：

- **網路竊聽(Eavesdropping)**：指駭客對於無線網路通訊內容進行監控，利用竊聽來獲取網路上的傳輸資料)。
- **訊息重播 (Message Replay)**：是指駭客將從無線網路上截取的某些通訊內容重新發送以欺騙網路的認證系統。。
- **訊息竄改 (Message Modification)**：訊息竄改指攻擊者針對無線網路通訊刪除訊息，注入錯誤的訊息，或修改訊息等等。
- **服務阻斷攻擊 (Denial of Service)**：攻擊者透過各種可能的方法 (Ping of Death、 SYN flooding 等等方式)，對於遠端主機服務，傳送大量的網路封包，造成目標主機資源或頻寬耗盡或服務當機的狀況。 不過由於無線網路使用者的網路頻寬通常遠低於後端伺服器網路設備的特性，遇到服務阻斷攻擊時，正在使用無線網路的使用者一般不會發覺。 不過有另外一種服務阻斷攻擊是利用 IP 協定的漏洞，駭客可以故意回應惡意破壞過的網路封包，給發出 DHCP Request 的主機，若破壞成功，可以讓遭受侵入系統無法回應網路封包要求。
- **中間人攻擊 (Man-in-the-middle Attack)**：是指駭客藉由扮演中間人的角色，讓兩端的通訊都經由中間人傳遞，並在通訊兩端不知情的情況下讀取、插入、 或更改傳輸的資料。

MANET 網路目前常見的用途

- **一般區域網路：**例如在家中或一般辦公場所等，經由符合IEEE802.11規格的行動設備建立路由網路來達到網路傳輸的目的。例如：PDA、手機、筆記型電腦等等行動式網路設備，可經由安裝藍芽介面的方式，將這些Base Station結合成隨意網路。尤其如歷史古蹟不適合佈置有線網路時，Mobile Ad Hoc Network更有其相當的便利性。
- **軍事用途或災區通訊**：戰場上或受災區，許多的網路基礎建設通常已被破壞而無法建置連線或是某些特殊場地受到地形地物的影響， 導致通訊困難，MANET網路容易建置且不需佈置實體網路的特性，可相當程度的適用於此類通訊需求。
- **臨時用途**：例如會議、展覽場上，行動式網路行動設備可以不經過Base Station（基地台）或Access Point(網路存取節點)直接通訊，可節省建置成本，並具有臨時彈性的優點。

MANET 網路特性：

行動式隨意網路作為一種新的組織網路方式，具有以下特點：

無需任何基礎建設：

行動式隨意網路相對傳統有線而言，最大的區別就是可以不需要基礎網路設施的支持，快速構建起一個移動通信網路。各節點通過分層網路協定和分散式演算法各自連結，節點可以快速、自動地組成一個獨立的網路。 而相對於無線網路，它亦不須要網路存取點或基地台，它的建立不需依賴於任何現有

的網路通信設施，具有相對的獨立性。因此這種網路特性很適合軍事用途或偏遠地區通信等應用。

動態拓撲架構（Dynamic Topology）：

由於主機可以在網路中隨意移動，Mobile Ad Hoc Network 是一個高度動態的網 路。會有多少網路節點於何時加入連結，或帶來多少網路流量均不可預測，因此，網路的拓撲架構並不固定，拓撲架構是隨時處在變化中，主機的移動會導致網路的連結範圍增加或減少。主機因為可能還身兼路由器的功能，因此，且由於變化的方式和時機都具有不可預測性。因此其網路路由的運算效率，對於整個網路的傳輸效率有絕對性的影響。

有限的電力或計算能力：

在 Ad Hoc 網路中，行動式主機通常為ＰＤＡ、手機或筆記型電腦。由於主機可能處在不停的移動狀態下，主機的能源主要由電池提供而無法獲得長期的電力供給，因此 Ad Hoc 網路有能源有限的特點，且由於攜帶式設備通常記憶體相對的小，其計算路由能力亦有不一致的特點。

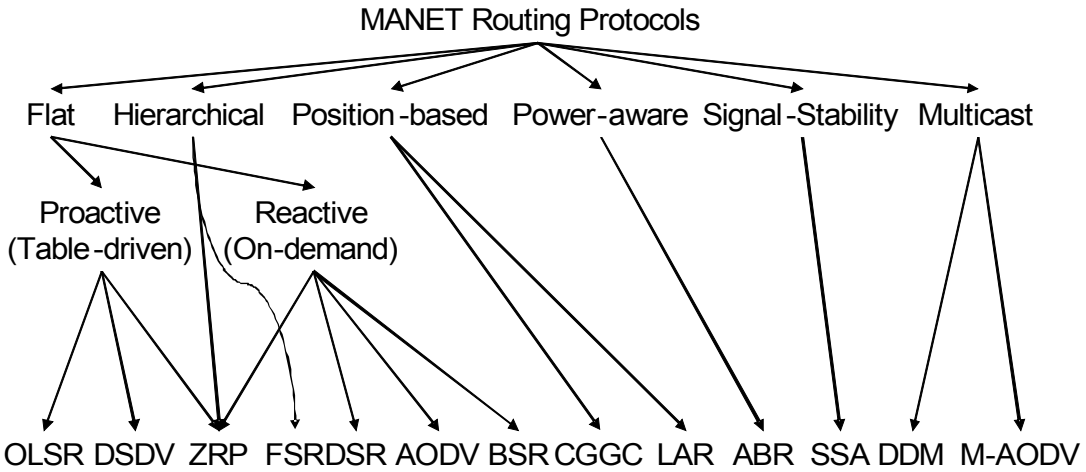
網路連結的強健性(robustness)：

在行動式隨意網路中沒有中心控制節點，主機通過分佈式協定互聯。一旦網路的某個或某些節點發生故障，其餘的節點仍然能夠正常工作。相對於有中心控制節點的網路，中心控制點一旦無法進行傳輸，連結網路即斷線的脆弱性， Ad Hoc 網路具有一定的強健性。因其所有節點的地位平等，形成一個對等式網路(Peer to Peer Network)，節點可隨時加入或離開，任何節點的故障或離開不會造成整個網路的斷線，本身即具有相當的強健性。

三、行動式隨意網路路由安全機制

行動式隨意網路（MANET）的這些特點使得它在安全性上受到較一般無線網路更為特殊的挑戰。因為它具有開放，動態變化分散式的拓撲結構，缺乏集中監控和管理，因而往往缺乏明確防線， 所有這些都挑戰網路安全的新技術，以傳統方式保護網路的防火牆和加密軟體已不再是足夠的和有效的。 路由問題在有限通訊網路上已經有相當多年的研究探討，技術已趨成熟。 近年在無線網路興起後，也有不少路由相關的研討，目前相關的研究都承襲傳統固定網路的路由演算法，尋找最佳的路由演算法以尋出最路徑。 但是無線通訊的環境遠比有線網路複雜且變動程度高，電波易受到地形地物的干擾，通訊信號強度及電力供應是否持續等均會影響路由的選擇，且 MANET 各節點的計算或應變能力暨移動性均差異甚大。我們需要新的架構和機制，以確保 MANET 的安全應用。

行動式隨意網路常見路由協定如以下圖表 :



網路的路由經常受到 2 種威脅，第一個來自外部的攻擊。 駭客可經由加入錯誤的路由資料，重覆或扭曲舊路由資訊，經由重複傳送網路封包或不具效率性的路由路徑來隔離網段或引入過量網路流量而導致效率低下或無法連接到正確目的地的路由。 要抵禦這種威脅，節點可以通過使用加密計劃，如數位簽名以保護傳輸資料同樣的方式保護路由資料。 第二個，也是一種更嚴重的威脅來自被破壞的節點，被破壞的節點可以廣告不正確的路由信息到其他節點。 檢測這種不正確的信息是極其困難的：僅僅要求每個節點經由簽署網路認證金鑰是行不通的，因為被破壞的節點能夠使用私鑰而產生有效簽名。

從路由的觀點來看，在行動式隨意網路，路由資料和和傳輸資料內容，兩者具有不同的性質和不同的安全需求。 傳輸資料內容因為為點對點的傳輸所以可以由任何點對點的安全機制 (如 IPSec）所保護。 然而，路由資料則是發送到鄰近節點處理，並可能將其適當的改動，一個路由節點可能會因此修改其相對應的路由表。因此，路由的中間節點需要能夠驗證傳送來的路由資料的真實性。另一個常見的路由傳輸特性是，在許多情況下，會有一部分的路由資料在傳輸時會有所變動。因此，我們可以區分路由資料中變動的及不變動的資料。要確認可變資料在經過中間節點沒有被竄改將增加計算的複雜性。

在MANET下環境下，封包轉發若根據節點長期固定的位址是不安全的，因為這種定址往往暴露了節點目前的位置，使得當網路拓樸變化時，行動式節點可能被追蹤並記錄下來；所以定期宣布每個節點的位置，從而使它可能使用位址作為一個可靠的當前的目的地地址是較為可行的辦法。 如果在連續定期的更新中間，MANET網路上足夠比率的節點之間的連續變化的位置更新將使得跟踪節點變得不可行。 不過此種定期的公布更新位址的方法將還有效率性的問題要

考慮。利用位置資料來計算路由路徑是實現大規模移動Ad Hoc網路的常見手段。但是，由於節點移動造成的網路拓撲架構的隨時改變和網路節點為了節省電池而隨時可能進入了休眠狀態，基於節點位置計算路由在此點上還有相當多的研究方法在進行。

現有的行動式隨意網路路由協定主要分為兩類 ：經由路由表驅動型路由(Table-Driven Routing Protocols) 和根據需求隨時產生之路由路徑 (On-Demand Routing Protocols) 。行動式隨意網路路由協定一般希望達成以下要求 ：節點可分散式操作，能有效地避免路由產生迴圈， 支持休眠模式操作，支援單向通訊並具良好的安全性等。因為Ad Hoc 網路主機移動為不可預測性，網路拓樸架構隨時改變的特性，Table-Driven 路由協定必須周期性廣播自己所在位置的訊息，告知網路中的每個節點，以更新路由表，但此一行為將會在隨時移動的網路環境消耗大量網路資源。所以根據需求隨時產生之路由路徑 (On-Demand Routing Protocols)更適合行動式隨意網路環境。

可信度路由協定 TRP (Trusted Routing Protocol) 由AODV(Ad Hoc On-Demand Distance Vector)路由協定衍生而來，其依據可信度模型來決定網路節點傳送來的路由資訊是否可以信賴。 信任機制是一種要求各節點經由主觀經驗和客觀評價機制的方式，信任度量根據主機的行為，如轉發網路封包，選擇適當的路線與否，都是組成的參數指標 ，經由過濾可疑的對象以決定可信任的往來節點，並以此建立可信賴的通訊環境。 在該協定中，節點間的信任關系可用可信度模型來表示，並且可信度評價可以不停的動態更 新，節點還可以彼此之間共同合作，以獲得相對客觀的看法以決定另一個節點路由的可信度。 行動式主機還可以根據它們之間的信任關係決定可否信任此路由行為。 經由各節點投票

決定信任與否，節點可以彈性選擇是否以及如何執行加密操作。 因此，路由計算成本降低。TRP路由協定是一個較為簡易但更為靈活的安全解決方案。 TRP比其他加密和認證設計的協定還設計了可信度評價機制，允許節點可以對其他節點的可信度作相對客觀的評價並加以交換此信賴訊息，進而隔離惡意節點，此法可保護整個系統的安全度與強健性，此法因而非常適合解決MANET環境中因破壞節點所產生的黑洞攻擊。TRP亦因為節點間彼此存在信任關系，各行動式主機之間通信時不需要一直請求認證 (Certificate)，這亦相當程度解決了一般可攜式設備CPU的計算能力有限的問題。

自我學習Ad Hoc路由協定SARP (Self-Learning Ad Hoc Routing Protocol)則是以廣播的方式經由搜尋加入訊息繞路的資訊進行路由搜訊，網路上的節點可以經由監聽方式或者直接接收到路由訊息時，分析此路由資訊並將其中可用的路徑記錄於路由表中。 當其進行路由路徑搜尋時，因為節點本身路由表可能已記載通往目的節點之路由路徑，因而減少路徑搜尋廣播產生之負擔。

攜帶方便的行動式設備面臨有限的可攜式電池容量的考驗。在隨意網路，行動式主機可切換到低功耗睡眠模式，在有需求下才被喚醒，然而節點彼此間並無時鐘同步機制導致複雜的問題。 在現有的標準下，如IEEE 802.11或藍芽機制，都假設網路是完全連接或有時鐘同步機制。行動式隨意網路 (MANET) 的存活性極度取決於其行動式主機電池的電力供給長度。 功率控制可以不僅影響電池的壽命，而且影響此連結網路的交通承載能力。 網路節點的傳輸功率不只決定網路拓撲結構，並對網路流通率 (throughput) 和行動式主機的電力消耗度具有相當影響力。 行動式隨意網路因為接收節點和發送節點間可使用比兩者直接通信小得多的電功率進行通訊傳輸，因此節省了相當的能量消耗。 並且經由中

間節點轉發資料，能夠有效降低對無線傳輸設備的設計難度和成本，同时擴大行動式隨意網路的連結範圍。

四、結論：

現代社會由於都會化程度高，產生對於網路頻寬之大量需求，而無線技術之進步，使得下一世代寬頻網際網路設計與實現產生巨大之改變。 寬頻網際網路將朝向支援從音樂、電影、到遊戲，都能火速下載的多媒體資料類型， 並能提供即時性與高移動性之便利需求發展，因此如今網路需要多樣性之服務品質與通訊安全保證。行動式隨意網路(MANET)有相當的彈性與便利性可以滿足這一波網際網路需求的趨勢，技術亦已日漸成熟，各式增強路由的安全協定有相當多的研究提出。 行動隨意式網路被認為是下一代行動通信技術方案中，末端網路(Last mile)最可行的方案之一。 一旦其在資通安全上通過考驗，行動式隨意網路的便利性和簡易佈置性將是網路發展的新主流，並將行動通訊帶往一個新的境界。

五、參考資料

[1] B. Lu and U. pooch. Cooprative security-enforcement routing in mobile Ad Hoc networks. *the 4th International Workshop on Mobile and Wireless Communications Network*, 2002.

[2]C. Perkins, E. Royer, and S. Das. IP Address Autoconfiguration for Ad Hoc Networks. *Internet Draft：draft-ietfmanetautoconf-01.txt*, 2001.

[3] H. Chan, A. Perrig, and D. Song, "Random Key Predistribution Schemes for Sensor Networks," Proc. of the IEEE Security and Privacy Symposium, Berkeley, CA, May 2003 (available at http://www.ece.cmu.edu/˜adrian).

[4] H. Mehta, "Dynamic Adaptive Routing in Mobile Ad Hoc Networks," M.S. Thesis, University of Maryland, College Park, December 2002.

[5] J. S. Baras and H. Mehta, "A Probabilistic Emergent Routing Algorithm for Mobile Ad Hoc Networks," in Proc. of the Conference on Modeling and Optimization inWireless, Mobile, and Ad Hoc Networks (WiOpt03), Sophia-Antipolis, France, March 2003.

[6] Frank Kagrl. Secure Routing for Vehicle Networks. *SEVECOM Kick-off Workshop* Feb. 2006 (Available at icapeople.epfl.ch/panos/SVCW/presentations/kargl-secroute.ppt).

[7] L. Eschenauer, V.D Gligor, and J.S. Baras, "On Trust Establishment in Mobile Ad-Hoc Networks",Security Protocols, Christianson et al. (eds.), Cambridge, UK, April 2002. To appear in Lecture in Computer Science, Springer-Verlag, 2003. (available at http://www.ee.umd.edu/˜gligor)

[8] Li, Zhi, Yu-Kwong Kwok, A New Multipath Routing Approach to Enhancing TCP Security in Ad Hoc Wireless Networks, ICPP 2005 Workshops, International Conference Workshops, Jun. 14-17, 2005, pp. 372-379.

[9] P. Papadimitratos, "Secure and Fault-Tolerant Communication in Mobile Ad Hoc Networks," *PhD Dissertation*, Cornell University, January 2005

[10] P. Papadimitratos and Z.J. Haas, "Secure Communication in Adverse Mobile Ad Hoc Networks," *Ad Hoc Wireless Networking*, D-Z. Du, Ed., Kluwer Academic Publishers, MA, November 2003

[11] P. Papadimitratos and Z.J. Haas, "Secure Message Transmission in Mobile Ad Hoc Networks," in Proc. of the *ACM WiSe 2003,* San Diego CA, Sept. 2003

[12] P. Papadimitratos and Z.J. Haas, "Secure QoS-aware Route Discovery in Ad Hoc Networks," in Proc. of the *2005 IEEE Sarnoff Symposium*, Princeton, NJ, Apr. 2005

[13] P. Papadimitratos and Z. J. Haas. "Secure On-Demand Distance-Vector Routing in Ad Hoc Networks." In Proc. of the *2005 IEEE Sarnoff Symposium*, Princeton, NJ, Apr. 2005

[14] R.B. Bobba, L. Eschenauer, V.D. Gligor, and W.A. Arbaugh. Bootstrapping Security Associations for Routing in Mobile Ad Hoc Networks. Institute for Systems Research, Technical Report 2002-44, May 2002. (Available at http://bellatrix.isr.umd.edu/TechReports/ISR/2002/TR-2002-44/TR-2002-44.pdf).

[15] Sergio Marti, T. J. Giuli, Kevin Lai, and Mary Baker, Mitigating Routing Misbehavior in Mobile Ad Hoc Networks, International Conference on Mobile Computing and Networking, Proceedings of the 6th annual international Conference on Mobile Computing and Networking, 2000.

[16] S. Yi, P. Naldurg, and R. Kravets. Security-aware Ad Hoc Routing for Wireless Networks. *ACM Int'l Symp. on Mobile Ad Hoc networking and computing*, 2001.

陸、建議事項

由於文化的不同，生活上有不少讓人耳目一新的見聞，臚列如下，或可作為本公司營運的參考。

一、 重視企業形象：在經過羅斯福路及新生南路口台大地下道時，看見台電所認養的地下道變的如此美輪美奐，印象極為深刻，地下道架設台電形象廣告看版，舉辦藝文展覽，對台電印象感覺就從純電力方面改向結合藝術、公益的企業形象靠攏；在去溪頭建行時，每每看見漂亮的台大農場，亦總是會對台大印象更深刻幾分。國外企業視企業形象為公司最大的資產，台電亦可認養某些適合的長期災區小型重建工程，並將當地規劃為台電某個適合的形象展示場所，既可幫助受災民眾亦可強化企業公益形象。

二、多舉辦與公益相結合之員工活動：有健康的員工才有健康的公司，尤其國營事業體系員工年齡明顯偏高，員工身體健康才有專注的體力與心力投注於工作上。雖然公司已提供員工諸多身體健康檢查與提供住院補助等等措施，但預防重於治療，建議公司每年擴大舉辦與員工運動賽事相結合之公益活動，如以為弱勢團體募款為名舉辦大型員工體育活動以強化員工身心靈健康。 在美國時，看到當地企業常會舉辦與公益結合之諸如馬拉松長程腳踏車活動，或短程路跑賽事。 我看到的作法是例如舉辦一個員工分組 50 公里騎腳踏車比賽甚至是高樓大廈接力爬樓梯比賽，員工可自由報名分組參加活動，每一組員工除須接力完成此一運動賽事外，還需要於事前各自訂出此組公益募款的金額，比如是為糖尿病或心臟病協會募款，由員工各自向親朋好友以各類方式勸募，於活動前募集到此筆金額後才可以

有資格參加此項比賽，否則此組就得棄權；勸募活動通常截止於活動一個月至半個月前，再來選手就專注於練習比賽。 這樣子就把一個單純的運動會，辦成兩階段式比賽並提升其趣味性與分組合作性，公司亦可於員工勸募金額外另捐出固定經費，以宣示公司公益活動決心並增大此公益活動宣傳性。員工方面因為運動賽事有競賽性並與公益活動結合而積極參與；而此類有趣的活動更因募款擴及當地民眾並與公益活動相結合亦常招致媒體多方報導，活動當天亦常見媒體轉播車現場報導，可大幅增進企業公益形象，達到為企業廣告效果；而多舉辦此類賽事亦可幫助員工身體健康，員工在感覺做好事之餘亦可因緊密的分組活動而增加對公司向心力。建議公司可每年固定舉辦此類活動，遇有重大災害時更可為災民舉辦募款、甚或捐血活動，吸引到的媒體版面為公司帶來正面的形象比起默默無聞的員工捐款將帶來更多正面效益。

台電每年贊助多項睦鄰活動，抑或於台灣發生重大災害時，舉辦員工募款，但這些活動雖達到實質金錢補助，卻無達到真正為台電加強公益形象之宣傳效益。本公司雖花費大量金錢回饋社會，但對本公司公益形象卻無太大增益，也未使社會大眾理解台電對社會每年有多少付出。若同樣這些活動可以更生動有趣的方式辦理，甚而吸引媒體報導，一樣的金錢補助除了幫助真正需要的人外，還可為公司增進社會溫暖公益形象，並幫助台電建立更活潑的社會印象，可謂一舉數得。

三、 整合各式通訊技術以建立多重通信路由，強化通信可靠度：

針對重要發電廠、或公司重要場所規劃多重路由系統通信以確保公司通訊穩定，在佈線便利的地方可佈設環狀光纖系統，在偏遠地區或佈置實體線路不便的地方除目前架設微波系統外或許可以架設無線網路，行動式隨意

網路具有架設方便、不需基礎建設，可應付臨時性緊急通訊需求的優點，目前已有相當多的研究正發展中，若再配合衛星通訊，等技術再行成熟後在公司偏遠地區可考慮以此作為緊急備用通訊方式。隨著 3G、4G 無線通訊技術的發展，網路高速寬頻化及行動式通信已是未來電信發展的主軸，公司電信通訊發展應邁向無線與有線整合發展以滿足並適應時代的需求。

四、 統一開發公司真正有需求之資訊應用系統：

擔任資訊人員以來，常受到公司各部門要求開發各式資訊應用系統，常遇到變電的要求變電的系統，工程的要求工程的系統。個別資訊系統效益提升固然重要，但資訊共用才最能發揮綜效；本公司是否應建立某個資訊平台，讓各單位員工可以由下而上正式反應所需求的系統；如果真有許多公司各單位要求某一系統，公司則可綜合考慮此一應用系統是否有統一開發的必要性，而不是各單位各自開發其部門所需系統，而浪費有限資訊資源。

柒、感謝

非常感激公司主管及各位同仁的支持讓我有這次出國進修的機會，有機會完整的接觸異國文化洗禮，擴展視野，並接觸不同人文風情的美好。 雖說資訊交流無國界，但是在不同的環境下親自體驗並與來自不同文化背景的想法互相衝擊交流，還是人生擁有的最美好的風景與永難忘懷的經驗。