出國報告（類別：國際會議）

創新、通訊及工程國際研討會議

服務機關：國立中正大學前瞻製造系統頂尖研究中心
姓名職稱：文志超博士後研究員
派赴國家：中國
出國期間：民國 104 年 10 月 23 日至 104 年 10 月 28 日
報告日期：民國 104 年 11 月 23 日

摘 要

ICICE 2015 創新、通訊及工程國際研討會 (International Conference on Innovation, Communication and Engineering, ICICE)於 2012 年開始舉辦且為亞太地區知名工程創新研討國際會議，該研討會的緣起最初由臺灣學者專家發起共同成立之以工程研發與知識創新為宗旨之學術機構，定名為臺灣知識創新學會 (Taiwanese Institute of Knowledge Innovation, TIKI) 。集合國內有志於知識創新學術研究之專業人士，共同促進數位內容學術研究發展，為我國知識創新產業技術發展與人才培育做出貢獻。為反應資通訊與製造自動化技術全球化的快速轉變，參加國際間有關知識創新學術相關工作，融合兩岸地區大學與研究機構積極參與，定期舉辦集會與國際性學術會議，推動相關工程技術與知識創新為基礎之專業研究與交流。

今年度 ICICE 2015 研討會是由是由臺灣知識創新學會（TIKI，臺灣)、福州大學（FZU，中國)、及中國湘潭大學（湖南/湘潭）共同籌辦，定於 2015/10/23 至 2015/10/28 於中國湖南省長沙市舉辦(2015)的國際研討會議。

目　次

壹、出國目的 1

一. 前言 1

二. 會議主題與特色 1

貳、會議活動簡介 2

一. 議程活動 2

二. 議題介紹 5

參、與會研討交流 6

一. 主要議題研討 6

二. 個人研討心得 7

肆、建議與總結 9

一. 建議 9

二. 總結 9

附 錄 10

壹、出國目的

一、 前言

臺灣知識創新學會與臺灣及中國大陸多所知名大學於 2015 年 10 月 22 日開始在中國湖南湘潭及張家界舉辦 2015 年創新、通訊及工程國際研討會 (International Conference on Innovation, Communication and Engineering; ICICE 2015)，匯集各產官研學界相關領域學者專家於 2015 年 10 月 23 日至 28 日共襄盛舉。本次研討會亦開放籌組特定議題(invited session)。

二、 會議主題與特色

ICICE 2015 國際研討會為鼓勵工業界，學術界和政府機構的專家溝通對話，交換彼此研究和開發經驗，實踐專業經營管理方面和工程領域的創新理念。今年主辦ICICE2015 國際研討會活動的目的，集結各產業與學術研究人員的相關成果，提供一個共通的交流平台。

此次研討會含有下列各領域或主題特色：

(一) 先進材料科學與工程

(二) 資訊科學與信息技術

(三) 通信科學與工程

(四) 創新設計，工業設計，創意設計

(五) 應用數學與計算機科學

(六) 管理科學

(七) 文化創意研究

(八) 電機與電子工程

(九) 機械與自動化工程

(十) 綠色技術和體系結構工程

貳、會議活動簡介

前瞻通訊與工程科技國際研討會 (International Conference on Innovation, Communication and Engineering; ICICE 2015)，匯集各產官研學界相關領域學者專家共襄盛舉，會議時間在 2015 年 10 月 23 日至 28 日。本次研討會除主題議程 (regular session) 外，亦包含自行籌組特定議題之議程(invited session)。主要會議行程表與相關活動參與介紹如下：

一、 議程活動

(一) 註冊報到

正式會議在 (10/23, 9:00am) 開始會場註冊報到，隨後便在會場工作人員導覽下，參觀各項活動會場的展示簡介。

2015 International Conference on Innovation, Communication and Engineering
October 22 - 29, 2015, Xiangtan, Hunan, P.R. China
ICICE 2015
4th Intl. Conf. Inno. Comm. Eng.
2015
The 4th
International Conference
on
Innovation
Communication
and Engineering
(ICICE 2015)
Changsha, Hunan, P.R. China
Xiangtan, Hunan, P.R. China
TAKI
灣 知
anese Institut

圖一、 ICICE2015國際研討會會場展示大廳(北辰洲際飯店)

(二) 會議開幕式

大會的開幕儀式在 9:15am 開始，首先由大會主席 A. D. Kim-Tak Lam 教授致歡迎詞，本次會議投稿共計收到 1058 篇，其中有 222 篇經大會評審委員選擇在 ICICE2015 會議中發表。

圖二、 ICICE2015國際研討會大會開幕致詞

(三) 大會專題演講

大會的第一場專題演講 (Keynote Speech) 緊接著在開幕儀式後於 10:30am 開始，由美國德州奧斯汀大學 (University of Texas at Austin) STEM 教育中心 (Center for STEM Education) James P. Barufaldi 教授發表，講題與相關內容，如下：

講題：以 STEM 科際整合教育對工程人才培育的觸媒作用 (Topic: Engineering as the Catalyst in STEM Education)

圖三、 ICICE2015 專題演講學者 James P. Barufaldi 教授

Barufaldi 教授目前擔任首席調查員為德州區域 Collaboratives 卓越的科學和數學

教學，首席研究員為美國國家科學基金會資助的項目，儀器開發探索專業成長和建構的兒童知識和技能的科學基礎平台目標。他曾擔任 UTeach 中學科學聯席主任和數學教師培養計劃，並編審 70 多博碩士論文在科學教育。從他的演講中提及科學、科技、工程與數學（Science, Technology, Engineering, Mathematics, 簡稱 STEM）的科際整合教育議題在近年來受到許多的關切與重視，從美國國家科學委員會與美國總統科技顧問委員會的報告中，不難看出美國重視培育 STEM 人才的趨勢。美國推動 STEM 科際整合教育的主要目的，以提升其國民科學與數學素養為主軸，藉此期望在國際學生能力評量測驗能有大幅的成長。

因此省思國內對於科技研發工程人才的培育，需透過動手實作活動可以培養整合理論與實務的能力。依據相關文獻的研究顯示，若針對學生的動手實作活動過程進行分析，可以發現多數學生在設計解決方案時，常憑直覺進行設計，而並非確實應用科學、數學等學科知識進行理論導向的設計。換言之，即使學生透過這些動手實作活動進行學習，學生也未必能夠在動手實作活動的過程中，培養如何整合理論與實務的能力。有鑑於此，欲推動 STEM 科際整合教育，並藉此培養能夠整合理論與實務的科技人才，應可在中小學階段強調動手實作課程，並將理論導向的設計、探究等策略納入動手實作過程中，以藉此培養學生整合 STEM 知識與實務的能力。

圖四、 ICICE2015 專題演講會場國際會議廳

二、　議題介紹

由本屆大會的研討內容之主題可分成資訊科學與信息技術、通信科學、電機與電子工程與工程與機電自動化工程整合科技等重要領域。針對目前物聯網應用與大數據分析，進行創新設計，工業設計，創意設計等相關議題的論文發表。

以下綜合整理本人參與主題研討 (Regular & Special Sessions) 場次，聽取簡報議題之相關論文內容介紹。

在通信科學與技術(Communication Science & Engineering) 領域，主要提到的無線通訊編碼正交分頻多工(OFDM)技術，以及應用在行動通訊傳輸品質改善的多因素分析與決策(MCDM)機制，將是未來應用的關心議題。。

在創新設計與創造力設計 (Innovation Design & Creative Design) 領域，主要提到結合目前熱門物聯網（Internet of Things，IOT)與穿戴裝置（Wearable devices) 技術。物聯網與智慧型穿戴式移動裝置的興起，對於界定使用者需求與結合服務創新來達到使用者經驗之最佳的滿意度，將是更深度思考的議題。在智慧系統的工業與消費整合設計 (Intelligence System Design on Industry and Consumer) 領域，主要提到過往產品開發，專注在產品本身，現今使用者導向設計與設計思考所激發出的軟硬體整合的服務創新，不再是傳統操作簡易性研究的運作模式，應朝向協助企業進行的使用者體驗設計的發展與運作。

参、與會研討交流

一、　主要議題研討

由本屆大會的研討內容之主題可分成資訊計算科學、通訊傳輸技術與機電工程整合自動化科技等重要領域，針對目前物聯網應用與大數據分析衍生問題，提出解決方案。資訊計算科學與通訊傳輸技術對於互聯網發展到今天規模，全球進行傳輸的協議 TCP/IP 協議，無線通訊協議，個人行動終端的構架與操作系統，制定標準化流程技術方案，都提出很好的解決方法。物聯網發展過程中，傳感、傳輸、應用各個層面會有大量的技術出現，會採用不同的策略。如今各專用網路，相互聯網形成大規模經濟整合的商業模式。因此，降低研發成本，統一技術標準，形成一個管理機制，這是物聯網面對問題，政府專門的部門應該出來管理和協調，提出相應的政策、統一法規和協調標準。

資訊計算科學的解決方案主要關注雲端運算“計算力”的 IT 技術與高速網際網路通訊技術兩方面著手進行發展。其中，T.－C Liang 等提出光纖(Fiber)通訊設備的感測組件控制，主要包括身體藉由壓力感知無線射頻標籤，將 ID 與遙測資料藉由標準無線協定傳送，經 Reader 判讀後，再將 ID 與 Telemetry 藉標準化介面傳到電腦。再藉由 J. –M Huang 等提出感測器無線網路，以 Progressive path selection (CCCA)方式，向資料庫軟體介面進行查詢，建構以顧客為核心、資訊透明化的供應鏈。

機電工程整合自動化科技的解決方案主要關注工具機(Machine tool)製造生產流程中，軸向機具運動與刀具更換造成的震動，對加工精度影響的品質效應。Shang －Liang Chen 等的論文針對此現象有深入討論相關機具損壞問題，並提出 ATCDF 偵測預防的方案。

Prof. Chang Liu, Stephen D. Prior 探討具有互補特性 Visual-inertial 感測器系統，可應用於多軸傳動運動與導航定位，移動位置精度、多軸運動狀態預估、以及 GPS-denied 環境對輸出軸運動的性能影響，並結論多感測裝置對應 SLAM 演算法量測定位器與加速規輸出軸的動態特性有明顯的影響，構成穩定性與高精度的補償。

J. T. Zou 提出 3D 運動擷取控制的 Indoor GPS 設計方法，可改善室內環境運動的 shadow effect，提升位置精度響應。

二、 個人研討心得

本人投稿論文的研討主題是智慧通訊信號處理與設計(Smart Signal Processing and Real-time Chip Design)，隨著網際網路整體發展而言，普及化應用造成網路頻寬需求增加，使得網路電話(Voice over IP, VoIP) 的使用率蓬勃上升，如 LINE 與 WeChat 等即時語音通訊軟體。VoIP 是利用網際網路來傳輸語音，其主要的優點有低通話成本、低建設成本、服務擴充容易以及日漸優良化的通話品質，這些優點也促使 VoIP 的網路服務應用越來越多。VoIP 主要是由信令控制通訊協定跟多媒體傳輸通訊協定兩部份所構成，信令控制通訊協定進行多媒體連線通道建立和多媒體傳輸參數交換。

2015 International Conference on Innovation, Communication and Engineering
October 22-29, 2015, Xiangtan, Hunan, P.R. Ch
ICICE
TIKI
臺灣知識創新學會
Taiwanese Institute of Knowledge Innovation

圖五、 作者在 ICICE2015 研討會議之論文成果發表

在通訊安全方面，VoIP 的技術雖然非常進步，但是 VoIP 防禦策略遠遠落後，如

何防禦 VoIP 服務遭受網路攻擊是個非常重要的問題。本論文提出 Traffic Filter 方法，此方法應用於網路之網路層(Network Layer)，能更快速的區分出網路服務之正常流量與不正常流量。本論文亦提出 VoIP Intrusion Detection/Prevention System (IDPS) ASIC 架構之設計與實現，結合 Traffic Filter 跟 SIP Stateful 構成更完善之 VoIP IDPS 網路偵測與防禦系統。

本屆大會作者論文編排在 Invited Session 的主題是 Smart Signal Processing and Real-time Chip Design，與同領域的專家學者交換意見，吸收許多寶貴經驗。在此要向下列諸位教授們表示謝意，雲林科技大學電子系許明華教授、中正大學電機通訊系朱元三教授、吳承崧教授以及虎尾科技大學蘇暉凱教授一併致謝。

肆、建議與總結

一、　建議

本次參與國際研討會 International Conference on Innovation, Communication and Engineering (ICICE 2015) 為第一次參與，研討會的活動內容主要聚焦於資訊、通訊與自動化相關技術整合創新設計及其應用。今年(2015)的會議舉行地點在中國湖南省長沙市國際會議場；由於中國近年來工商業快速大幅躍升，互聯網路基礎建設也蓬勃發展，催生電子商務等網路服務。製造業方面在國際先進數控工具機與控制器的發展，也是重點國家之一。藉由本次研討會議的參與，可體會截然不同的實務研究氣氛。TIKI 知識創新學會雖然成立不久，其成員多半是學界後起之秀，每年在大陸籌辦跨國性國際研討會，建立臺灣與大陸兩岸學術交流搭橋鋪路。目前國際的大型研討會針對製造自動化領域，發表許多相關論文針對重要問題，已提出許多創新見解方案。可因此得知目前國際間諸多製造自動化技術發展，將朝物聯網應用整合自動化科技之虛擬與實機之虛實系統(Cyber Physical System, CPS)相關先進課題，因此推薦國內對於製造自動化相關研究有興趣的專家學者多參加歐美國舉行的 ASME, SME, IEEE 以及 International Federation of Automatic Control (IFAC)國際研討會議。

二、　總結

本人第一次參與 ICICE 2015 國際研討會的活動，與參與研討會學者教授們進行理論與實務經驗交流，助益良多。針對主題內容聚焦於資訊、通訊與自動化 (Innovation, Communication and Engineering) 相關技術整合創新設計及其應用。對於本人日後的研究在自主開發電腦數值控制器(CNC Controller) 之開放性架構平台與即時性作業系統，運動控制即時限制以及智能化控制系統軟體開發等，將是做為未來期刊論文投稿與研討會主題發表考慮的重點。

附　錄

附件一

IEICE 2015 大會手冊與論文集

2015

4th Intl. Conf. Innov. Commun. Eng.

2015

The Fourth International Conference on Innovation, Communication and Engineering

October 23-28, 2015

Xiangtan, Hunan, P.R. China

Organized by:

Fuzhou University, P.R. China

National Formosa University, Taiwan

Chia Nan University of Pharmacy & Science, Taiwan

Kun Shan University, Taiwan

Southern Taiwan University of Science & Technology, Taiwan

St. John's University, Taiwan

Osaka Institute of Technology, Japan

Kongju National University, Korea

Hannam University, Korea

Jimei University Fujian, China

Taiwanese Institute of Knowledge Innovation (TIKI)

Sponsors:

Fujian Information Industry Association

Fuzhou [illegible] Industrial Design Creative Park

[illegible] Fujian [illegible] Industrial Design Co., Ltd.

The International Conference on Innovation, Communication and Engineering

October 23-28, 2015, [illegible]

論文研討 Regular Sessions (Breakout Sessions, 10/23~10/28)

(A) Advanced Material Science & Engineering

(B) Communication Science & Engineering

(C) Computer Science & Information Technology

(D) Computational Science & Engineering

(E) Electrical & Electronic Engineering

(F) Mechanical & Automation Engineering

(G) Green Technology & Architecture Engineering

(H) Innovation Design & Creative Design

(I) Industrial Design & Design Theory

(J) Cultural & Creative Research

(K) Applied Mathematics

(L) Management Science

論文研討 Invited Sessions (Poster Sessions, 10/23)

(IV1) Smart Signal Processing and Real-time Chip Design

(IV2) Intelligence System Design on Industry and Consumer

(IV3) Design Science and Technology

(IV4) Computer Simulation and Data Analysis

(IV5) Creative Media

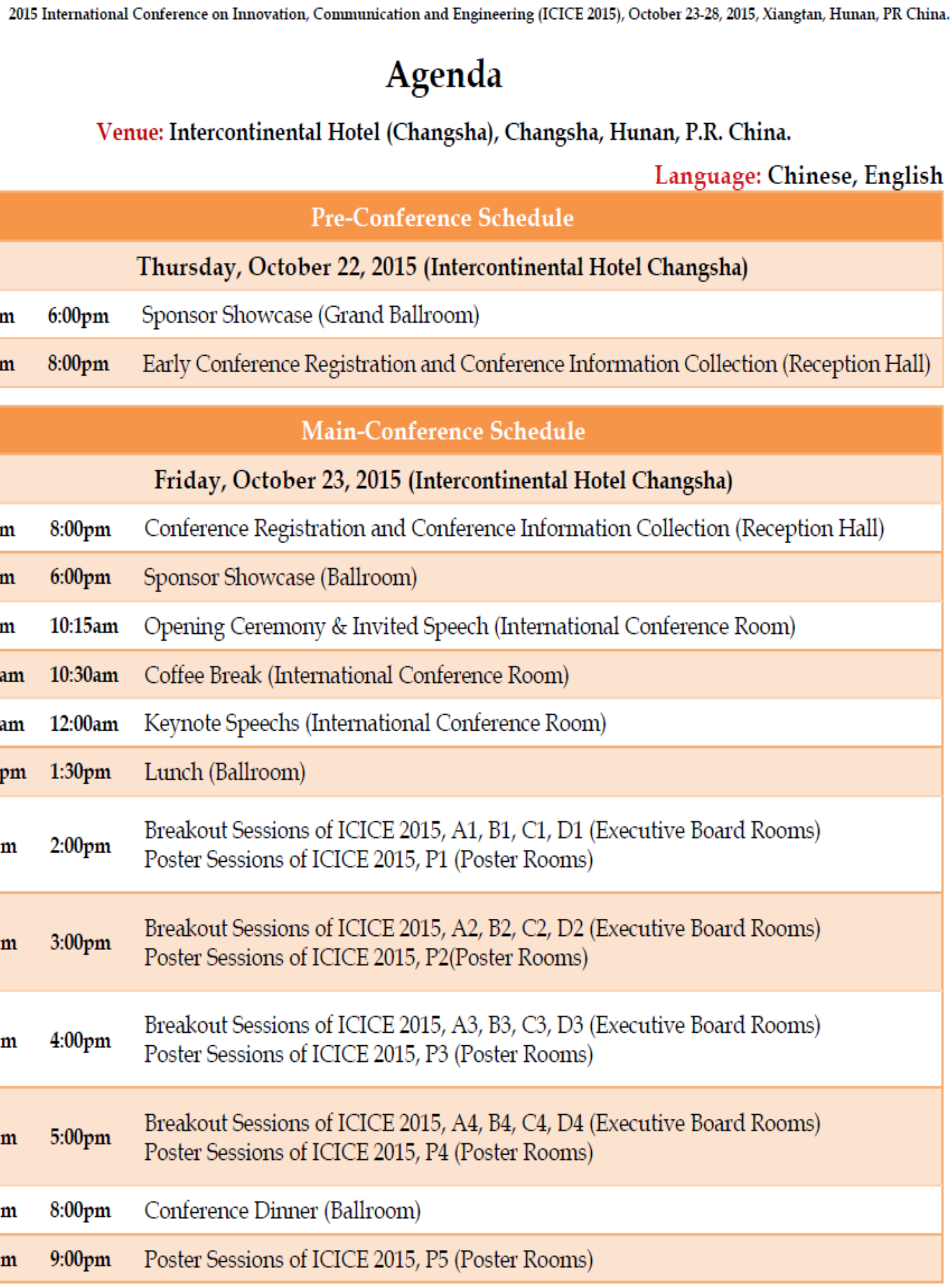
(IV6) Applications for Clustering and Classification Analysis

(IV7) Advanced Materials and Mechanics Application

(IV8) Art & Design

附件二

會議議程表



2015 International Conference on Innovation, Communication and Engineering (ICICE 2015), October 23-28, 2015, Xiangtan, Hunan, PR China.

Agenda

Venue: Intercontinental Hotel (Changsha), Changsha, Hunan, P.R. China.

Language: Chinese, English

Pre-Conference Schedule		
Thursday, October 22, 2015 (Intercontinental Hotel Changsha)		
2:00pm	6:00pm	Sponsor Showcase (Grand Ballroom)
4:00pm	8:00pm	Early Conference Registration and Conference Information Collection (Reception Hall)

Main-Conference Schedule		
Friday, October 23, 2015 (Intercontinental Hotel Changsha)		
8:00am	8:00pm	Conference Registration and Conference Information Collection (Reception Hall)
9:00am	6:00pm	Sponsor Showcase (Ballroom)
9:15am	10:15am	Opening Ceremony & Invited Speech (International Conference Room)
10:15am	10:30am	Coffee Break (International Conference Room)
10:30am	12:00am	Keynote Speechs (International Conference Room)
12:10pm	1:30pm	Lunch (Ballroom)
1:00pm	2:00pm	Breakout Sessions of ICICE 2015, A1, B1, C1, D1 (Executive Board Rooms) Poster Sessions of ICICE 2015, P1 (Poster Rooms)
2:00pm	3:00pm	Breakout Sessions of ICICE 2015, A2, B2, C2, D2 (Executive Board Rooms) Poster Sessions of ICICE 2015, P2(Poster Rooms)
3:00pm	4:00pm	Breakout Sessions of ICICE 2015, A3, B3, C3, D3 (Executive Board Rooms) Poster Sessions of ICICE 2015, P3 (Poster Rooms)
4:00pm	5:00pm	Breakout Sessions of ICICE 2015, A4, B4, C4, D4 (Executive Board Rooms) Poster Sessions of ICICE 2015, P4 (Poster Rooms)
6:00pm	8:00pm	Conference Dinner (Ballroom)
8:00pm	9:00pm	Poster Sessions of ICICE 2015, P5 (Poster Rooms)

附件三：IEICE 2015 研討會發表論文與論文海報

2015 International Conference on Innovation, Communication and Engineering

October 23 - 27, 2015, Xiangtan, Hunan, P.R. China

ASIC Design and Implementation for VoIP Intrusion Detection/Prevention System

Ming-Jen Chen[1,a], Chih-Chao Wen[2,b], Hsin-Chen Lin[3] and Yuan-Sun Chu[4,c]

[1,3,4] Department of Electrical Engineering ,National Chung Cheng University, Chia-yi, Taiwan (R.O.C.)

[2] Advanced Institute of Manufacturing with High-tech Innovations (AIM-HI), National Chung Cheng University, Chia-yi, Taiwan (R.O.C.)

[a]mingjen.chen@gmail.com, [b]ccwen@ccu.edu.tw, [c]chu@ee.ccu.edu.tw

Keywords: VoIP, IDPS, SIP stateful protocol analysis, ASIC, TCP/IP.

Abstract.

With the growing of Internet, voice over IP (VoIP) becomes more popular telephony application. VoIP is an Internet protocol, which is used for voice transmission over Internet. The main advantages of VoIP are low calling expense, low construction cost, easy scalability, and good voice quality. VoIP protocol is mainly constituted by the controlling signal and multimedia transmission. The controlling signal protocol, SIP and H.323 is used for making multimedia connection and controlling multimedia traffic. Because VoIP application is stacked over TCP/IP network, the security threats for TCP/IP network are also quite serious to affect VoIP application. Generally, the Traffic Filter method is proposed to fast identify normal traffic flow from abnormal traffic flow in the network layer. The Traffic Filter has the false positive problem for quick detection. Nevertheless, the characteristic of SIP stateful protocol analysis is to detect attack completely, but with slow processing speed. In this paper, the ASIC design and implementation for VoIP Intrusion Detection/Prevention system (IDPS) are integrated with Traffic Filter and Stateful Protocol Analysis. By combing VoIP network attack detection with defense mechanism, the merits of proposed VoIP IDPS can provide complete attack detection as well as increase processing speed. In addition, ASIC design and implementation for VoIP IDPS by parallelized architecture can improve not only fast data processing but also high data throughput up to 2.66Gbps.

1 INTRODUCTION

According to VoIP market prediction [1], the global VoIP services market was valued at USD 70.90 billion in 2013 and is expected to reach USD 136.76 billion by 2020, growing at a CAGR of 9.7% from 2014 to 2020. The Asia Pacific region is expected to be the fastest growing market for VoIP services. The CAGR for revenue generated in Asia Pacific is expected to be 13.6% from 2014 to 2020.

In report from TransNexus [2], the government's involvement in the telecom industry brings up another 2014 VoIP trend to watch. The hype over government surveillance of communications has brought to light many of the vulnerabilities of VoIP security. Without the well VoIP security policy, it is not difficult for anyone – government or criminal – to eavesdrop on VoIP calls. Although VoIP technology is very progressive, VoIP defense strategies are lagging far behind. Therefore, VoIP attack is a very serious problem. For VoIP security threats, Intrusion Prevention System (IPS) is useful to find unusual behavior from VoIP traffic.

The rest of the paper is organized as follows. In section 2, we describe the background and motivation to VoIP IPS. The architecture design is proposed for VoIP IPS in Section 3. The system implementation of VoIP IPS is realized in Section 4. In Section 5, we evaluate and discuss performance for VoIP IPS. Finally, we give the conclusion.

2 BACKGROUND AND MOTIVATION

VoIP protocol is mainly constituted by the controlling signal and multimedia transmission. The controlling signal protocol is used for making multimedia connection and controlling multimedia traffic, such as SIP (Session Initiation Protocol) and H.323. SIP improves the shortcomings of H.323, including the high complexity, slower calling setup, and low scalability. H.323 is gradually replaced by SIP in VoIP applications. Because VoIP application is over the TCP/IP network, so the security threats of TCP/IP network are also affect VoIP application threats to be quite serious.

VoIP security research organization specializing VOIPSA (Voice Over IP Alliance) [3] presents a list of VoIP attacks, which can be mainly divided into Request Flood, Malformed message, Spoof message, and Call Hijacking. Most IDS/IPS systems [4][5] only detect attacks by Stateful Protocol Anomaly Detection (SPAD) method. SPAD is used to distinguish the normal network communication behavior based on specified transmission protocol, and it has high accuracy of distinguishability between right and wrong network behavior. Most attacks are interpreted and extracted from application layer for identification. The characteristic of SPAD would have complete detection attack, but with slow processing speed.

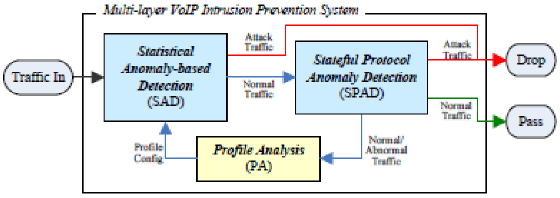


Figure 1. VoIP IPS system based on multi-layer intrusion prevention architecture

3 ARCHITECTURE DESIGN FOR VOIP IPS

This research proposed a VoIP Intrusion Prevention System (VoIP IPS) with the integration of Statistical Anomaly-based Detection (SAD) and Stateful Protocol Anomaly Detection (SPAD) methodologies based on Multi-layer Intrusion Prevention Architecture as shown in Figure 1. SAD can quickly detect as a traffic filter, but it has the problem with false positive ratio. SPAD can do fully comparison, but its network throughput is limited because of the complicated analysis algorithm. We extend the system with SAD as a traffic filter, which can quickly distinguish between normal and abnormal network traffic. The detection accuracy of traditional SAD is not very well, and traditional SPAD has performance issue. In this research, both SAD and SPAD modules are design to complement each other in IPS System. SPAD increases accuracy of attack detection, and SAD improves detection rate. The overall processing speed will be dramatically enhanced. The function descriptions for each methodology are presented as followings.

3.1 *Statistical Anomaly-based Detection (SAD)*

Statistical Anomaly-based Detection (SAD) is designed for packet filtering. There are four parameters of composition in detection profile for traffic filter to distinguish between normal and abnormal traffic, such as number of sessions per second, inter-arrival time, interval time and request to response message ratio.

3.2 *Stateful Protocol Anomaly Detection (SPAD)*

Stateful Protocol Anomaly Detection (SPAD) is usually implemented by finite state machine (FSM) and defines normal VoIP packet behaviors based on RFC3261 (SIP: Session Initiation Protocol) [6]. It is used to analyze the VoIP transactions for distinguish normal and abnormal network behavior. There are two concept of VoIP FSM design:

In addition to compliance with RFC3261, this research refers to SIP transaction flows (shown in Figure 2) in practice to design FSM based on RFC documents.

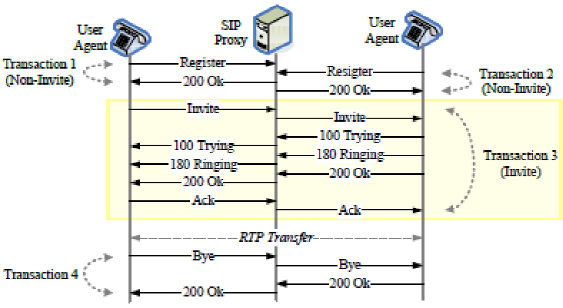


Figure 2. SIP transaction flows

Two blocks—Invite Transaction block and Non-Invite Transaction block—are defined in according to Invite and Non-Invite Transaction definition from RFC 3261. The proposed FSM of SPAD module is shown in Figure 3. When SIP packets passed and forward from SAD to SPAD. The packets will be classified into normal or abnormal traffic by FSM state checking.

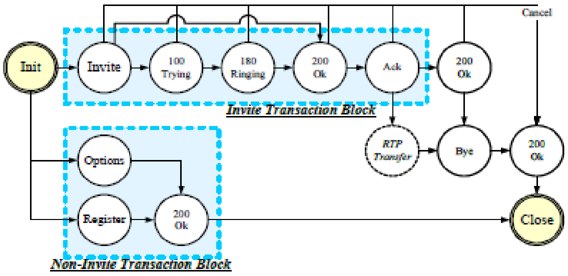


Figure 3. Finite state machine of SIP protocol

3.3 *Profile Analysis (PA)*

After SPAD distinguished normal and abnormal packets from SIP traffic, information of normal and abnormal packets will be sent to Profile Analysis (PA) for profile parameters analysis. The analyzed profile parameters will be used to update the parameters, number of sessions per second, inter-arrival time, interval time and request to response message ratio, in SAD. According to frequently profile update, it will improve the accuracy of SAD.

4 SYSTEM IMPLEMENTATION OF VOIP IPS

In addition, VoIP IPS system is implemented by hardware-based parallel computing to achieve fast data processing and high data throughput. The main system is divided into Statistical Anomaly-based Detection (SAD) module, SIP Stateful Protocol Anomaly Detection (SPAD) module and Profile Analysis (PA) module. Each packet will be transmitted between VoIP proxy and VoIP user agent and checked by VoIP IPS system.

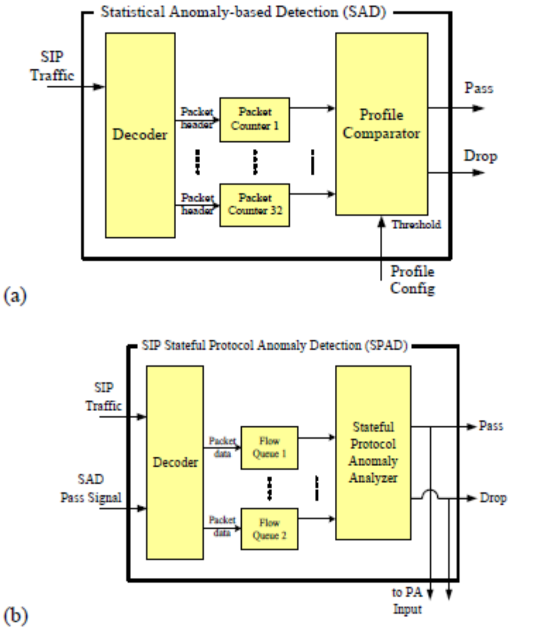


Figure 4. (a)Statistical anomaly-based detection (SAD) module; (b) SIP stateful protocol anomaly detection (SPAD) module;

4.1 *Statistical Anomaly-based Detection (SAD) Module*

Statistical Anomaly-based Detection (SAD) module is designed in according to profile parameters defined in section 3.1. Each packet is first checked its source/destination IP pair by IP compare sub-module. If packet belongs to existing IP pair, the packet information will be checked with profile parameters within existing IP pair in Parameter Comparator sub-module. If IP pair information is new to SAD module, the packet information will be added in profile parameter registers. The profile parameters in PA module are "Number of sessions per second", "Inter-arrival time", "Interval time", and "Request to response message ratio". The first two are used to compare the session count and difference time between N and N+1 request (or response). Third parameter is omitted in hardware design as hard monitored by IDS or IPS. Parameter Comparator sub-module of fourth parameter is designed with a divider for message ratio counting. The SAD module blocks are shown in Figure 4(a).

4.2 *SIP Stateful Protocol Anomaly Detection (SPAD) Module*

SIP Stateful Protocol Anomaly Detection (SPAD) module is designed with parallel processing as shown in Figure 4(b). Each VoIP session can be handled in one Flow processing module. With multiple flow processing modules, every request and response message of same flow will be queued the same register and passed to SPA Analyzer sub-module for parallel comparison.

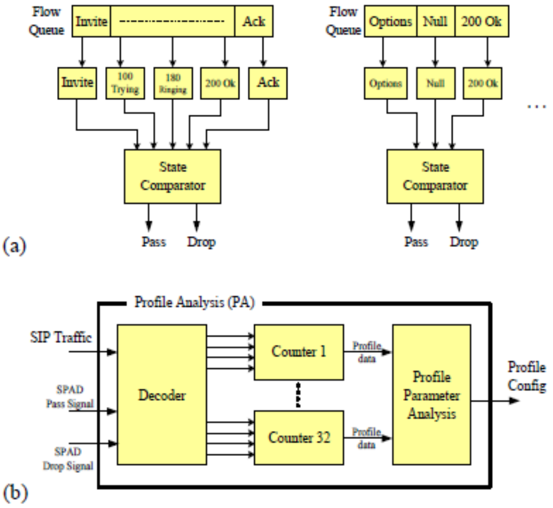


Figure 5. (a) Finite state machine comparator of stateful protocol anomaly analyzer sub-module; (b) Profile Analysis (PA) Module.

Stateful Protocol Anomaly Analyzer sub-module checks SIP request/response packets with predefined stateful protocol finite state machine as shown in Figure 5(a). If state transfer of packet does not match the finite state machine, the transaction may be considered as attack.

4.3 *Profile Analysis (PA) Module*

Profile Analysis (PA) module can generate new thresholds of profile parameters for SAD module by Profile Parameter Analysis sub-module with the input of normal and abnormal traffic from SPAD module. Architecture of PA module is shown in Figure 5(b).

4.4 *VoIP IPS System*

The VoIP IPS chip layout is shown in Figure 6. It has 215.1*215.2 um^2, chip speed is 500MHz, and power consumption is 337.1217 uW. Throughput of VoIP IPS is 2.66Gbps.

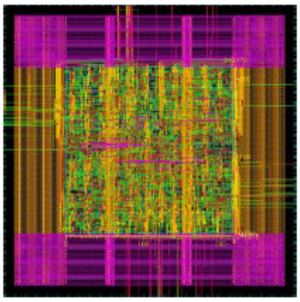


Figure 6. Chip layout of VoIP IPS

5 EXPERIMENTAL RESULTS AND ANALYSIS

5.1 *Experimental Environment and Tool*

VoIP IPS system must be placed between VoIP proxy and VoIP user agents for protecting the VoIP communications. When SIP communication start, every SIP packets will be monitored by VoIP IPS system. If there are Attackers send abnormal SIP packets, attack packets may be detected and discard by the IPS system.

Attack traffics are generated by Sivus [7] – a VoIP vulnerability scanner tool. There are several types of attack are generated for VoIP system testing, such as DoS Attack, Spoof Attack and Malformed Message. At start of experiment, SAD module will bypass all packets without setting any parameter, and send to SIP SPAD module for further checking. When SPAD module divided all packets into normal and abnormal, the attribute of normal and abnormal traffic will be sent to PA module for analysis and generate profile parameters for updating SAD module. After profile parameters setup, SAD module is enabled to support fast traffic distinguish and accelerate overall IPS system performance.

Table 1. Experimental results of IPS.

Normal Traffic Ratio	Abnormal Traffic Ratio	(VoIP IPS with SAD) Processing Time(ns)	(VoIP IPS without SAD) Processing Time(ns)	Speed Improvement Rate
100%	0%	30000	27000	-11.11%
90%	10%	27300	27000	-1.11%
80%	20%	24600	27000	8.89%
70%	30%	21900	27000	18.89%
60%	40%	19200	27000	28.89%
50%	50%	16500	27000	38.89%
40%	60%	13800	27000	48.89%
30%	70%	11100	27000	58.89%
20%	80%	8400	27000	68.89%
10%	90%	5700	27000	78.89%
0%	100%	3000	27000	88.89%

5.2 *Experiment Results of VOIP IPS*

The performance for IPS system is evaluated by adjusting the ratio of attack traffic under SAD module running conditions. The SIP SPAD module will cost 9 clock cycles for traffic analysis, but only 1 clock cycle for traffic analysis by SAD module. If most of the VoIP abnormal traffic is distinguished by SAD module, the system time will reduce to 90%.

Table 1 presents the results of experiment. Normal traffic distinguished from SAD module (1 clock cycle) will be sent to SIP Stateful Protocol Anomaly Detection module (9 clock cycles) for further analysis. Abnormal traffic can be classified within cost 1 clock cycle, but normal traffic will cost 10 clock cycles. If the ratio of normal traffic is increase, the overall processing speed will increase relatively. When the ratio of abnormal traffic is more than 60%, the overall processing time with SAD module will faster than without SAD module about 50%. When the abnormal traffic ratio increase, the overall detection effect will be more significant.

6 CONCLUSION

In this paper, we introduce several methods for VoIP security. The traditional stateful protocol analysis is used to do fully comparison based on protocol state change but in poor performance because of the complexity computing. And traditional traffic filter method can quickly distinguish between normal network traffic and abnormal network traffic, but accuracy of detection is not very well. Therefore, we proposed the integrated method for SAD (traffic filter) and SPAD (stateful protocol analysis) to complement its own advantages in VoIP IPS system. The SPAD method increases accuracy of attack detection, and SAD improves detection accuracy. The performance for overall system processing speed can be increased dramatically. The VoIP IPS system support would complete VoIP attack protection, such as Spoofing Attack, SIP Flooding Attack, Call Hijacking, and Malformed Message Attack. In additions, the proposed VoIP IPS chip design and implementation in parallel computing achieves fast data processing and high data throughput up to 2.66Gbps.

REFERENCES

[1] Transparency Market Research, "VoIP Services Market (Corporate Consumers and Individual Consumers) - Global Industry Analysis, Size, Share, Growth, Trends and Forecast 2014 – 2020," Transparency Market Research, New York, 2014.

[2] TransNexus. (2014). 2014 VoIP Industry Trends [Online]. Available: http://transnexus.com/company/newsletters/issue-9-january-2014/2014-voip-industry-trends/

[3] Voice Over IP Security Alliance. (2005). VoIP Security and Privacy Threat Taxonomy [Online]. Available: http://www.voipsa.org/Activities/VOIPSA_Threat_Taxonomy_0.1.pdf

[4] H. Sengary *et al.*, "VoIP Intrusion Detection Through Interacting Protocol State Machines," in Int. Conf. on Dependable Systems and Networks, 2006, pp. 393-402.

[5] E. Y. Chen, "Detecting DoS Attacks on SIP Systems," in 1st IEEE Workshop on VoIP Management and Security, 2006, pp. 53-58.

[6] SIP: Session Initiation Protocol, RFC 3261, 2002.

[7] SiVus, The VoIP Vulnerability Scanner – SiVuS [Online]. Available: http://www.securityfocus.com/tools/3528

2015
The Fourth International Conference on Innovation, Communication and Engineering
October 23 - 28, 2015, Xiangtan, Hunan, P.R. China || http://2015.icice.net/

ASIC Design and Implementation for VoIP Intrusion Prevention System

Ming-Jen Chen*, Chih-Chao Wen**, Hsin-Chen Lin* and Yuan-Sun Chu*
*Department of Electrical Engineering, National Chung Cheng University
**Advanced Institute of Manufacturing with High-tech Innovations (AIM-HI), National Chung Cheng University,
Chia-yi, Taiwan R.O.C

Abstract— With the growing of Internet, voice over IP (VoIP) becomes more popular telephony application. VoIP is an Internet protocol, which is used for voice transmission over Internet. The main advantages of VoIP are low calling expense, low construction cost, easy scalability, and good voice quality. McAfee Labs pointed out that VoIP technology is still very progressive, but VoIP defense strategies are lagging far behind. Therefore, VoIP attack is a very serious problem. Voice over IP Security Alliance (VOIPSA) proposed that Intrusion Detection/ Prevention Systems are useful to find unusual behaviour from VoIP traffic.

In this paper, the ASIC design and implementation for VoIP Intrusion Prevention system (IPS) with hierarchical architecture of Statistical Anomaly-based Detection (SAD) and Stateful Protocol Anomaly Detection (SPAD) modules is proposed. SAD is used to offload SPAD loading to increase VoIP IPS processing performance. And Profile Analysis (PA) module is proposed to decrease SAD false positive ratio by updating SAD profile threshold based on SPAD results.

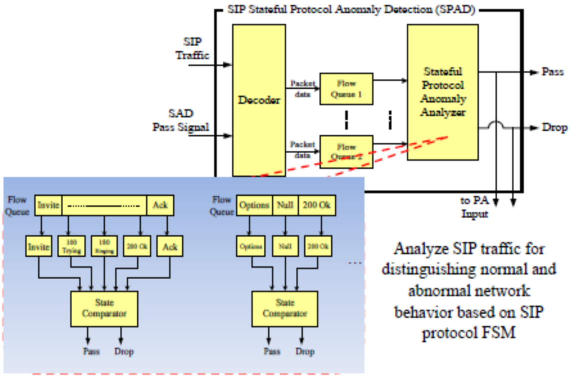
Introduction

VoIP technology is very progressive, VoIP defense strategies are lagging far behind. Therefore, VoIP attack is a very serious problem. For VoIP security threats, Intrusion Prevention System (IPS) is useful to find unusual behavior from VoIP traffic.

Motivation

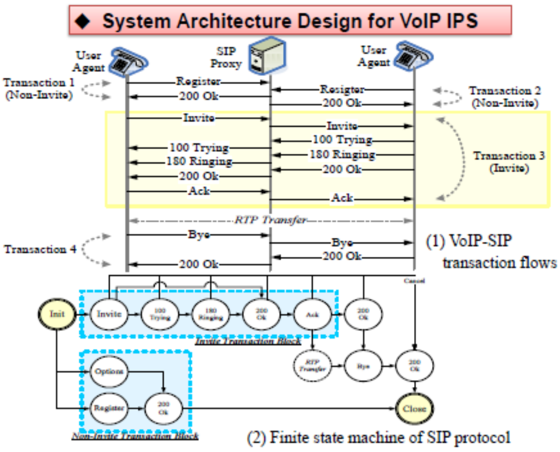
SPAD is used to distinguish the normal network communication behavior based on specified transmission protocol, and it has high accuracy of distinguishability between right and wrong network behavior. Most attacks are interpreted and extracted from application layer for identification. The characteristic of SPAD would have complete detection attack, but with slow processing speed.

◆ System Implementation for VoIP IPS



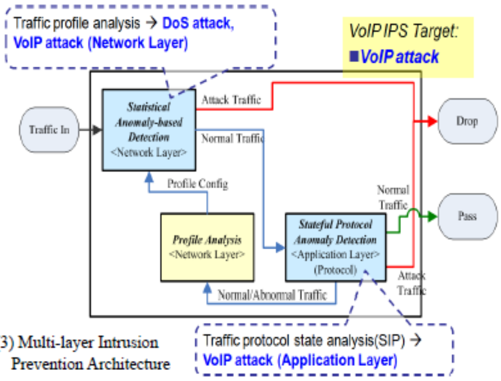
Analyze SIP traffic for distinguishing normal and abnormal network behavior based on SIP protocol FSM

◆ System Architecture Design for VoIP IPS



(1) VoIP-SIP transaction flows

(2) Finite state machine of SIP protocol


Traffic profile analysis → DoS attack, VoIP attack (Network Layer)
VoIP IPS Target:
■VoIP attack
Traffic In
Statistical Anomaly-based Detection <Network Layer>
Attack Traffic
Normal Traffic
Profile Config
Profile Analysis <Network Layer>
Stateful Protocol Anomaly Detection <Application Layer> (Protocol)
Normal Traffic
Attack Traffic
Normal/Abnormal Traffic
Drop
Pass
Traffic protocol state analysis(SIP) → VoIP attack (Application Layer)

(3) Multi-layer Intrusion Prevention Architecture

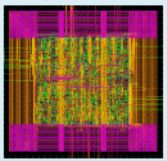
◆ Results and Evaluations

◆VoIP IPS
- ➢Reduce SAD false positive problem by SPAD
- ➢Frequently update SAD profile threshold by PA, increase SAD accuracy
- ➢Offload SPAD analysis load by SAD

◆Processing speed
- ➢ Within 20% attack traffic, the processing speed increases 8.89%
- ➢ Within 60% attack traffic, the processing speed increases 48.89%

◆ VoIP IPS throughput: 2.66Gbps

Chip layout of VoIP IPS
Size: 215.1*215.2 um^2
Chip speed: 500MHz
Power consumption : 337.1217 uW.



System Speed Improvement Rate
(with SAD vs. without SAD)

Normal Traffic Ratio	Abnormal Traffic Ratio	(VoIP IPS with SAD) Processing Time(ns)	(VoIP IPS without SAD) Processing Time(ns)	Speed Improvement Rate
100%	0%	30000	27000	-11.11%
90%	10%	27300	27000	-1.11%
80%	20%	24600	27000	8.89%
70%	30%	21900	27000	18.89%
60%	40%	19200	27000	28.89%
50%	50%	16500	27000	38.89%
40%	60%	13800	27000	48.89%
30%	70%	11100	27000	58.89%
20%	80%	8400	27000	68.89%
10%	90%	5700	27000	78.89%
0%	100%	3000	27000	88.89%

◆ Conculsion

This paper introduces several methods for VoIP security. The traditional stateful protocol analysis is used to do fully comparison based on protocol state change but in poor performance because of the complexity computing and the accuracy of detection.

Therefore, we proposed the integrated method for SAD (traffic filter) and SPAD (stateful protocol analysis) to complement its own advantages in VoIP IPS system. The SPAD method increases accuracy of attack detection, and SAD improves detection accuracy.

The performance for overall system processing speed can be increased dramatically. The VoIP IPS system support would complete VoIP attack protection, such as Spoofing Attack, SIP Flooding Attack, Call Hijacking, and Malformed Message Attack. In additions, the proposed VoIP IPS chip design and implementation in parallel computing achieves fast data processing and high data throughput up to 2.66Gbps.