出國報告(出國類別：國際會議)

2012 年第 4 屆通信、移動與計算國際學術會議發表

服務機關：國立中興大學

姓名職稱：黃宣尹研究生

派赴國家：中國大陸杭州省桂林

出國期間：101/05/21~101/05/23

報告日期：101/08/06

目　次

一、摘要

近年來，P2P（peer-to-peer）系統在研究與實用上都受到莫大的的關注。許多 P2P 系統如 CAN、Pastry、Chord、Tapstry 等雖能支援有效率的查詢，但僅支援完全比對（exact-match）形態的資源尋找方式。因此，許多語意式（semantic-based）的 P2P 系統被提出以突破在查詢方面的限制。在語意式 P2P 系統中，資源由敘述性資料(metadata)所描述，並因爲敘述性資料(metadata)具備的語意，語意式 P2P 系統得以支援更加複雜的語意查詢。在本篇論文中，我們提出了一個混合式架構的語意式 P2P 系統，稱爲 RDF-Chord。在 RDF-Chord 中，我們利用了 RDF 的語意設了一組金鑰（key），根據這些金鑰我們能夠有效的利用 RDF 語意並顯著的降低查詢的空間。從我們的實驗結果中我們可以看出 RDF-Chord 是一個具高度延展性並極有效率的語意式 P2P 系統。

二、本文

(一)目的

雖然本次會議議題範圍極爲廣泛，但其中的 5 大研討會都包含了和資訊安全相關的議題，因此，本著本計畫希望能夠了解資訊安全與個資防護的最新發展的宗旨，本人決定參與此次會議以獲得向來自不同國家的學者學習的機會。

(二)過程

此議會於 5 月 21 日至 23 日於桂林電子科技大學舉行，依各自探討的主題分爲 5 個技術研討會和三個受邀講演：

技術研討會

(1) 無線通信網路研討會(Wireless Communication Networks Symposium)

(2) 衛星與光纖通信網路研討會(Satellite and Optical Communication Networks Symposium)

(3) 移動與遠程通訓研討會(Vehicular Technology and Telematics Symposium)

(4) 計算機網路架構與未來網際網路研討會(Computer Networks and Future Internet Symposium)

(5) 運算研討會(Computing Symposium)

受邀講演

(1) 感知無線電與協作通信網絡(Cognitive Radio and Cooperative Communication Networks)

(2) 智慧電網(Smart Grids)

(3) 超越 4G 通訊標準(Beyond IMT-Advanced)

此次會議一共收到 511 篇投稿論文，並錄取了其中的 194 篇，錄取率約 38%。爲了培養用英文上台報告的經驗、觀摩他國學者如何簡報並學習資訊安全與 P2P 系統相關之知識，本人投稿論文於運算研討會並全程參與聆聽所有演講者的報告

內容。

會議議程如附錄(1)所示，筆者在 21 日至 23 日期間參與會議。筆者受邀擔任第二場運算研討會(CS2)之主持人，主持該時段之會議進行，並在該研討會發表投稿之論文，報告期間全程使用英文。

21 日上午先是參與開幕儀式，並請幾位特約講師講解感知無線電與協作通信網絡、智慧電網及 4G 通訊標準等研究領域的最新內容。22 號下午開始直至 23 日會議結束都是由各個議程的報告者報告其研究內容，其他午/晚餐時間與各成員的交流便不在此贅述。

本人主持時段之議程包含本人與其他五位演講者，其中僅有一位爲教授，其他都是博士或碩士生。第一位演講者 Lei Sun 介紹了在日本利用 3D 技術模擬虛擬實境的各種應用。虛擬實境爲一當前熱門的話題，它所包含的技術與應用層面相當廣博，此外它對人類的生活所造成的影響與衝擊正與日俱增。它將帶領人類進入一個嶄新、前所未有的多樣感知的仿真世界，提供人類與電腦之間溝通的介面，並強化電腦解決問題的能力，甚至將成爲人與人之間互動的媒介；第二位報告者 Carlos Rioja del Río 爲一西裔人士，也是本議程報告者中唯一一位教授。他的報告內容爲介紹其爲 CPU 設計的動態排程(dynamic scheduling)方法及其撰寫的排程模擬器，因虛擬機器的資源管理成爲重要的議題，在服務虛擬化技術中，CPU 的調度是關鍵，虛擬機器如何對應實體機器的工作排程會直接影響到整體系統效能表現；本人爲第三位報告者，報告內容於心得中介紹；演講者 Zhongtao Li 介紹了 P2P 系統 CAN 並提出了改良，由於 CAN 是利用多維座標空間概念來建構的點對點架構；CAN 也是利用每個節點所擁有的路由表（coordinate routing table）來搜尋檔案，藉由設計的傳輸協定確可改善 P2P 檔案共享系統的運作效能。Xian-Feng Sheng 介紹了利用雲端技術中的分散式隱私雲(distributed-private cloud)對資源進行分配的動態調整（dynamic adjustment）演算法，由於電腦網路頻寬及硬體設備相關技術發展快速，讓網際網路相關程式運用更加發展快速，因近年來雲端主題更加討論熱絡，而且雲端運算又主要是透過分散節點協力合作完

成一個大型的工作研究在一個動態階層式雲端運算網路架構下，結合排程演算法之內容，使得每個需要執行工作能被分配到適合的資源並且有效提昇每個服務節點負擔與降低資源浪費；最後一位講者 Chengqi Yi 介紹了他在微網誌方面的研究，微網誌與一般傳統部落格不同，其中檔案容量較傳統的部落格小，但是使用者上還是會在相同事務上有其原因運用它的道理，強勢回應的風險，針對企業回覆相關問題時，需先學會尊重提問人，因爲微網誌的傳播速度是無遠佛屆，短時間可以集結大量的聲援，因此需要理性溫和處理客戶的反應才不會造成反彈聲浪；微網誌同時也能輕鬆地即時抒發自己當下的心境來表達自己的想法內容，但是在留言過程中需小心不要帶有任何言語有關政治評論造成網友們熱烈討論。

(三)心得

雖然發表的文章是屬於 P2P 網路的研究，但是本著符合本計畫宗旨並希望增進跨領域知識的原則，筆者亦參與了大部份的演講。然而，雖然網站上公布 5 大研討會中都包括和資訊安全相關的議題，但在與會前夕才得知發表之文章中僅有兩篇牽涉到資訊安全議題，迫於註冊費已繳且機票已訂妥，本人只能選擇挑出該兩篇文章進行簡單介紹。因此，本篇心得報告包含了本人發表之文章以及其他兩篇和資訊安全相關文章的簡單介紹並附上參與報告之照片於附錄以茲證明：

(1) 點對點網路節點下(P2P)查詢(RDF-Chord: A Semantic-based P2P System for RDF Queries)

由於 Peer-to-Peer (P2P)軟體在資源分享方面被廣泛的使用，大量的資源被存放於 P2P 系統之中，因此，當使用者在搜尋資源時，可能會得到大量、駁雜以至於難以篩選的結果；亦可能發生搜尋的結果不符合需求的情況。許多研究試圖在 P2P 系統中加入語意的架構，藉著語意來描述資源以達到支援複雜的語意查詢，並提供更加精確的查詢結果。這些結合語意的 P2P 系統被稱爲語意式 P2P 系統(semantic-based P2P system)。在本研究中我們提出了 RDF-Chord，一個能夠支援八種資源描述框架(RDF，Resource Description Framework)的合取/析取查詢(conjunctive/disjunctive query)以及範圍查詢(range

query)的語意式 P2P 系統。RDF-Chord 採用多層的架構，成功的提高了查詢的效率並降低維護成本，使得系統在整體上的成本低於其他功能類似的系統。

(2) P2P 非構造式攻擊和可擴展的分佈式網絡(A Method to Construct an Attack and Fault Tolerant Scalable Distributed Network)

P2P 系統如 Gnutella 由許多分散的節點所組成，能夠有效的分散由傳統集中式伺服器-客戶端架構所帶來的 traffic 問題。然而也因爲不使用集中式伺服器，這些 P2P 系統對於網路故障(network-failure)以及節點大量進出網路的容忍度很低。因此，此篇論文依據兩種網路故障的情況：網路節點自然進出以及由網路攻擊所造成的故障進行模擬。此論文提出了雙峰度(bimodal degree)的計算方式，並以 Gnutella 爲基礎，根據節點峰度的分布構築了一個對於錯誤容忍度高的 P2P 架構。

(3) 安全和實用的認證和金鑰協議智能卡(Secure and Practical Authentication and Key Agreement Scheme Using Smart Card)

此篇論文探討了前人所提出在智能卡(Smart Card)上進行認證和金鑰協議(key agreement)的方法，指出前人的方法中容易遭受攻擊的部份，並依此提出了一個加強安全性的方法。

(四)建議

(1) 在 P2P 非構造式攻擊和可擴展的分佈式網絡(A Method to Construct an Attack and Fault Tolerant Scalable Distributed Network)一文中提出的問題乃是針對非結構式系統，然後許多系統採用的是結構式或混合式的系統，這些系統是否會遇到類似的問題，以及是否能夠更好的解決這些問題，是一個值得研究的方向。

(2) 我們可以發現在眾多的議題當中，P2P 系統的資訊安全問題已經漸漸受到重視。除此之外，也有一些研究在探討社群網路中的隱私問題。由於社群網路運作的模式其實十分類似 P2P 系統，將 P2P 結合社群網路並解決個人隱

私方面的資訊安全問題亦是一個可能發展的方向。

(3) 本會議主辦於桂林，因此對於無出國經驗的研究生來說，在吃、住不至於因爲語言隔閡產生不便的情況；又此會議爲國際會議，在會議中全程使用英語，也能夠學習到使用英文報告、溝通的經驗，建議針對有潛力但無出國發表經驗的學生，能夠考慮補助參與會議，以提供其出國磨練的機會，並減輕其因英文對話需求所帶來的緊張情緒，使其未來在跨足國際之時不至因無經驗及恐懼而裹足不前。

三、附錄

(1) 議程

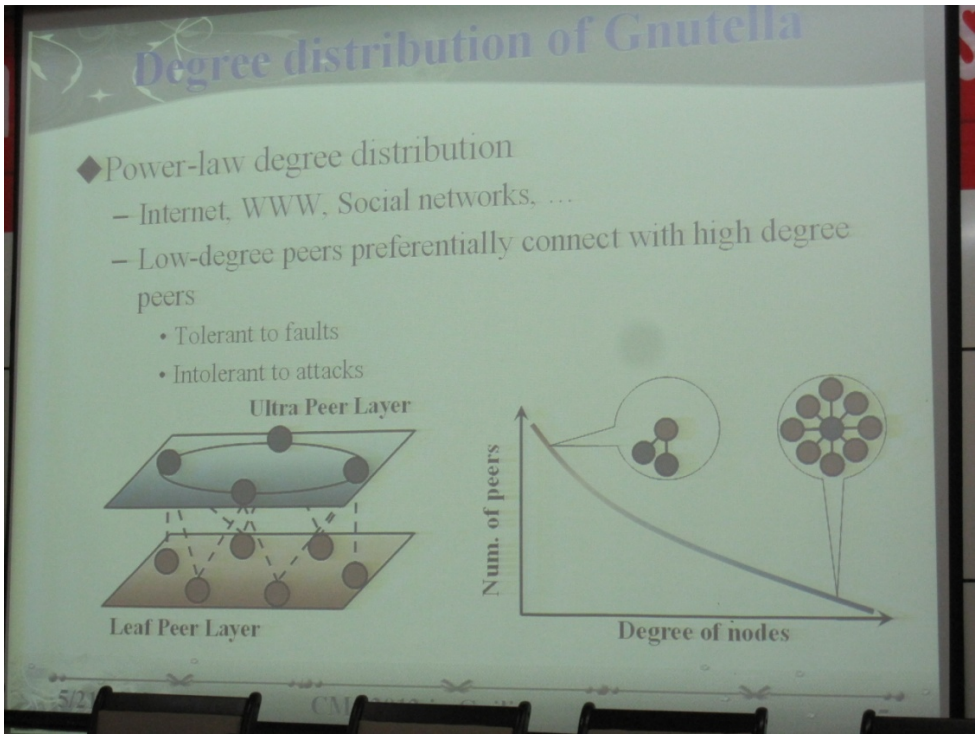
表一、議會議程

Day	Time	Paper No.	Room
Monday 21 May	7:30-12:30	7:30 Start registration 8:30-8:45 Opening speech given by Prof. Cheng-Xiang Wang 8:45-9:00 Welcome speech given by Prof. Simin Li, Vice- President of Guilin University of Electronic Technology 9:00-10:00 Keynote speech 1 given by Prof. Ying-Chang Liang 10:00-10:30 coffee/tea break 10:30-11:30 Keynote speech 2 given by Prof. Nirwan Ansari 11:30-12:30 Keynote speech 3 given by Prof. Vincent Lau	
	12:30-13:30	Lunch	
	14:00-15:30	5	SS1
	15:30-16:00	Coffee/Tea Break	
	16:00-18:00	8	SOCN & VTT & CNFI
Tuesday 22 May	8:30-10:00	3	SS2
	10:00-10:30	Coffee/Tea Break	
	10:30-12:30	6	WCNS1
	12:30-13:30	Lunch	
	14:00-15:30	6	CS1

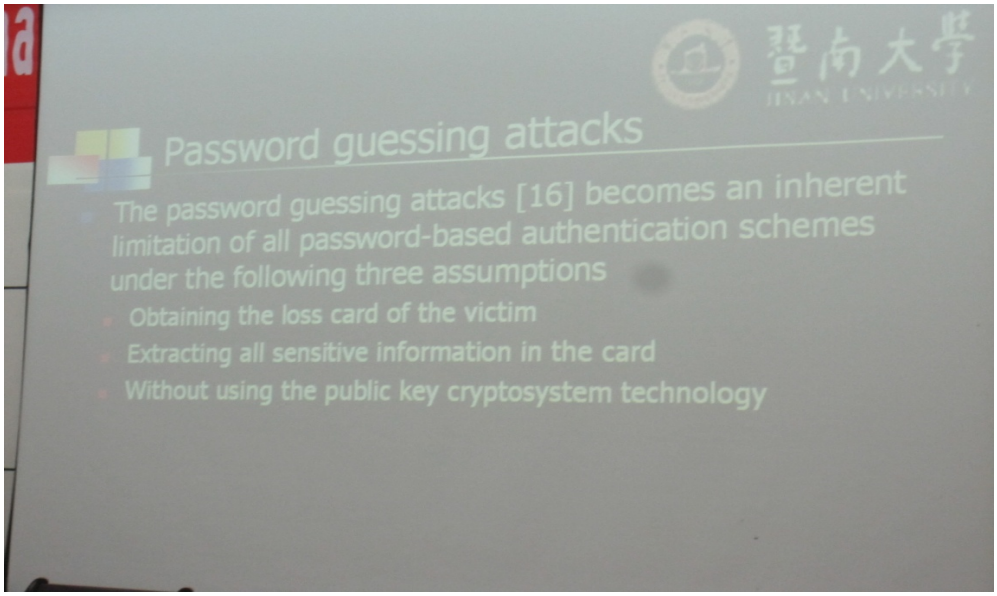
	15:30-16:00	Coffee/Tea Break	
	16:00-18:00	7	CS2
	18:00-20:00	Banquet	
Wednesday 23 May	8:30-10:00	7	WCNS2
	10:00-10:30	Coffee/Tea Break	
	10:30-12:30	7	WCNS3
	12:30-13:30	Lunch	
	14:00-16:00	7	WCNS4

(2) 與會照片

圖一、RDF-Chord: A Semantic-based P2P System for RDF Queries



圖二、A Method to Construct an Attack and Fault Tolerant Scalable Distributed Network



圖三、Secure and Practical Authentication and Key Agreement Scheme Using Smart Card