應用於 4G 核心網路支援各種異質網路之 Cross-layer AAA

吳庭育、陳麒元、陳建宏、張凱迪、鍾俊豪
tyw@mail.ndhu.edu.tw
國立東華大學電機工程學系
趙涵捷
hcc@niu.edu.tw
國立宜蘭大學電子工程學系

摘要

第四代（4G）行動通訊系統預期會擁有更高的多媒體資訊承載能力、更快的傳輸速率及採用 IP 來傳遞資料等多項功能特點，未來服務網路勢必形成整合之 All-IP 的網路架構。另外傳統 OSI 網路七層架構已行之多年，各層級間互相分工來共同達成網路傳輸之目的。因此我們利用 Cross-layer 了的技術來提升 4G 網路的效能，所以本篇論文提出「應用於 4G 核心網路支援各種異質網路之 Cross-layer AAA」系統，可以在異質網路中進行認證整合，使 UE 在 Handoff 的過程中進行使用者認證的過程中，同時應用 Cross-layer 的技術使用底層協定來產生上層金鑰所需的 Seed 進行後續資料傳輸 IPsec 使用的金鑰，並經由我們設計的 AAA-Analyzer (Authentication, Authorization, Accounting，AAA）提供異質網路間計費、監控及側錄來解密傳輸資料等。

關鍵詞：第四代行動通訊、核心網路、AAA。

Abstract

The 4th generation mobile communication system certainly will have a lot of improvement such as supporting higher multimedia loading, faster transmission rate, and implementation of IP, the future service of the network will definitely convey into an All-IP network. Moreover, the traditional layered OSI model that each of the layers is given a certain task, now we introduce the concept of Cross-layer network to improve the performance of 4G network, we proposed in this paper “Application of Cross-layer AAA that supports various Heterogeneous Network Environment”, that is capable of authenticate in the heterogeneous network environment, and enable UE to acquire IPsec Key that is generated by Cross-layer technology during the handoff procedure, through our AAA-analyzer (authentication, authorization, accounting, AAA), we can provide accounting, control and monitoring of transmitted data in an heterogeneous network environment.

Keywords: 4G, Core Network, AAA.

1. 前言

網際網路及無線通訊的快速發展，使得人們得以隨時隨地利用輕便的無線裝置擷取或傳達語音、數據、多媒體等資訊。以技術而言，採用 IP 做為各種不同的通訊網路介面協定已是必然趨勢。第三代（3G）通訊的環境裡，使用者於靜止的狀態下，最快傳送速度可達 2Mbps，在移動的狀態下可達 384Kbps，但對於頻寬需求愈來愈大的多媒體應用服務而言，這樣的頻寬更顯得不足。第四代（4G）行動通訊系統預期會擁有更高的多媒體資訊承載能力、更快的傳輸速率及採用 IP 來傳遞資料等多項功能特點，因此服務網路必會是一整合之 All-IP 的網路架構。

傳統 OSI 網路七層的協定架構已行之多年，各層級間互相分工共同來達成網路傳輸之目的，分層負責的架構雖然可降低網路的複雜度、更快導入新的傳輸技術使整個網路更具有彈性，然而在現今多變及講求效率的環境下，卻也出現了無線網路環境(Wireless)或移動式(Mobile)網路環境下性能低落之問題，這些議題包含了無線網路介面的高錯誤率(Error Rate)、有效地節約電能消耗、服務品質

(Quality of Service)之提供和逐漸增加的移動式網路等。

有鑑於此本篇論文提出「應用於 4G 核心網路支援各種異質網路之 Cross-layer AAA」系統，這套系統建置 4G 網路測試平台並針對 Wi-Fi 網路及核心網路環境等，異質網路間使用者認證、金鑰的產生及資料加密等方式進行 Cross-layer 的整合。

2. 背景介紹

2.1 4G 和 WLAN 系統整合目標及功能

早在幾年前3GPP組織即針對雙網整合互通的可行性做了全盤的研究，以對WLAN和3GPP系統的相關標準影響最小為前提，提出六大漸近目標，從最簡單易實現的統一帳單和客服開始，漸近到完全無縫的系統整合服務，而其中每一目標皆涵蓋前一目標之功能。以下將簡單說明這六大漸近目標。

1) Common Billing and Service Care：此目標對原3GPP系統及WLAN並無新的需求，屬於系統管理的問題，使用者從行動網路業者取得一份帳單就可以同時繳納兩種網路的費用。
2) 3GPP System Based Access Control and Charging：以原3GPP系統的AAA機制統一兩種網路，讓使用者感覺不出兩種網路的認證差異；除此之外，在本階段使用者仍無法透過WLAN使用3GPP系統所提供的服務。關於此目標，3GPP已制定相關標準，於3GPP系統架構中新增AAA伺服器，並兼容WLAN之IEEE 802.1X認證架構，提出EAP-SIM之認證方法。目前此技術也已成熟。
3) Access to 3GPP System PS Based Services：讓使用者透過WLAN也可以使用3GPP系統所提供的數據服務，例如IMS Base服務、Location Base服務、即時訊息等。由於3GPP系統為一私有網路，故要讓3GPP以外的網路使用其服務需特別考量安全問題。關於此目標，目前3GPP已制定相關標準，但仍持續改版中。
4) Service Continuity：讓使用者於跨系統漫遊時，前目標所支援的服務連線不會中斷，其間使用者可能會感受到暫時的資料傳輸中斷，但不需手動重建服務連線。然而有些服務可能受限於新網路的服務能力等因素而被迫終止。關於本目標，目前雖有很多機構進行相關研究，但3GPP尚未完成相關標準。
5) Seamless Services：讓使用者於跨網漫遊時，消除前目標所能容忍的資料遺失和使傳輸中斷時間最小化。關於本目標，目前雖有很多機構進行相關研究，但3GPP尚未完成相關標準。
6) Access to 3GPP CS (Circuit Switched) Services：更進一步讓使用者可以透過WLAN使用3GPP CS 網路所提供的服務，但不隱含WLAN需提供具CS特性的服務。關於本目標，3GPP尚未完成相關標準。

2.2 Cross-layer

傳統TCP/IP網路七層的架構已行之多年，以傳統TCP/IP層之間的觀念可能無法解決很多問題，需考慮換個角度來看，以Cross-layer的方式來完成目的。圖 1 為 Cross-layer 協調平台 (Coordination Plane)，由圖中可看出，Security不再和以往一樣，只單做在Network層，Mobility也是，以前關注的問題在Network的 IP換手，而忽略上層可能出現的問題，現今以多層的方式去考慮，也將解決這樣的煩惱。因此我們提出建置4G網路測試平台並針對Wi-Fi網路及核心網路環境等，異質網路間使用者認證、金鑰的產生及資料加密等方式進行Cross-layer的整合；我們針對Wi-Fi網路及4G Cellular 網路，異質網路間使用者認證、資料加密及金鑰的產生等方式進行Cross-layer的整合。

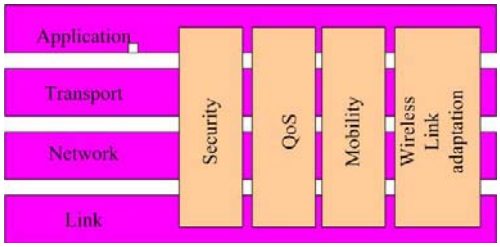


圖 1 Cross-layer 協調平台

3. 設計原理分析

本次系統分成五大主軸：1. 4G 網路及 Wi-Fi 的認證整合系統、2. AAA-Analyzer 系統、3. Cross-layer 加密金鑰產生系統、4. 加密資料側錄系統、5. 異

質網路計費系統，以下就針對這五項系統的設計原理進行介紹：

3.1 4G 網路及 Wi-Fi 的認證整合系統

我們根據 3GPP 標準所開發的系統，在封包交換網路所包含的元件有：無線電接取網路(Radio Access Network，RAN)和核心網路（Core Network）兩大部分。RAN 部分包括了無線電網路控制器(Radio Network Controller，RNC)與 Node B。核心網路部分則包括了 GPRS 支援節點(Serving GPRS Support Node，SGSN)，GPRS 閘道支援節點(Gateway GPRS Support Node，GGSN)，和本籍用戶伺服器(Home Subscriber Server，HSS)。如圖 2 所示之核心網路部分。

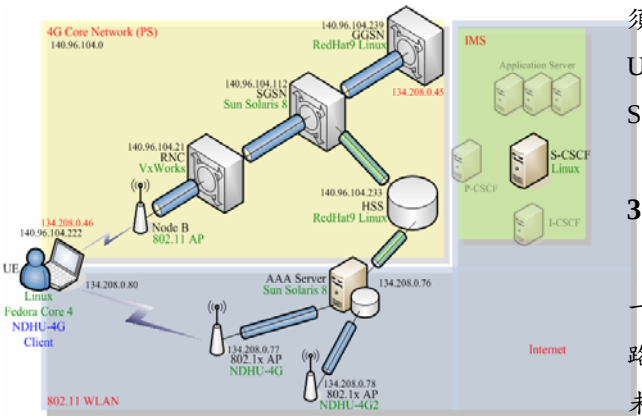


圖 2 4G 測試平台示意圖

在 RAN 方面，Node B 就像是無線區域網路的基地台，提供使用者終端設備(User Equipment，UE)連上核心網路的無線(Radio)傳輸介面。RNC 則作為 Node B 的控制者，負責管理 UE 與核心網路之間的連線。一個 RNC 和一個或多個的 Node B 組成一個無線電網路子系統(Radio Network Subsystem，RNS)，RAN 就是由這些 RNS 所構成的。

在核心網路方面，SGSN 連接核心網路與一個或多個的 RAN，負責存取控制(Access Control)、位置管理(Location Management)，路由管理(Routing Management)等工作。GGSN 則連接核心網路與外部的網路，作為核心網路與外部網路溝通的介面，負責核心網路內要傳到外部網路的封包轉送與路由，以及行動管理(Mobility Management)等工作。HSS 則是作為維繫整個網路運作的資料中心，其中最主要的元件是本籍位置記錄器(Home Location Register，HLR)，負責保存使用者的 Identity 位置以及所要求的服務等資訊。

由於 3GPP 手機的 Radio 是使用 License Band，需取得執照才能使用，因此我們改採用屬於 ISM Band 的 802.11g 來替代，透過廣播方式的 UDP 封包來模擬無線電網路，由於 UE 模擬程式上的協定堆疊(Protocol Stack)皆符合 3GPP 的規範，所有封包的行為皆與 3GPP 手機相同。透過 UE 連線程式能夠讓使用者進行取得封包交換網路中服務的流程，以便達到與手機相同的功能。

與無線網路達成雙網整合方面，認證伺服器(AAA Server)支援 EAP-SIM 認證方法來提供 UE 取得無線網路的服務連線。在驗證過程中 AAA Server 須向 HLR 取得 SIM 卡所屬之相關資訊，方可與 UE 進行後續的相互認證及授權程序。另外 AAA Server 亦收集計費資訊，提供後端之計費需求。

3.2 AAA-Analyzer 系統

未來電信網路業者他們經營的網路不單單是同一性質的網路，而是集合各種異質網路的 Mesh 網路，因此各種型態的網路的整合認證、計費等都是未來電信網路面臨的問題，如圖 3 所示。

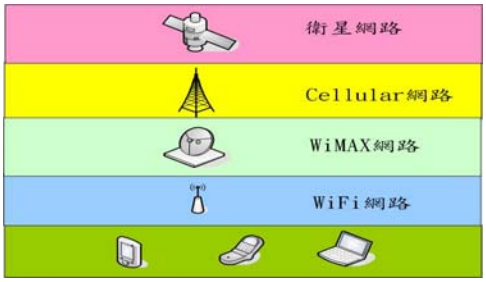


圖 3 各種異質網路的涵蓋

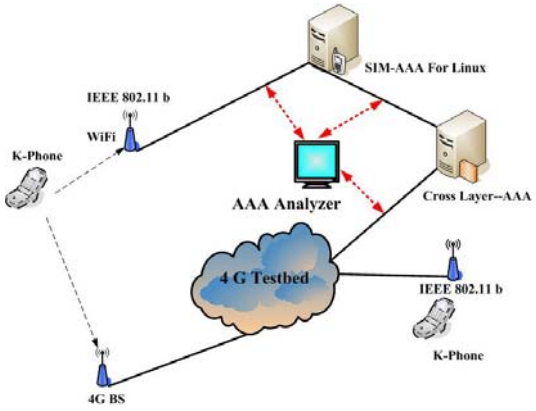


圖 4 AAA-Analyzer 系統架構圖

而 AAA-Analyzer 系統可以解決這些問題，為了分析通訊網路在同質/異質網路間進行 Inter Domain 或 Intra Domain Handoff 的過程，經由我們開發的這套 Analyzer AAA 監控系統來分析每一個信令的通聯過程，並且將這些過程以圖示方式呈現，以利網管人員進行監控；藉由我們這套系統可以追蹤使用者所在位置，如因特殊需求：例如防治犯罪，我們可以啟用 UE 加密的金鑰進行資料解碼，方便相關犯罪資料收集，如圖 4 所示。

3.3 Cross-layer 加密金鑰產生系統

使用 Analyzer AAA 系統的方式監控所有 UE 進行認證的過程，在認證的過程產生的 Cross-layer 金鑰進行後續資料的加密，如圖 5、6 所示，我們將這些資料存放在 Cross-layer AAA 主機中，可以明確的知道 UE 正使用哪種型態的網路進行連結，針對個別身份別或網路形態進行計費。

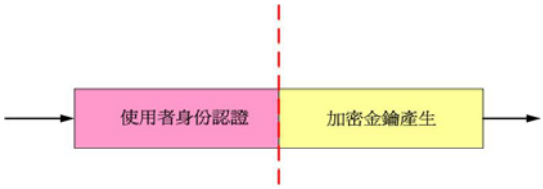


圖 5 UE 使用者認證階段與傳輸資料加密階段

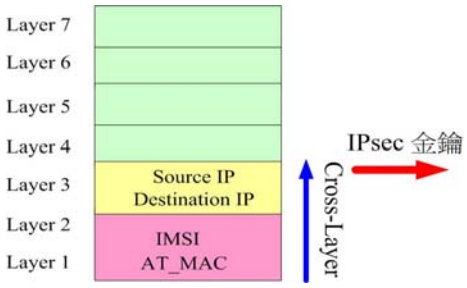


圖 6 Cross-layer IPsec 金鑰

3.4 加密資料側錄系統

另外我們提出的 Cross-layer AAA 可以提供使用者一個安全的通訊程序，配合國內電信法規規定，這些通訊器材必須配合檢調單位進行犯罪行為調閱通聯記錄及監聽的動作，可以經由 Analyzer AAA 系統進行認證資料及加密資料的還原及側錄的工作如圖 7 所示。

3.5 異質網路計費系統

因應未來無線通訊的營運，將會是各種異質網路的營運模式，並且使用者可以依據自己的所在地點及連結的無線環境，選擇自己適合的費率及連結速率，本次開發的系統，提供使用者可以選擇採用時間計費或流量計費的方案，提供一個依使用者需求導向設計之彈性化的計費系統。

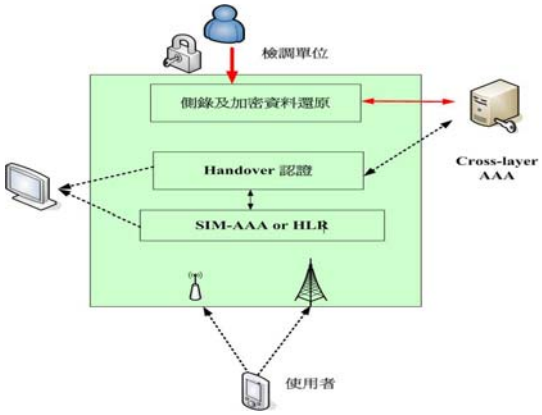


圖 7 AAA-Analyzer 內部模組設計

4. 實作結果

圖 8 所示為本篇論文提出「應用於 4G 核心網路支援各種異質網路之 Cross-layer AAA」系統，封包交換核心網路之運作流程如圖 9 所示，我們所開發的 4G 整合型 UE（圖中 a）要透過封包交換核心網路使用網路資源，首先 UE 會透過 RNC（圖中 b）來轉送(Relay) Attach Request 向 SGSN（圖中 c）登記註冊，此封包中含有 UE 的識別資訊。在 SGSN 收到請求後，利用這識別資訊對 4G UE 進行認證，SGSN 在認證成功之後，也會向 HLR（圖中 e）更新 UE 的位置資訊。接著 SGSN 會送出 Attach Accept 的訊息至 UE，以完成整個 Attach 的流程。當完成 Attach 的程序後，UE 會繼續進行 PDP Context Activation 動作。首先 UE 送出 Activate PDP Context Request 至 SGSN，請求取得 PDP Address。SGSN 收到了 Activate PDP Context Request 後，將會送出 Create PDP Context Request 至 GGSN（圖中 d），接著 GGSN 即建立此 UE 的 PDP Context，並且回傳 Create PDP Context Response 至 SGSN。SGSN 在收到回應之後，將在 SGSN 與 UE 之間建立通道。當 Attach 與 PDP Context Activation 的程序皆完成後 UE 便可以透過核心網路來存取服務或外部的網路資源。

無線網路運作流程如圖 10 所示，4G 整合型 UE（圖中 f）透過具有 802.1x 驗證功能之 AP(Access

Point)（圖中 g）轉送封包至 AAA Server（圖中 h）請求 Access-Request 行為，並主動告知此 SIM 卡使用者身份。當 AAA Server 接收請求封包，開始溝通驗證的方式，如目前所支援之 EAP-SIM 方法。當 UE 將驗證所需資訊回傳給 AAA Server，若此時 AAA Server 無 SIM 卡使用者之認證資料，則向 HLR（圖中 e）取得使用者身分資料，獲取資訊後 AAA Server 即可檢查 SIM 卡用戶是否可被授權使用 WLAN 資源，接著 UE 便可以透過 AP 來存取外部的網路資源或服務。圖 11 為 UE 連結 4G 及 SIM-Base 介面。

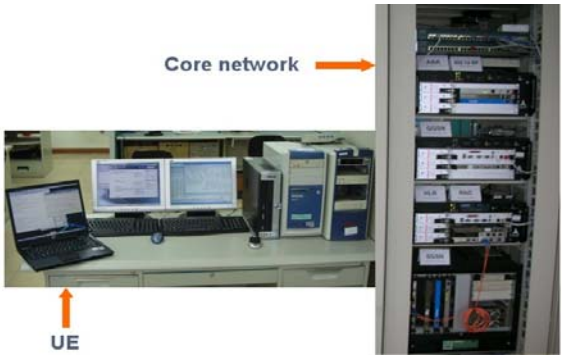


圖 8 應用於 4G 核心網路支援各種異質網路之 Cross-layer AAA 系統

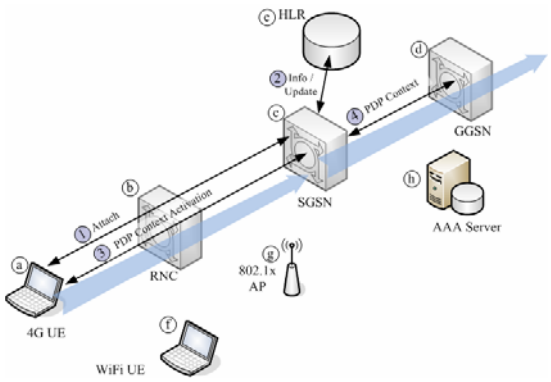


圖 9 4G 平台運作流程(I)

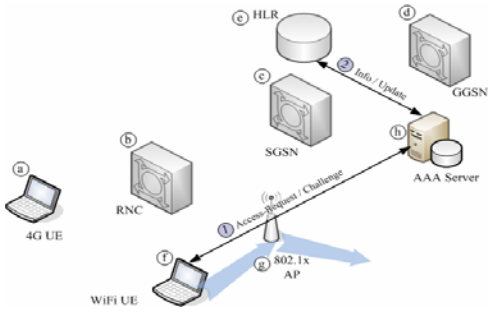


圖 10 4G 平台運作流程(II)

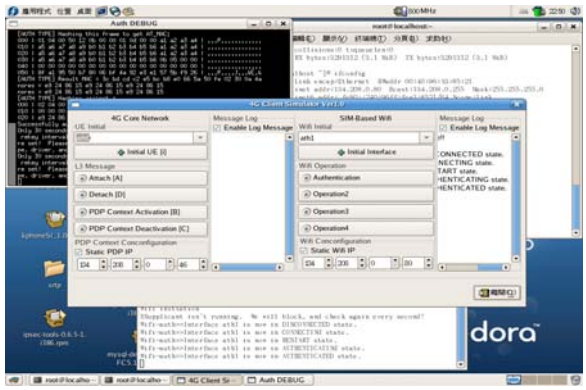


圖 11 UE 連結 4G 及 SIM-Based 介面

AAA-Analyzer 系統提供異質網路間計費、監控及側錄來解密傳輸資料等，此程式是以 Perl 語言撰寫而成，當使用者於 UE 端使用 4G 及 SIM-Based 介面進行連結時，AAA-Analyzer 便能將每一個傳輸信令擷取分析並以圖形化顯示，如圖 12 所示。

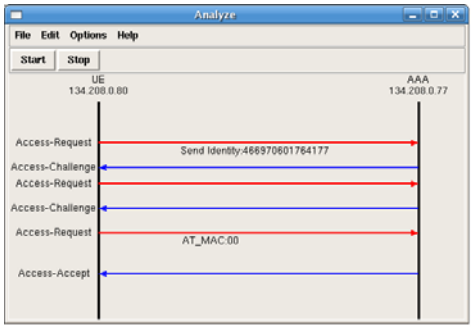


圖 12 AAA-Analyzer 各項交握訊號

我們在使用 Cross-layer 技術協助 UE Handoff 的過程之使用者認證及使用底層協定來產生上層金鑰所需的 Seed 參數進行後續資料傳輸 IPsec 使用的金鑰資料加密。另外為配合檢調單位進行各項通聯資料的還原，我們使用交通大學資訊系陳懷恩教授研發之 SIPv6 Analyzer 側錄系統為基礎搭配我們研發的解密機制側錄加密過的 SIP 通聯資料，經解密後原音重現，如圖 13 所示為 IPsec 解密機制搭配 SIPv6 Analyzer 系統。

最後，計費系統基本上是建構在一個計費的 Application Server，我們使用 PHP 的程式來開發，而得到計費資料的方式，是從 HLR 的 Raduis Server 上的資料庫所取得。由於 Radius Server 上的資料庫只紀錄 Core Network 的連線資料，並無 IB3G 上網的資料，所以 Radius Database 中建立了另一個表格，內有 source_ip, dest_ip,packet_id,packet_size,

auth_accept 這幾個欄位，用來分別記錄 IB3G 的連線資料，並且利用這上面的資料，透我我們所建立的計費程式，讓使用者可以即時查詢通話明細。本系統提供兩種計費方式讓使用者選擇，分別是時間計費，以及流量計費，提供一個 Web 介面，讓使用者可以查詢自己的使用狀況，讓使用者選擇最划算的方案，如圖 14、15 所示。

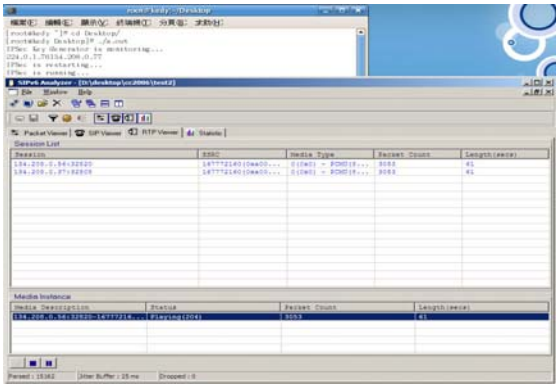


圖 13 P2P 側錄系統

4G CrossLayer 收費系統

Cellular 連線牌共應繳金額

使用者	計費方式	總上傳流量	上傳費率	總下載流量	下載費率	Cellular總流量應繳金額
DiegoChung	以流量計費	2.296875 (Kb)	25 (元/Kb)	2.296875 (Kb)	15 (元/Kb)	34 (元)

WiFi 無線網路連線牌共應繳金額

使用者	計費方式	總上傳流量	上傳費率	總下載流量	下載費率	WLAN總流量應繳金額
DiegoChung	以流量計費	125 (Kb)	0.05 (元/Kb)	366 (Kb)	0.02 (元/Kb)	13 (元)

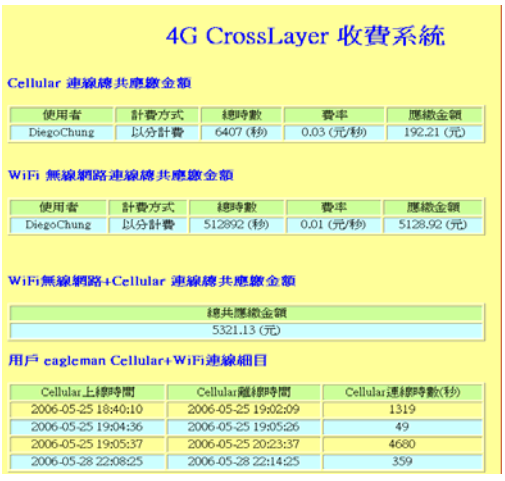
WiFi無線網路+Cellular 連線牌共應繳金額

總共應繳金額
47 (元)

用戶 eagleman Cellular+WiFi連線細目

Cellular上線時間	Cellular上傳流量	Cellular下載流量
2006-05-25 18:40:10	0	0
2006-05-25 19:04:36	1	1
2006-05-25 19:05:37	0	0
2006-05-28 22:08:25	0	0

圖 14 計費系統—以時間計費



4G CrossLayer 收費系統

Cellular 連線牌共應繳金額

使用者	計費方式	總時數	費率	應繳金額
DiegoChung	以分計費	6407 (秒)	0.03 (元/秒)	192.21 (元)

WiFi 無線網路連線牌共應繳金額

使用者	計費方式	總時數	費率	應繳金額
DiegoChung	以分計費	512892 (秒)	0.01 (元/秒)	5128.92 (元)

WiFi無線網路+Cellular 連線牌共應繳金額

總共應繳金額
5321.13 (元)

用戶 eagleman Cellular+WiFi連線細目

Cellular上線時間	Cellular離線時間	Cellular連線時數(秒)
2006-05-25 18:40:10	2006-05-25 19:02:09	1319
2006-05-25 19:04:36	2006-05-25 19:05:26	49
2006-05-25 19:05:37	2006-05-25 20:23:37	4680
2006-05-28 22:08:25	2006-05-28 22:14:25	359

圖 15 計費系統—以流量計費

5. 結論

本篇論文所開發之「應用於 4G 核心網路支援各種異質網路之 Cross-layer AAA」系統，的優點有：提供異質網路可以進行整合認證、協助 OP 維運人員可以掌控各項認證狀況，協助維運及故障排除、產生高效率及高安全性的 Seed 參數、協助打擊犯罪、可以針對各種環境依據時間、流量進行計費。未來尚有許多發展空間，例如可以在加入 IEEE 802.16 及 IEEE 802.20 等無線連結技術，可以應用更加廣泛。

參考文獻

[1] S.S. Dixit, “Evolving to Seamless All-IP Wireless/Mobile Networks,” IEEE Communications Magazine, Vol.39, No.12, pp.31-32, December 2001.

[2] NTP, “B3G 規劃報告”電信國家型計畫辦公室,11,2001.(www.ntpo.nsc.gov.tw/B3G)

[3] S. Huusko, “Nokia All-IP System Design Principles,” 3GPP all-IP Workshop, Nokia. (http://nokia.com)

[4] S. Wickware, “All IP in UMTS Networks- Benefits and Challenges,” Nortel Networks, (http://www.nortel.com)

[5] K.E.E Raatikainen, “Middleware Solution for all IP Networks,” Proceedings of the Second International Conference on 3G Mobile Communication Technologies, pp.335-340, 2001.

[6] H.C. Chao, Y.M. Chu, and M.T. Lin, ”The Implication of the Next-Generation Wireless Network Design: Cellular Mobile IPv6,” IEEE Transactions on Consumer Electronics, , Vol.46, No.3 , pp.656-663, 2000.

[7] T. Robles, A. Kadelka, H. Velayos, A. Lappetelainen, A. Kassler, L. Hui, D. Mandato, J. Ojala, and B. Wegmann, ”QoS Support for an All IP System Beyond 3G,” IEEE Communications Magazine, Vol.39, No.8 , pp.64-72, 2001.

[8] A.T. Campbell, J. Gomez, S. Kim, A.G. Valko, C.Y. Wan, Z.R. Turanyi, “Design, Implementation, and Evaluation of Cellular IP,” IEEE Personal Communications, Vol.7, No.4, pp.42-49, Aug. 2000.

[9]]W. Yurcik and D. Doss, “A Planning Framework Far Implementing Virtual Private Networks,” IT Professional, Vol.3, No.3, pp.41-44, 2001.

[10] K. Segaric, P. Knezevic, and S. Dembitz, “Possible Problems and their Solutions with IPv6 Router Announcement,” Proceedings of the International.

[11] 3GPP TS 24.228、3GPP TS 23.102、3GPP TS 23.002 v360、3GPP TS 23.002 v480、3GPP TS 23.002 v5c0、3GPP TS 23.002 v690.

[12] http://mobile01.com/topicdetail.php?f=18&t=1752&PHPSESSID=e82953549a5d71b0395f95556035df1e.

[13] 3G Americas, IMS Overview and Applications july, 2004.

[14] Vassilios Koukoulidis and Mehul Shah, The IP Multimedia Domain in Wireless Networks: Concepts, Architecture, Protocols and Applications 2004.

[15] 3GPP TR 22.934, “Feasibility study on 3GPP system to Wireless Local Area Network (WLAN) interworking”.

[16] 3GPP TS 23.234, “3GPP system to Wireless Local Area Network (WLAN) interworking; System description”.

[17] 3GPP TS 33.234, “3G Security; Wireless Local Area Network (WLAN) interworking security”.

[18] CCL AAA Server for WLAN-GPRS Interworking 系統需求規格書。

[19] H. Haverinen and J. Salowey, EAP SIM Authentication, Internet draft <draft-haverinen-pppext-eap-sim-11.txt> , Jun 2003.

[20] L. Blunk et al., Extensible Authentication Protocol (EAP), Internet draft <draft-ietf-pppext-rfc2284bis-03.txt>, May 2003.