出國報告（出國類別：訪問、考察、學術交流）

江西師範大學訪問、考察、學術交流報告

服務機關：國立中正大學資管系
姓名職稱：古政元教授
派赴國家：中國大陸
出國期間：103 年 03 月 06 日至 103 年 03 月 10 日
報告日期：103 年 05 月 07 日

摘要

此行前往中國大陸江西師範大學的目的在透過訪問、考察、學術交流等活動加強與中國大陸大學院校間的學術交流與未來的合作可能，尤其江西師範大學的前身是中正大學，兩校之間確實有某種特殊程度的連結，所以兩校校方早已簽署成為姊妹校，這次除了透過講學、合作交流會議及學生交換協議確立更多實質合作關係與管道之外，也希望能更進一步的深化彼此間的合作強度。

由於國立中正大學的學術水準在國際上一直表現相當優秀，因此也吸引許多中國大陸江西師範大學學生的想往，本校管理學院與江西師範大學商學院之前已經建立非常深厚的友誼，彼此間的互動相當頻繁，此次為了宣傳我校的聲譽以及招收大陸的優秀學子，並洽談合作交流協議及學生交換的方式，再加上江西師範大學商學院的極力邀約，因此我等在主秘及管理學院院長帶領之下前往該校訪問、考察及學術交流。大陸地區的大學雖然進展頗快，然實質內涵及整體發展仍有很大的精進空間，近些年開始投入對外交流，但與臺灣的大學院校進行密切交流的時間不算太長，因此彼此間也還處在摸索互動的模式之下，期許此次參訪能為爾後的實質交流建立起良好的基礎。

目次

目的

本計畫所欲達成的目的如下：

(1) 加強本校管理學院與江西師範大學商學院之前已經建立起的深厚友誼。

(2) 宣傳國立中正大學的聲譽和研究成果以及吸引中國大陸的優秀學子。

(3) 談判達成實質交流之協議及老師學生交換的方式。

過程

103 年 03 月 06 日晚上 18:05 抵達南昌昌北機場後，江西師範大學商學院安排專車接往該校瑤湖校區住宿白鹿會館。

第二天，103 年 03 月 07 日上午 9:00 起，由江西師範大學商學院趙院長陪同我校一行人參觀校園，參觀地點包括了校史柱、校史館、圖書館、檔案室等。該校之檔案室存放有許多當年創校為中正大學時歷史非常悠久的文物，例如中正大學印信、創校校長手札、中正大學公文及當年之中正大學聘書等，這些文物雖然與本校國立中正大學並不直接相關，但由於校名相同，仍然引起我等一行參觀人士的駐足觀賞。詳見下圖一至五。

圖一 校史柱 (前方四根長柱)

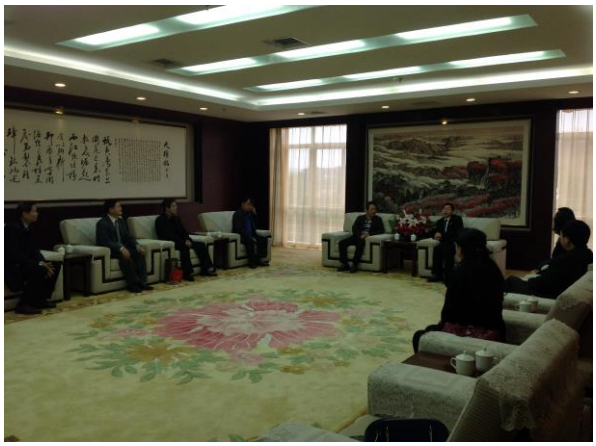
圖二 檔案室

圖三 校史館

圖四 圖書館(一)

圖五 圖書館(二)

參觀完校史柱、校史館、圖書館、檔案室後，上午 11：00 我等前往知行樓會見該校領導，陪同會見人員包括校辦、港澳台辦、商學院趙院長等人，詳見下圖六與七。



圖六 會見領導、校辦、港澳台辦、商學院院長

圖七 眾人合影

下午 2:30~4:30 前往商學院進行演講座談及國立中正大學管理學院與江西師範大學商學院合作交流協商。演講座談主題為資訊安全與管理，首先由國立中正大學管理學院洪新原院長簡報本校管理學院在資訊安全與管理所投資的設備及相關之研究成果，接下來由本人資管系古政元教授進行專題演講，我所講授的題目為無線感測網路中節點複製攻擊的偵測方法。現今，無線感測網路已被廣泛使用於許多應用當中，例如家庭安全監控，醫療應用以及交通管制等，然而，節點複製的攻擊已經被證明對無線感測網路造成莫大的傷害，但卻一直沒有被很有效率的處置。因此，在這項研究中，我們提出一個需要較少成本和通訊流量的檢測方法，經由詳細之分析和模擬後顯示，該方法有很不錯的效率，整個演講的投影片列在附錄一中供作參考。下一場的演講則由施東河教授講授行動支付。

演講完成後進行詢答，江西師範大學商學院電子商務系主任孫德林提出了三個非常大但與演講議題較無關的問題。具體問題如下：

一、我校在碩士點和本科電子商務專業設置了電子商務與信息化創業方向，請從學科和專業建設視角提出指導性意見。

二、請對我校電子商務與信息化創業卓越工程師拔尖創新人才培養方面提出建設性意見。

三、我校目前正在建設全校集中的實驗大樓，其中有 1200 平方的面積是建設為電子商務實驗中心（以國家教育部電子商務與信息化創業卓越工程師培養項目為基礎），我們準備設置以下 14 個實驗室：

1. 電子商務模擬實驗室
2. 數據庫與商務智能實驗室
3. ERP、CRM、SCM 實驗室
4. 物流工程實驗室
5. 移動電子商務實驗室
6. 網絡營銷策劃與數据挖掘實訓室
7. 物聯網與雲計算實驗室
8. 網絡金融實驗室

9. 文化創意產業創業實驗室

10. 電子商務戰略性新興產業實驗室

11. 電子商務與信息化創業綜合實驗室

12. 電子商務與信息化創業卓越工程師實驗室

13. 《創業基礎》課程實驗室

14. 阿里巴巴電子商務創業實訓室

請對這 14 個實驗室的設置和實驗室的軟體、硬體的配置情況提出建設性的意見。

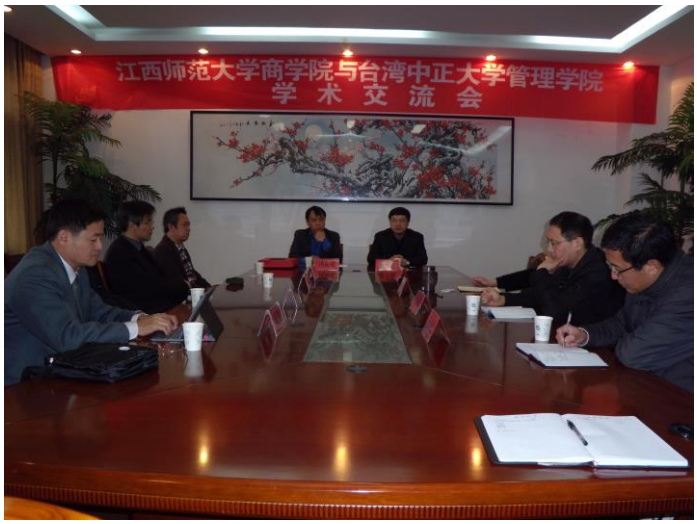
由於時間有限，所以除了院長略作說明之外，我個人提供建議該系應該透過加強對外交流去得到這方面資訊，此外我也告知可以提供我在敝校資訊安全與管理實驗室和行動商務實驗室建置的經驗供作參考。

在演講及 QA 完畢之後，該院許多學生仍積極上前與我方教授攀談與問答，從這也可以看出該院學生之好學不倦精神。

國立中正大學管理學院與江西師範大學商學院學術交流會議

講學完畢之後，於 2014 年 3 月 7 日下午 3:30 至 4:30 間，國立中正大學管理學院與江西師範大學商學院舉行學術交流會議，會議記錄如下:

應江西師範大學商學院趙衛宏院長邀請，國立中正大學主秘及管理學院洪新原院長一行 6 人於 2014 年 3 月 6 日至 10 日對江西師範大學商學院進行了回訪。2014 年 3 月 7 日下午 03:30 開始，兩院在商學院三樓會議室舉行了學術交流會議。國立中正大學主任秘書陳朝輝，管理學院院長洪新原，資管系教授古政元，運競系主任林晉榮，雲林科技大學資管系教授施東河；江西師範大學商學院院長趙衛宏，黨委書記李曉園，副院長劉榮春、吉宏，黨委副書記張漢龍參加會議。詳如下圖八所示。



圖八 國立中正大學管理學院與江西師範大學商學院學術交流會議

會議雙方介紹了各自學院概況以及大學部教學、研究生教育、學生管理、對外交流等方面的情況，並就進一步鞏固兩院友好關係，推進兩院交流與合作事宜進行了商討。雙方會議所形成之會議結論如下：

一、雙方同意由江西師範大學商學院每學期派遣 2 名交換生、8 名訪問生赴國立中正大學管理學院交流。國立中正大學按照本校政策給予交換生和訪問生相對應之優惠待遇。其中，訪問生按照國立中正大學相關規定繳納費用，但由管理學院盡最大努力向校方爭取免除學費。

二、雙方原則同意互派專業教授到對方院校擔任兼職教師或進行合作研究，具體方式及細節問題有待雙方進一步商議協調。

三、雙方原則同意在職責權限清晰的前提下，開展聯合指導研究生方面的合作，具體方式及細節問題有待進一步商議協調。

四、如果國立中正大學申辦 2016 年亞太電腦資訊系統年會（PACIS）成功，則邀請江西師範大學作為大會的協辦單位，具體負責大陸地區大學院校參與此次國際學術會議的聯繫協調以及論文收集等工作。

第三天，103 年 03 月 08 日時值週六，一行人略作休息。

第四天，103 年 03 月 09 日時值週日，由江西師範大學商學院安排前往南昌市中心之校本部參觀暨觀摩假日 EMBA 班上課教學情形，我們看到該院 EMBA 外語課程由美國教師教導 EMBA 學生英文的

聽說讀寫，這樣子的規劃讓這些業界在職學生的英文能力突飛猛進，頗值得我方學習，稍晚該院安排我等一行人與 EMBA 學生餐敘，藉此我們聽取這些學生在學習上的意見，相信可以做為我方未來調整 EMBA 課程的參考，席間該院 EMBA 學生表達嚮往未來將前往台灣移地教學。

第五天，103 年 03 月 10 日，一早起床後眾人搭機返台。

心得及建議

參與此次中國大陸江西師範大學訪問、考察及學術交流活動，著實有不少的收穫，也讓我留下深刻的印象。大陸地區的大專院校如獲選為國家之重點培育對象時，將獲得相當可觀經費的挹注，硬體設備得以發展迅速，但是師資水準及實質內涵等軟體條件卻不是一蹴可幾的，目前仍有很大的改善空間，因此許多學校有很高度的意願與臺灣的大專院校進行交流，江西師範大學是中國大陸江西省的重點大學，目前該校的資源與學生人數皆呈現成長的狀態，所以亟欲與本校建立起更密切的合作關係，希望透過國立中正大學在國際上的聲譽及學術上成就提升該校的學術水準和研究成果。台灣大專院校目前所面臨的問題除了經費拮据之外，碩博士研究生人數及做研究能力大幅衰退，因此藉由雙方的交流或許可以互相有所助益。

此次演講完後，商學院電子商務系主任孫德林提出的問題在在顯示，該校不缺資源及優秀學生，但缺乏有豐富研究經驗與深厚國際關係的學者帶領大型計劃及建立專業實驗室，我方則有許多優秀的教授學者但需要資源及優秀學生的參與，所以這也是雙方可以截長補短的另一例證。

大陸地區的大專院校近年積極對外發展，因此我方可感受到其亟欲拓展交流深度的意願，中國大陸地大物博，各地區的文化特色差異頗大，代表性學校的發展也都各有特色，也或有許多可供我方大專院校參考學習之處，汲取他人之長也可以是改進我們自己的良好方法。尤其中國大陸地區的同學對於至台灣擔任交換學生或訪問學生的意願非常高，這從與該校學生接觸的過程當中可以強烈的感覺出來，因此這次的國立中正大學管理學院與江西師範大學商學院學術交流會議中，該校商學院積極爭取增加免學費交換生的名額，經我方帶回相關要求並呈請我校吳校長裁示，基於與江西師範的特殊情誼，校長同意將免學費的交換學生名額由 2 名提高到 8 名，管理學院院長洪新原教授立即回覆電子郵件告知江西師範大學商學院院長趙衛宏。電郵細節如下：

-----Forwarded message-----

From:洪新原<syhung@mis.ccu.edu.tw>

To:cysung<cysung@ccu.edu.tw>,陳朝輝教授<seichen@eq.ccu.edu.tw>,林晉榮<zinronglin@gmail.com>,古政元<cooperku@mis.ccu.edu.tw>,施東河理事<shihdh@gmail.com>,vita tai<hotelday0605@gmail.com>,zwh4005@sina.com<zwh4005@sina.com>

Date: Tue, 22 Apr 2014 10:34:57

Subject: Re: 回复：江西師大商院訪問

趙院長, 您好:

有個好消息, 讓您知道. 就是本校吳校長已經同意, 基於與江西師範的特殊情誼, 特將免學費的交換學生名額由 2 名提高到 8 名. 希望貴院能積極爭取, 好好運用. 謝謝!

p.s. 這次的努力, 陳主秘使力甚多.

洪新原

由於少子化的關係，目前國內大學招收足夠優秀研究生以協助教授進行研究已經越來越困難，這個現象到了今年更為嚴重，這將大大影響我大專院校的研究能量與研究產出，或許在不影響我國內研究生就學權益的前提之下，加強招收中國大陸地區優秀研究生是可以考量的解決管道之一，我國立中正大學已提供不小優惠給予江西師範大學商學院，因此或該與江西師範大學商學院合作，請其選派優秀教師及研究生參與我校教授主持之研究計畫，這有可能稍解目前我校教授缺少優秀研究人力(尤其是博士班學生)的現況。

此外，在觀摩江西師範大學商學院 EMBA 教學後，我建議我方管院 EMBA 加入外師的外語課程以增強學生英文的聽說讀寫能力。

附錄一

A Detection Method for Replication Attacks in Wireless Sensor Networks

Dr. Cheng-Yuan Ku
Department of Information Management
National Chung Cheng University, Taiwan, R.O.C.

Curriculum Vitae

- National Chiao Tung University, Control Engineering, BS, 1987
- Northwestern University, EECS Master, 1993
- Northwestern University, EECS Ph.D., 1995
- Specialty: Computer and Communication Network, Information Security and Management, Applications of E- and M-commerce, Cloud Computing

Introduction (I)

- Nowadays, the wireless sensor networks are widely used in many applications, such as home security monitor, healthcare applications, and traffic control.
- However, a new-type attack named node replication has been proved to be a harmful attack for WSNs.

Introduction (II)

- Node replication attack is an attack that adversaries capture nodes and extract some secret information to duplicate nodes instead of compromising the cryptosystem.
- With increasing clones of the sensor nodes, adversaries could control the network gradually.

Introduction (III)

- We propose an improved method which needs less memory and communication cost to detect the so-called node replication attack.
- Simple analysis shows that this method is efficient.

Related Works (I)

- Within earlier papers, two types of general approaches against node replication attacks named Centralized Detection and Local Detection were proposed.

Related Works (II)

- The Centralized Detection relies on a central base station which examines every neighbor list of sensor nodes. If the replicated node is discovered, it floods the message to the whole network.
- However, there are usually high volumes of traffic near the base station.

Related Works (III)

- The idea of local detection is that every sensor is responsible for its neighbors. If any node finds suspicious node, the voting mechanism could get rid of it.
- Unfortunately, this local detection fails to detect two replicated nodes which locate faraway more than two hops or above.

Related Works (IV)

- Parno et al. suggested two protocols: Randomized Multicast protocol and Line Selected Multicast protocol which are improved from the previous solutions.

Related Works (V)

- In Randomized Multicast protocol, each node announces its location, and their neighbors randomly select the witness nodes to forward this claim for verification.
- However, this protocol needs a high communication cost since the claim messages are almost flooded throughout network for high detection rate.

Related Works (VI)

- As for Line Selected Multicast Protocol, the neighbors send the location claim to the witnesses who are randomly selected and every node stores the location claim along the way.
- Once the intermediate node receives conflicting claim message, it broadcasts the alert message. However, they assume nodes are stationary.

Detection Method (I)

- **Step 1: Random Number Broadcasting**

  A random number R(t) is generated at time t. R(t) is distributed to all nodes by the coordinator. Central-based station is not necessary because the coordinator could be a general sensor node elected by voting mechanism.

Detection Method (II)

- **Step 2: Signature Authentication**

As a node α receives R(t) at time T(α), this node signs its ID and T(α) and then pass this authentication to each neighbor. T(α)'s would be different if they come from different nodes because these values are related to the distances and the routing paths.

This makes the adversary difficult to predict T(α)'s because the routing path is different for each transmission.

Detection Method (III)

- **Step 3 : Select the Witnesses**

Each neighbor of node (α) will receive authentication and then send to a set of witnesses with probability P_λ. If P_λ is selected to be high, the detection rate will be high with high communication cost.

The set of witnesses is generated from a random function, Random_Fun [ID (α), R(t)]. Therefore, the witnesses could be anywhere. It makes the adversary hard to comprise all ubiquitous witnesses.

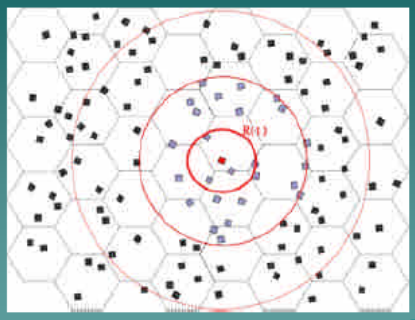
Detection Method (IV)

- **Step 4: Detection**

When the witness receives authentication at the first time, it simply stores it in memory and extracts ID(α) into cache for duplicate verification. If another authentication is received with different T(α') but the same ID, then this witness will send alarm to all nodes.

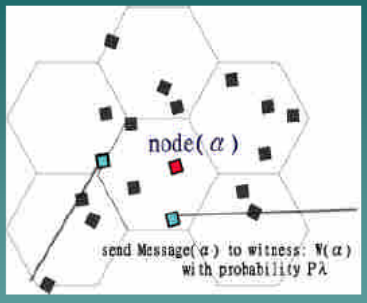
In fact, there is usually a set of witness responsible for detecting a node.

An Example (I)



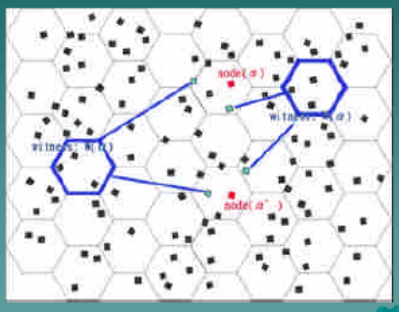
Random Number R(t) is broadcasted

An Example (II)



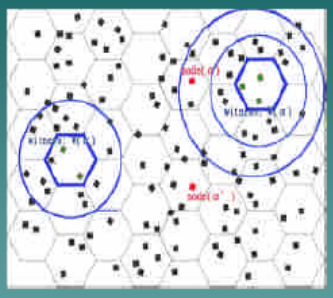
Neighbors would select the witnesses and send the authentication

An Example (III)



Some groups of nodes are selected as the witnesses

An Example (IV)



The witnesses alarm all nodes by flooding network

Protocol Analysis (I)

- We assume only one witness for detection. (G=1)
- E[Detection Rate for one replication node]= $(1-(1-P_\lambda)^d)^2$

Protocol Analysis (II)

Table Success Rate for Detecting One Replication under Different P_λ

Prl	P_λ	d	Prl	P_λ	d
0.996998	0.15	40	0.993240	0.15	35
0.999734	0.2	40	0.999915	0.25	35
0.999980	0.25	40	0.999189	0.2	35
0.999999	0.3	40	0.999992	0.3	35
0.984797	0.15	30	0.966900	0.15	25
0.997526	0.2	30	0.992458	0.2	25
0.999643	0.25	30	0.998495	0.25	25
0.999955	0.3	30	0.999732	0.3	25
0.923983	0.15	20	0.832922	0.15	15
0.977074	0.2	20	0.930869	0.2	15
0.993668	0.25	20	0.973452	0.25	15
0.998405	0.3	20	0.990527	0.3	15

Conclusions

- In our protocol, the mobile sensor nodes are considered since it is reasonable for the sensor nodes to be mobile, not stationary, in the real world.
- Besides, our protocol provides good communication overhead and lower memory need compared with previous protocols and the probability of detection is high.